Electronic Invoicing: Data, Infrastructures and Interconnection Possibilities

This repository documents, based on official sources, the data and infrastructures being implemented around the French electronic invoicing reform.

The objective is to clearly distinguish between:

- **ESTABLISHED**: explicitly established by an official source;
- **TECHNICALLY DEDUCIBLE**: made possible by the documented architecture, without any corresponding use being officially established;
- **HYPOTHESIS**: a scenario requiring additional evidence;
- **TO BE ESTABLISHED**: an identified question for which the sources examined do not yet provide sufficient evidence to draw a sufficiently robust conclusion.

Documentation

Chapter 1 — Invoicing Data

Invoicing, transaction and payment data transmitted to public authorities, as well as the level of granularity of those data.

→ Read Chapter 1

Chapter 2 — Data Retention, Access and Purposes

Retention of invoices and data, actors involved in their processing and transmission, official objectives of the reform, and elements that remain to be established regarding access, processing and potential data reuse.

→ Read Chapter 2

Chapter 3 — Environmental Data

Digital Product Passports, product identification, structured environmental data, carbon footprint, interoperability and the technical possibilities for linking these data with transaction data.

→ Read Chapter 3

Chapter 4 — Digital Euro and Payment Infrastructures

Architecture of the digital euro, payment data, programmability and the safeguards provided for.

→ Read Chapter 4

Chapter 5 — Interconnections

Investigation of existing, planned, experimented or technically possible interconnections between the different infrastructures.

→ Read Chapter 5

Chapter 6 — Legal Safeguards

GDPR, purpose limitation and data combination, profiling, proportionality, data subject rights, the CNIL, safeguards specific to the infrastructures examined, evolution of the legal framework and limits on interconnections.

→ Read Chapter 6

Chapter 7 — Conclusions

Synthesis of established facts, technical capabilities, documented interconnections, legal safeguards and elements that remain unestablished.

→ Read Chapter 7

Sources

Registry of the official sources used in the investigation.

→ View the sources

Chapter 1 — Invoicing Data Transmitted to the Administration

> **Navigation:** ← Back to the table of contents

This first chapter documents the invoicing, transaction and payment data transmitted to the administration as part of the French electronic invoicing reform.

The purpose of this repository is to document, based on official sources, the data collected, transmitted and processed as part of the French electronic invoicing reform.

The objective is not to present as established future uses that have not been established.

The method consists of documenting each component of the system separately, then examining the technical and legal possibilities for cross-referencing or further development of these infrastructures.

Each element is classified according to four levels:

- **ESTABLISHED**: explicitly established by an official source.
- **TECHNICALLY DEDUCIBLE**: made possible by the architecture or available data, without a corresponding officially established use.
- **HYPOTHESIS**: potential scenario requiring additional evidence to be demonstrated.

- **TO BE ESTABLISHED**: identified question for which the sources examined do not yet allow a sufficiently solid conclusion to be drawn.

Table of Contents

---

1. Transmission of invoicing data to the administration

1.1 The principle of transmission is officially established

Status: ESTABLISHED

The French electronic invoicing reform does not merely replace paper or PDF invoices with electronic documents.

It also organizes the transmission of data to the tax administration.

The DGFiP distinguishes three mechanisms:

1. electronic invoicing between businesses concerned;
2. electronic transmission of transaction data;
3. electronic transmission of payment or receipt data.

As part of electronic invoicing, approved platforms extract from the invoice the regulatory data intended for the administration S1.

For transactions subject to e-reporting, transaction or payment data are also transmitted to the administration S2-S3.

1.2 Role of the Public Invoicing Portal

Status: ESTABLISHED

Following the refocusing of the Public Invoicing Portal (PPF), it notably retains a role as a central hub for transmitting invoicing and transaction data to the tax administration S4.

The architecture can therefore be represented, in simplified form, as follows:

```
Business
   ↓
Approved platform
   ↓
Extraction / transmission of regulatory data
   ↓
Public Invoicing Portal
   ↓
Tax administration
```

The PPF is therefore not merely a directory enabling invoice routing.

It also constitutes a point of concentration for data intended for the administration S4.

1.3 Domestic B2B invoicing data transmitted to the administration

Status: ESTABLISHED

The DGFiP publishes a summary table of the invoice data that must be transmitted to the administration for domestic transactions carried out between two VAT-liable businesses established in France S1.

These data are introduced progressively in two stages.

From September 1, 2026

Data	Granularity
Supplier's SIREN	Invoice
Supplier's country of establishment	Invoice
Customer's SIREN	Invoice
Customer's country of establishment	Invoice
Transaction category: goods, services or both	Invoice
Issue date	Invoice
Unique invoice number	Invoice
Amount excluding VAT by VAT rate	Invoice
VAT amount by rate	Invoice
Applicable VAT rate	Invoice
Total amount excluding VAT	Invoice
Total VAT amount	Invoice
Currency	Invoice

Depending on the transaction, other information must also be transmitted:

- supplier's intra-Community VAT number;
- customer's intra-Community VAT number;
- identification of any tax representative;
- reference to the initial invoice in the event of a correction;
- option for payment of VAT on debits;
- reason for VAT exemption;
- self-billing;
- special VAT scheme;
- reverse charge;
- membership of a VAT group;
- actual date of delivery of the goods or performance of the service;
- date of payment of a deposit in the situations provided for.

From September 1, 2027

The granularity of the data transmitted increases.

The following notably become mandatory:

Data	Granularity
Precise description of the goods supplied or services provided	Invoice line
Quantity of goods or services	Invoice line
Unit price excluding VAT	Invoice line
Discounts, rebates and reductions	Line or document, as applicable
Fees and charges, for example transport costs	Line or document, as applicable
Delivery address when different from the customer's address	Line or document, as applicable
Date of the corrected invoice	Invoice
Early payment discount information	Invoice
Eco-contribution	Line or document, as applicable

From September 1, 2027, the administration therefore no longer receives only accounting and tax totals for domestic B2B invoices.

The regulatory transmission also includes information identifying the precise nature of the goods or services invoiced, their quantity and their unit price excluding VAT S1.

1.4 International B2B e-reporting

Status: ESTABLISHED

Transactions carried out with a VAT-liable business not established in France are also subject to data transmission to the administration S2.

From September 1, 2026, the information transmitted includes, in particular:

- identification of the French business;
- identification of the foreign business, notably through its intra-Community VAT number or a foreign identifier where one exists;
- supplier's country;
- customer's country;
- transaction category;
- invoice date;
- invoice number;
- amount excluding VAT by VAT rate;
- VAT amount by rate;
- VAT rates;
- total amount excluding VAT;
- total VAT amount;
- currency.

Depending on the transaction, other tax or transaction-related data are also transmitted.

From September 1, 2027, the following are notably added:

- precise description of the goods or services;
- quantity;
- unit price excluding VAT;
- price reductions;
- fees and charges;
- delivery address in the cases provided for;
- certain information relating to corrective invoices;
- eco-contribution.

The line-by-line granularity provided for certain data in 2027 therefore also applies to international B2B transactions falling within the scope of e-reporting.

1.5 Specific case of B2C

Status: ESTABLISHED

The processing of transactions carried out with non-taxable persons, particularly individuals, must be distinguished from B2B.

For these transactions, the DGFiP currently provides for aggregated transmission on a daily basis.

For each category of transactions concerned, the following are notably transmitted:

- date of the day;
- total taxable amount excluding VAT for the day's transactions;
- corresponding VAT amount;
- breakdown by VAT rate where several rates apply.

The documented regulatory framework therefore does not support the conclusion that, under the general B2C e-reporting framework, the administration receives individual details of each product purchased by each individual.

This distinction is essential:

B2B: data that may reach invoice-line level from 2027.

B2C: transaction data currently provided in aggregated form on a daily basis S2.

This distinction must be preserved in any subsequent analysis.

1.6 Payment data

Status: ESTABLISHED

The reform also includes e-reporting of payments for transactions where VAT becomes chargeable upon receipt of payment, notably certain supplies of services S3.

The data transmitted include:

- the date of actual receipt of payment;
- the amount received;
- the breakdown of the amount by VAT rate where necessary.

Where an electronic invoice exists, the transmission may be linked to it through its “paid” status.

The information then includes, in particular:

- the invoice number;
- the payment date;
- the amount received by VAT rate.

For certain international B2B transactions without the submission of an electronic invoice, payment data are also transmitted on an invoice-by-invoice basis.

For B2C, payment data follow the same logic as transaction e-reporting: they are aggregated on a daily basis.

1.7 Transmission architecture

Status: ESTABLISHED

Version 3.2 of the external specifications describes the Public Invoicing Portal as a central hub S4.

Its role includes the centralization of:

- invoicing data;
- transaction data;
- payment data;
- certain information relating to the invoice life cycle.

These data are then transmitted to the tax administration.

The architecture can therefore be represented in simplified form as follows:

```
Business
   ↓
Approved platform
   ↓
Regulatory data
   ↓
Public Invoicing Portal
   ↓
Tax administration
```

The complete invoice and the regulatory data transmitted to the administration must not be confused.

The administration receives the data provided for by the applicable legislation and specifications.

1.8 What this first chapter establishes

Status: ESTABLISHED

At this stage, the official documents establish that the reform creates a national infrastructure enabling the automated collection and transmission of structured economic data to the tax administration.

These data notably make it possible to identify:

- the businesses participating in a transaction;
- the date and number of the invoice;
- the general nature of the transaction;
- amounts excluding VAT;
- VAT rates and amounts;
- certain information relating to delivery;
- certain information relating to payment.

From September 1, 2027, for the B2B transactions concerned, this granularity also includes:

- the precise description of the goods or services;
- their quantity;
- their unit price excluding VAT.

It is therefore established that, for the B2B transactions concerned, the infrastructure enables structured data precisely describing the economic content of certain invoice lines to be transmitted to the administration.

However, the documents examined at this stage do not establish:

- that every purchase made by an individual is individually transmitted to the administration;
- that an individual consumption profile is created;
- that these data are currently used to calculate an individual carbon footprint;

- that they are cross-referenced with environmental data;
- that they are linked to a payment system or a digital currency;
- that a mechanism for individually restricting purchases is planned.

Chapter 2 — Data Retention, Access and Purposes

Navigation: ← Back to the table of contents

This chapter examines what happens to the data after it is transmitted as part of the French electronic invoicing reform.

Three questions are examined separately:

1. how long invoices and data must or may be retained;
2. which actors may access the information;
3. for what purposes these data may be used.

An essential distinction must be made between:

- the mandatory retention of invoices and documents by taxable persons;
- retention or processing carried out by approved platforms;
- retention of data transmitted to the tax administration.

These three mechanisms must not be confused.

Table of Contents

2.1 Retention of invoices and tax documents

Status: ESTABLISHED

The transmission of data to the administration does not remove the retention obligations applicable to businesses.

As of September 1, 2026, Article L. 102 B of the French Tax Procedures Code provides that books, registers, documents and records subject to the administration's rights of access, investigation and audit must be retained for six years S8.

Where they are created or received in electronic form, they must be retained in that form for the prescribed period.

This obligation notably concerns supporting documents enabling tax audits to be carried out.

Changes from January 1, 2027

The legislation provides for a significant change from January 1, 2027.

The general period provided for by Article L. 102 B then increases from six to ten years S8.

Books, registers, documents or records subject to the administration's rights of access, investigation and audit will have to be retained for ten years from the last transaction recorded or from the date on which the document was created.

Where they are created or received in electronic form, they will have to be retained in that form for this period.

A new Article L. 102 B bis also specifies that the retention of invoices must guarantee, from their issuance until the expiry of their retention period, the authenticity of their origin, the integrity of their content and their legibility S9.

Interim conclusion

From January 1, 2027, the French regulatory environment therefore provides for retention of up to ten years for documents and records falling within the scope of Article L. 102 B.

This retention obligation applies to taxable persons and to documents subject to administrative audit.

It does not, by itself, establish that the tax administration retains for ten years a copy of all data transmitted to it as part of electronic invoicing.

This question must be examined separately.

2.2 Retention and processing by approved platforms

Status: ESTABLISHED

Approved platforms are not merely instantaneous technical relays.

The French General Tax Code and its implementing provisions impose several obligations on them relating to the processing, transmission, security and, in certain cases, retention of information S10.

The platforms must notably ensure the transmission of electronic invoices under conditions guaranteeing:

- the authenticity of their origin;
- the integrity of their content;
- their legibility.

These guarantees must be ensured from the issuance of the invoice until the end of its retention period S10.

The platforms must also implement processes enabling the processing of:

- electronic invoices;
- invoicing data;
- transaction data;
- payment data.

These processes are among the elements reviewed as part of the registration and audits of approved platforms.

Retention of certain information related to the operation of the system

The regulations explicitly provide for certain retention obligations.

For example, when a taxable person authorizes a platform to update its information in the central directory, the corresponding formal agreement must be retained by the platform.

This agreement must be retained for three years after the date on which it ceases to have effect S10.

Platform audits also examine their processing, monitoring and archiving mechanisms, as well as the security measures applied to invoices and data.

Important limitation

These obligations do not establish that every approved platform must retain, for an identical period, all invoicing, transaction and payment data that it processes.

A distinction must be made between:

- the legal retention of the invoice;
- the retention of technical or regulatory elements by the platform;
- the transit and processing of regulatory data;
- the retention of data by the tax administration.

2.3 Retention of data by the administration

Status: TO BE ESTABLISHED

Chapter 1 established that invoicing data are transmitted to the tax administration by approved platforms.

The regulations notably provide that certain invoicing data must be transmitted by the issuer's platform within twenty-four hours following the submission of the invoice S11.

The existence of this transmission is therefore established.

However, the sources examined at this stage do not establish a single general period during which the tax administration would retain all invoicing, transaction and payment data received as part of the reform.

It would therefore be incorrect to infer from the retention period imposed on businesses that the DGFiP automatically retains these same data for an identical period.

Question remaining to be documented:

> For how long are the invoicing, transaction, payment and life-cycle data transmitted by approved platforms and centralized by the Public Invoicing Portal retained in the administration's systems?

2.4 Access to data

Status: ESTABLISHED / TO BE ESTABLISHED

The reform organizes several levels of data processing and transmission.

The legislation makes it possible to identify the main actors involved in the circulation of these data, but at this stage of the analysis it does not make it possible to establish exhaustively which administrative agents or departments may individually access each category of data once received by the administration.

Approved platforms

Approved platforms occupy a mandatory intermediary position within the electronic invoicing system S10.

They notably ensure:

- the receipt and processing of electronic invoices;
- the compliance checks required by the regulations;
- the transmission of invoices to the platforms of their recipients;
- the transmission of regulatory invoicing data to the administration;
- the transmission of transaction and payment data when subject to e-reporting.

They therefore process the information necessary to carry out these operations S10.

This access does not, however, mean that the platforms have a general right to reuse the data for any other purpose.

The tax administration

The French General Tax Code explicitly provides for the transmission to the administration of data generated by the system S7.

For B2B electronic invoicing, data from electronic invoices are transmitted to the administration by the approved platform chosen by the taxable person S7.

For transactions subject to e-reporting, transaction data and, in the situations provided for by the legislation, payment data are also transmitted to the administration S7.

The regulations also provide for a dedicated solution enabling the collection of S12:

- invoicing data;
- transaction data;
- payment data;
- certain information relating to processing statuses.

It is therefore established that the tax administration receives a structured set of economic data generated by the system.

The central directory must be distinguished from the tax data transmitted

The State also provides approved platforms with a central directory intended to enable the addressing of electronic invoices S12.

This directory notably contains information enabling the identification of taxable persons, public-law legal persons and approved platforms, as well as the information necessary for invoice routing S12.

Access to this directory by platforms must not be confused with general access to tax data collected by the administration.

These are two different functions of the system:

- the directory is primarily used for the identification and addressing of invoices;
- the dedicated solution collects the regulatory data intended for the administration S12.

What remains to be established

The sources examined therefore establish the circulation of data between businesses, approved platforms and the tax administration.

They do not yet establish with sufficient precision:

- which administrative departments have direct access to the databases containing these data;
- which categories of agents may individually access them;
- which technical authorizations are required;
- whether certain other departments or administrations may obtain direct or indirect access to these data;
- which logs and control procedures govern such access.

These elements require specific research into the data processing operations concerned, their authorization rules and any legislation or documents relating to their protection.

Question remaining to be documented:

> Which departments, agents or organizations may access the invoicing, transaction and payment data received by the administration, and under what authorization and traceability rules?

2.5 Official purposes of the reform

Status: ESTABLISHED

The transmission of data to the administration is not merely a technical consequence of the dematerialization of invoices.

The tax administration explicitly identifies several objectives associated with the reform and with the use of the information it makes possible to collect.

The Directorate General of Public Finances identifies four official objectives S5:

1. strengthening business competitiveness through the benefits of dematerialization;
2. ultimately simplifying VAT reporting obligations, notably through pre-filled returns;
3. improving the fight against VAT fraud;
4. improving real-time knowledge of business activity and the management of public policies.

These objectives are presented directly by the DGFiP in its documentation relating to the reform S5.

Automatic and continuous use of data

The educational documentation published by the DGFiP provides an additional clarification regarding the fourth objective S6.

It states that the availability and use of data obtained automatically and continuously should facilitate the management of the economy by public authorities.

The information reported through invoicing should notably provide real-time knowledge and visibility of economic conditions, particularly by sector of activity.

It is therefore officially established that the use of data generated by the system does not serve exclusively the purpose of VAT control.

The data must also contribute to knowledge of economic activity and the management of public policies.

Distinction between established purposes and their future uses

The existence of this public policy management objective does not, however, mean that any public policy could freely use the data collected.

At this stage, the sources examined establish:

- the objective of combating VAT fraud;
- the objective of pre-filling VAT returns;
- the objective of real-time knowledge of business activity;
- the objective of public policy management;
- the use of data obtained automatically and continuously to improve knowledge of economic conditions.

They do not, by themselves, establish:

- the use of the data for environmental policy;
- the creation of an individual carbon footprint;
- the use of the data to restrict certain transactions;
- their interconnection with a digital monetary infrastructure;
- a general right allowing the administration to reuse the data for any future purpose.

These potential possibilities must be examined separately in the chapters devoted to environmental data, payment infrastructures, interconnections and legal safeguards.

Interim conclusion

The reform therefore establishes not only a mechanism for transmitting data to the tax administration, but also officially provides for the information obtained to contribute to more timely knowledge of economic activity.

Public policy management is explicitly among the stated objectives of the reform.

ESTABLISHED:

> The administration states that data obtained automatically and continuously should notably improve real-time knowledge of economic activity and facilitate the management of the economy by public authorities.

TO BE ESTABLISHED:

> Which public policies may legally use these data, in what form, at what level of granularity and subject to what limitations?

2.6 Tax audits and combating fraud

Status: ESTABLISHED / TO BE ESTABLISHED

Combating VAT fraud is explicitly one of the official objectives of the French electronic invoicing reform S5.

The DGFiP indeed identifies “improving the fight against VAT fraud” as one of the reform's four objectives.

This purpose must be considered in relation to the nature of the information transmitted to the administration.

As documented in Chapter 1, the system organizes the electronic transmission of data relating to:

- electronic invoices;
- transactions subject to e-reporting;
- payments or receipts in the situations provided for by the legislation.

Data directly related to the determination of VAT

The French General Tax Code explicitly establishes a link between certain data transmitted and the determination of the tax S7.

For transactions where VAT becomes chargeable upon receipt of payment, payment-related data are communicated electronically to the administration S7.

The legislation specifies that the data to be transmitted are those necessary to determine when value added tax becomes chargeable S7.

Transaction data transmitted as part of e-reporting also include, depending on the situations provided for by the legislation, information such as:

- the transaction category;

- the taxable amount excluding VAT;
- the tax rate;
- the corresponding VAT amount;
- the total amount of VAT due in France;
- the date of the transactions.

The system therefore provides the administration with structured data that can be directly used to determine certain elements relating to VAT S7.

Organized and automated transmission

The reform also changes the way in which this information reaches the administration.

Regulatory data from electronic invoices are extracted and transmitted by approved platforms.

Transaction and payment data subject to e-reporting are also transmitted electronically through these platforms.

These are therefore not merely pieces of information that may be requested on an occasional basis by the administration as part of an audit.

The system provides for their electronic transmission in accordance with the obligations, frequencies and procedures defined by the legislation.

Monitoring of transmission obligations

The DGFiP also has a service responsible for the registration and monitoring of approved platforms S13.

The missions officially assigned to this service notably include:

- monitoring the transmission obligations applicable to approved platforms and their users;
- the possible imposition of financial penalties in the event of non-compliance;
- the possible withdrawal of a platform's registration in the event of repeated breaches.

The transmission of data is therefore itself an obligation subject to administrative monitoring S13.

What these elements establish

It is established that:

- combating VAT fraud is an official objective of the reform S5;
- structured data relating to invoices, transactions and payments are transmitted electronically to the administration S7;
- some of these data are explicitly defined as necessary to determine when VAT becomes chargeable S7;
- transaction data include elements enabling the taxable bases and corresponding VAT amounts to be determined S7;
- compliance with transmission obligations is itself monitored by the administration S13.

These different elements therefore establish a direct link between the transmission infrastructure introduced by the reform and the tax objectives relating to VAT.

Algorithmic processing of electronic invoicing data

The available documentation now establishes that data generated by electronic invoicing are intended to be integrated into the DGFiP's automated “fraud targeting and query enhancement” (CFVR) processing system S37.

In its opinion of June 18, 2026, the CNIL states that the addition of these data substantially increases the volume of information processed, with the DGFiP estimating the volume of electronic invoices at approximately 2 to 3 billion per year S37.

These data are intended to feed the DGFiP's secure data platform and may be used to identify anomalies and businesses presenting certain tax risks S37.

Query results may also be cross-referenced with other data within the CFVR processing system. This system notably uses algorithmic and machine-learning methods, including certain unsupervised learning methods S37.

The CNIL nevertheless highlights the risks of bias and the amplification of such biases, and considers it essential that results generated by algorithmic processing do not replace human analysis prior to the opening of a tax audit S37.

What these elements do not establish

These elements do not, however, establish that:

- each electronic invoice automatically triggers an individual analysis or tax audit;
- each business automatically receives a risk score based on all of its invoices;
- algorithmic results automatically lead to the opening of an audit;
- invoicing data are systematically cross-referenced with all other databases held by the administration;
- the data may be reused without limitation for purposes unrelated to those provided for by the processing systems concerned.

The existence of algorithmic processing and cross-referencing possibilities within CFVR is therefore established. The exact scope of the processing, the cross-references performed and the data actually used must be distinguished from this documented capability.

Interim conclusion

ESTABLISHED:

> Data generated by electronic invoicing are intended to feed the CFVR processing system and the DGFiP's secure data platform. They may notably be used to identify anomalies and certain situations presenting a tax risk, within a processing system using algorithmic and machine-learning methods S37.

TO BE ESTABLISHED:

> What is the exact scope of the processing applied to electronic invoicing data within CFVR, which other categories of data are actually cross-referenced with them, and how do these analyses contribute to the targeting of tax audits?

2.7 Knowledge of economic activity

Status: ESTABLISHED / TO BE ESTABLISHED

Real-time knowledge of business activity is explicitly one of the official objectives of the reform S5.

The DGFiP also states that the availability and use of data obtained automatically and continuously should facilitate the management of the economy by public authorities S6.

The information reported through invoicing should notably provide real-time knowledge and visibility of economic conditions, particularly by sector of activity S6.

An explicitly documented economic policy management objective

The stated objective is not limited to producing general statistical knowledge of the economy.

The preparatory documents for the reform indicate that improving real-time knowledge of business activity should enable economic policy to be managed "as closely as possible to the economic reality of economic actors" S14.

The preliminary assessment of the system also provides a concrete example of an envisaged use of this information: the data collected could enrich analytical models in order to facilitate the detection and support of businesses in difficulty S14.

It is therefore established that the reporting of data generated by the system was notably designed to improve the capacity to analyze the economic situation and contribute to the management of economic policies.

An infrastructure providing structured economic data

As established in Chapter 1, the data transmitted to the administration include, depending on the transactions concerned, the identification of the businesses participating in the transaction, invoice dates and numbers, the transaction category, amounts excluding VAT, VAT rates and amounts, as well as certain payment-related information S1-S2-S3.

From September 1, 2027, certain B2B transactions also include invoice-line-level data, notably the precise description of the goods or services, the quantity and the unit price excluding VAT S1-S2.

These data therefore do not consist solely of overall tax totals: in the situations provided for by the legislation, they also describe the economic content of transactions with a greater level of granularity.

Combined with the automated and continuous reporting of information S6, this granularity provides the administration with a data infrastructure enabling more detailed and timely knowledge of certain components of economic activity.

What these elements establish

It is established that:

- real-time knowledge of business activity is an official objective of the reform S5;
- data obtained automatically and continuously are intended to contribute to knowledge of economic conditions, particularly by sector of activity S6;
- the management of the economy by public authorities is explicitly mentioned in the DGFiP's documentation S6;
- the preparatory work for the reform refers to managing economic policy as closely as possible to the economic reality of economic actors S14;
- enriching analytical models in order to facilitate the detection and support of businesses in difficulty is explicitly presented as an example of a possible use of the data collected S14.

These elements therefore establish that the data collection provided for by the reform also has a dimension of observing and analyzing economic activity, distinct from its use for VAT and combating fraud.

What these elements do not establish

These sources do not, however, by themselves establish that:

- each business is subject to permanent individual economic monitoring;
- the data from each invoice are currently used to automatically assign an economic profile or score to each business;
- all available data are systematically used in economic analytical models;
- the data may be freely used for any public policy;
- the data are currently cross-referenced with environmental, monetary or individual behavioral information.

The exact nature of the processing carried out using these data, their level of aggregation, the analytical models actually used and the legal rules governing these uses must be distinguished from the possibilities offered by the infrastructure.

Interim conclusion

ESTABLISHED:

> The reform provides for economic data obtained automatically and continuously to contribute to improving real-time knowledge of business activity and economic conditions, particularly by sector of activity, in order to facilitate the management of the economy and economic policies S5-S6-S14.

ESTABLISHED:

> The preparatory work for the reform explicitly mentions, as an example, the possibility of enriching analytical models with the data collected in order to facilitate the detection and support of businesses in difficulty S14.

TO BE ESTABLISHED:

> Which analytical models are actually fed by data generated through electronic invoicing, at what level of granularity, in what form and under what rules governing access, aggregation and reuse?

2.8 Limitations and elements remaining to be established

Status: TO BE ESTABLISHED

The elements documented in this chapter establish the existence of an organized system for the collection, transmission and use of structured economic data through approved platforms and the tax administration.

They also make it possible to identify several official objectives associated with the reform, notably combating VAT fraud, pre-filling tax returns, real-time knowledge of business activity and public policy management S5-S6.

However, certain essential characteristics of the processing of these data remain to be documented.

Retention period by the administration

The retention obligations imposed on businesses and certain obligations applicable to approved platforms are established S8-S9-S10.

However, the sources examined do not yet establish a single general period during which the tax administration retains the invoicing, transaction, payment and life-cycle data received as part of the reform.

TO BE ESTABLISHED:

> What is the retention period for each category of data in the administration's systems, and which rules determine their deletion or archiving?

Access and authorizations

The circulation of data between businesses, approved platforms and the administration is documented S7-S10-S11-S12.

However, the sources examined do not yet make it possible to exhaustively identify the departments, agents or organizations that may access the different categories of data once they have been received by the administration.

TO BE ESTABLISHED:

> Which departments and agents have access to the data, under what authorizations, and which logging and control mechanisms make it possible to trace their access?

Automated processing and data cross-referencing

The electronic and structured transmission of data is established, as is the objective of automatic and continuous use notably intended to improve knowledge of economic conditions S4-S6.

The preparatory work for the reform also mentions the possibility of enriching analytical models using the data collected, notably in order to facilitate the detection and support of businesses in difficulty S14.

The existence of automated processing applied to electronic invoicing data is no longer merely a possibility to be established. The CNIL confirms their integration into the CFVR processing system, which notably uses algorithmic and machine-learning methods for tax analysis and targeting S37.

However, the exact scope of these processing operations and the cross-references actually performed remains to be documented.

TO BE ESTABLISHED:

> Which algorithmic methods are actually applied to electronic invoicing data within CFVR, which other categories of data are cross-referenced with them, and at what level of granularity?

Cross-referencing with other databases

The existence of an infrastructure enabling the transmission of structured economic data does not demonstrate that these data are systematically cross-referenced with other databases held by the administration or by other public bodies.

The sources examined in this chapter notably do not establish the existence of systematic cross-referencing with environmental, social, banking, monetary or individual consumption data.

TO BE ESTABLISHED:

> With which other databases may information generated through electronic invoicing be legally or technically cross-referenced, and which cross-references are actually performed?

Reuse for public policy management

Public policy management and real-time knowledge of business activity are explicitly among the official objectives of the reform S5-S6.

This wording does not, however, by itself determine all the public policies that may use the data collected or the legal conditions under which such reuse could take place.

A distinction must notably be made between the general objectives announced for the reform and the precise legal purposes attached to the different data processing operations.

TO BE ESTABLISHED:

> What are the precise legal purposes of the processing operations concerned, and under what conditions may the data be reused for other public policies?

Aggregation, anonymization and granularity

The sources examined establish that certain data are transmitted with a high level of granularity, notably at invoice-line level for certain B2B transactions from September 1, 2027 S1-S2.

They also establish that general B2C e-reporting is based on data aggregated on a daily basis and therefore does not, based solely on the elements examined, establish that the details of each individual purchase made by an individual are transmitted to the administration S2.

However, the level of granularity actually used in economic or statistical analyses carried out using these data remains to be documented.

TO BE ESTABLISHED:

> Do processing operations intended to provide knowledge of economic activity and support public policy management use individual, aggregated, anonymized or pseudonymized data, and at what stage do these transformations take place?

Interim conclusion

The main uncertainties identified therefore no longer concern the existence of the transmission infrastructure or the general nature of the data collected, which are documented, but rather the precise conditions governing their retention, access, use and potential reuse.

These questions will need to be examined against the legislation relating to data processing, authorization rules, legal safeguards and any technical documentation describing the systems actually used.

They also constitute essential points of verification for the following chapters, particularly when a possible interconnection with another infrastructure is examined.

2.9 What this chapter establishes

The analysis of legislative and regulatory texts and official documents now makes it possible to distinguish the established characteristics of the system from the elements that remain to be documented.

ESTABLISHED

The French electronic invoicing reform establishes an organized infrastructure enabling the electronic transmission to the administration of structured data relating to invoices, transactions and, in the situations provided for by the legislation, payments S4-S7.

Approved platforms process and transmit the information necessary for the operation of this system and are subject to regulatory obligations as well as an administrative monitoring mechanism S10-S13.

Businesses remain subject to their own obligations regarding the retention of tax documents. The period provided for by Article L. 102 B of the French Tax Procedures Code increases from six to ten years from January 1, 2027 under the conditions provided for by the legislation S8, while the rules applicable to invoices also impose guarantees relating to the authenticity of their origin, the integrity of their content and their legibility S9.

These retention obligations do not, however, make it possible to infer an identical retention period by the administration for the data it receives.

Combating VAT fraud, pre-filling VAT returns, real-time knowledge of business activity and public policy management are among the officially stated objectives of the reform S5.

The DGFiP also states that the availability and use of data obtained automatically and continuously should facilitate knowledge of economic conditions, particularly by sector of activity, as well as the management of the economy by public authorities S6.

The preparatory work for the reform also mentions, as an example, the possibility of enriching analytical models with the data collected in order to facilitate the detection and support of businesses in difficulty S14.

It is therefore established that the infrastructure does not serve solely a technical function of transmitting invoices: the data collected are also intended to contribute to tax objectives and to knowledge of economic activity.

TO BE ESTABLISHED

The sources examined in this chapter do not yet establish with sufficient precision:

- the retention period for each category of data in the administration's systems;
- the departments and categories of agents that may directly access the different data;
- the precise authorization, logging and access-control rules;
- the precise scope of the algorithmic processing applied to electronic invoicing data within CFVR and the exact methods used to cross-reference them with other data within the processing system;
- the existence and nature of systematic cross-referencing with other databases;
- the level of granularity actually used for economic analyses and public policy management;
- any aggregation, anonymization or pseudonymization mechanisms applied;
- the precise legal purposes attached to the different processing operations and the conditions under which the data may be reused for other public policies.

Limit of the analysis

The existence of an infrastructure enabling the collection and use of structured economic data does not, by itself, demonstrate the existence of a general system of individual economic surveillance.

Nor does it demonstrate the existence of an interconnection with environmental data, a digital monetary infrastructure or mechanisms enabling certain transactions to be conditioned or restricted.

These hypotheses require the existence of other infrastructures, compatible data and interconnection mechanisms that must be documented separately.

The following chapters will therefore successively examine environmental data, digital payment infrastructures, interconnection possibilities and the legal safeguards that may govern or limit these uses.

Chapter conclusion

ESTABLISHED:

> The French electronic invoicing reform organizes the transmission of structured economic data to the administration and explicitly provides for their use for tax purposes, as well as to improve real-time knowledge of economic activity and public policy management S5-S6-S7.

ESTABLISHED:

> Official documentation provides for the use of data obtained automatically and continuously, and the preparatory work explicitly envisaged their use to enrich certain economic analytical models S6-S14.

TO BE ESTABLISHED:

> The precise conditions governing retention by the administration, access to the data, the scope and methods of automated processing, cross-referencing with other databases and reuse for other public policies remain to be documented.

HYPOTHESIS:

> Any future interconnection of this infrastructure with other data systems cannot be inferred solely from the existence of the electronic invoicing system and must be examined separately.

Chapter 3 — Environmental Data

> **Navigation:** ← Back to the table of contents

This chapter examines the systems that make it possible to associate structured environmental data with products, as well as their level of granularity and the infrastructures intended to make them accessible.

The objective is notably to determine which environmental information can be associated with a product, in what form it can be identified or accessed, and whether a link with the economic data examined in the previous chapters is officially provided for.

An essential distinction must be made between:

- environmental data relating to a product;
- the digital identification of a product;
- the calculation of a product's environmental or carbon footprint;
- the possible attribution of this information to a transaction;
- the possible establishment of an individual environmental profile.

The existence of the first elements does not automatically demonstrate the existence of the subsequent ones.

Table of contents

3.1 The Digital Product Passport

Status: ESTABLISHED

The European Union has established a legal framework for the Digital Product Passport under Regulation (EU) 2024/1781 on ecodesign for sustainable products S15.

The system does not merely consist of displaying environmental information intended for consumers. It is based on an infrastructure that makes it possible to associate a set of structured digital data with a product and make those data accessible according to rules defined by the regulation S15.

A digital identifier associated with the product

The Digital Product Passport must be linked, through a data carrier, to a persistent unique product identifier S15.

Depending on the rules applicable to each product group, the passport may be established at the level of:

- the model;
- the batch;
- the individual item.

The level of granularity is therefore not necessarily limited to a general product category: the regulatory framework allows a passport to correspond, where the rules applicable to the product so provide, to an individual item S15.

Data designed to be usable by computer systems

The data contained in the Digital Product Passport must be based on open standards and use an interoperable format S15.

They must also, where appropriate, be:

- machine-readable;
- structured;
- searchable;
- transferable through an open and interoperable data exchange network.

The regulation also provides for technical, semantic and organizational interoperability between Digital Product Passports S15.

The system therefore constitutes a structured data infrastructure designed to enable their processing and circulation between different computer systems, according to the applicable access rights.

A digital registry managed by the European Commission

The regulation provides for the establishment by the European Commission of a digital registry of product passports S15.

This registry contains at least the unique identifiers provided for by the system. For certain imported products, it also contains the corresponding commodity code S15.

The European Commission manages the registry.

The Commission, the competent national authorities and customs authorities have access to the registry for the performance of the tasks assigned to them under Union law S15.

A public web portal must also allow stakeholders to search for and compare certain data contained in the passports, within the limits of their respective access rights S15.

Interconnection with another public infrastructure is explicitly provided for

The regulation explicitly provides for an interconnection between the Digital Product Passport registry and the European Union Customs Single Window Certificates Exchange System, EU CSW-CERTEX S15.

This interconnection is intended to enable the automated exchange of information with national customs systems S15.

The corresponding checks must notably make it possible to electronically and automatically verify the correspondence between certain identifiers provided upon importation and the information contained in the registry S15.

It is therefore established that the Digital Product Passport architecture is not designed as a necessarily isolated system: the regulation already provides for its interconnection with another European public digital infrastructure for certain customs purposes.

Limit at this stage

This interconnection with customs systems does not demonstrate the existence of an interconnection with electronic invoicing systems, approved platforms, banking infrastructures or payment systems.

It does, however, demonstrate that the technical and legal framework of the Digital Product Passport provides for structured identifiers, interoperability mechanisms and at least one automated interconnection with another public infrastructure.

The possible existence of other connections must therefore be investigated separately.

Interim conclusion

ESTABLISHED:

> The European Union is establishing a Digital Product Passport infrastructure that makes it possible to associate structured and interoperable data with uniquely identified products, with a level of granularity that may, depending on the applicable rules, extend to the individual item S15.

ESTABLISHED:

> The regulation provides for a digital registry managed by the European Commission and explicitly organizes its interconnection with the European EU CSW-CERTEX infrastructure in order to enable automated exchanges of information with national customs systems S15.

TO BE ESTABLISHED:

> Are there other infrastructures, standards, identifiers, projects, partnerships or interoperability mechanisms that enable or prepare for the cross-referencing of Digital Product Passport data with invoicing, transaction or payment data?

3.2 Environmental data that may be associated with products

Status: ESTABLISHED

The Digital Product Passport is intended to make information relating to the characteristics, composition, durability and environmental impacts of the products concerned accessible S15-[S16].

The exact content of a passport is not identical for all products. Mandatory data depend on the product group and the requirements laid down by the applicable European acts S15.

Information relating to environmental impacts

According to the European Commission, a Digital Product Passport may notably provide, depending on the product and the applicable legislation, information relating to:

- carbon footprint;
- environmental footprint;
- durability;
- repairability;
- recyclability [S16].

The system can therefore directly associate information with a product that makes it possible to characterize certain environmental impacts or environmental performance.

The existence of data relating to a product's carbon footprint does not, however, mean that an individual carbon footprint is calculated for its purchaser.

At this stage, this is information associated with the product.

Composition, materials and substances

The information made accessible may also concern the materials and components used in the product [S16].

Information relating to hazardous substances or substances of concern may also be included depending on the applicable requirements S15-[S16].

The passport may therefore provide structured information describing not only the product commercially, but also certain characteristics of its material composition.

Durability, repair and use

The information that may be made accessible also includes elements relating to:

- the product's lifespan or durability;
- its repairability;
- repair instructions;
- the availability of spare parts;
- its use and maintenance [S16].

This information is notably intended to enable the various actors with the corresponding access rights to better understand the product's characteristics throughout its life cycle.

End of life, reuse and recycling

The Digital Product Passport may also provide information relating to:

- disassembly;
- reuse;
- recycling;
- management of the product at the end of its life [S16].

The DPP may therefore potentially provide information relating to the product beyond its initial placing on the market.

Environmental data associated with an identifiable product

The important point for the remainder of the analysis results from the combination of the elements established in Sections 3.1 and 3.2.

The European framework makes it possible to associate a Digital Product Passport with a uniquely identified product, with a level of granularity that may, depending on the applicable rules, extend to the individual item S15.

This passport may contain, depending on the product group concerned, information relating to carbon or environmental footprint, composition, durability, repairability and recyclability S15-[S16].

It is therefore established that the European infrastructure makes it possible to associate structured environmental characteristics with digitally identifiable products.

What this does not establish

These elements do not establish:

- that a carbon footprint is necessarily calculated for every product marketed in the European Union;
- that every individual item necessarily has an individual passport;
- that a product's carbon footprint is automatically linked to the identity of its purchaser;
- that an individual environmental history of purchases is created;
- that these data are transmitted to the tax administration;
- that they are currently cross-referenced with invoicing, transaction or payment data.

These different mechanisms must be investigated separately.

Interim conclusion

ESTABLISHED:

> The European Digital Product Passport framework makes it possible to associate structured environmental information with digitally identifiable products, which may notably concern their carbon or environmental footprint, composition, durability, repairability and recyclability S15-[S16].

ESTABLISHED:

> Depending on the requirements applicable to the product group concerned, the passport may be defined at the model, batch or individual item level S15.

TO BE ESTABLISHED:

> For which product categories will the carbon or environmental footprint actually be mandatory, according to which methodology, at what level of granularity, and in what form will the corresponding values be recorded in the Digital Product Passport?

TO BE ESTABLISHED:

> Is there a mechanism enabling the product identifier from the Digital Product Passport to be retained or transmitted in an electronic invoice, a commercial transaction or a payment system?

3.3 Identification and granularity of data

Status: ESTABLISHED / TECHNICALLY DEDUCIBLE

The Digital Product Passport and the standards used in electronic commercial exchanges have mechanisms enabling products to be identified in a structured manner.

The analysis of these mechanisms reveals a technical point of correspondence between the two infrastructures: the possible use of standardized product identifiers.

Unique identifiers for the Digital Product Passport

Regulation (EU) 2024/1781 provides that the Digital Product Passport is linked to a unique and persistent product identifier S15.

Depending on the requirements applicable to the product group concerned, the passport may be established at the model, batch or individual item level S15.

The regulation also provides for unique identifiers relating to the economic operators and facilities associated with the product S15.

These mechanisms are notably intended to enable the traceability of products and the actors concerned throughout the value chain.

The GTIN among the Digital Product Passport data

Annex III to Regulation (EU) 2024/1781 includes among the data that may be included in the Digital Product Passport the Global Trade Item Number, or GTIN, or an equivalent identifier for products or their parts S15.

The GTIN is a standardized identifier used in commercial supply chains to identify items.

The Digital Product Passport may therefore include, in addition to its own unique identifier, a standardized commercial product identifier S15.

Standardized identifiers also present in electronic commercial exchanges

Electronic invoicing standards also make it possible to associate a standardized identifier with the item appearing on an invoice line.

In the model used by Peppol BIS Billing, business term BT-157 corresponds to the item's standard identifier S17.

This identifier is associated with a registered identification scheme S17.

Peppol commercial flows also use this standardized product identification mechanism in other documents in the commercial chain, notably orders, where the GTIN is explicitly provided as an example of a standard item identifier S17.

There are therefore standardized mechanisms enabling a structured product identification to be retained throughout different stages of a commercial exchange.

A technical point of correspondence between the infrastructures

The preceding elements make it possible to identify an important technical correspondence.

On the one hand, the Digital Product Passport may contain a GTIN or an equivalent identifier for the product or its parts S15.

On the other hand, the standards used for electronic commercial exchanges make it possible to carry a standardized item identifier at invoice-line level and in other commercial documents S17.

TECHNICALLY DEDUCIBLE:

> When a product referenced in a Digital Product Passport and an item appearing in an electronic commercial document use the same standardized identifier, notably a GTIN, this identifier can technically constitute a key for cross-referencing the two sets of data.

Such cross-referencing does not necessarily require the two infrastructures to use the same database: the existence of a common identifier can enable a system with access to the necessary data to establish a correspondence between the records.

A level of granularity that must be distinguished

This technical possibility must, however, be interpreted with caution.

A GTIN generally identifies a commercial product reference and does not, by itself, demonstrate the identification of a specific physical item.

The DPP regulation specifically distinguishes several possible levels of granularity: model, batch or individual item S15.

Likewise, the presence of a standardized identifier in an invoice format does not mean that this identifier is necessarily provided in every electronic invoice.

The technical possibility of cross-referencing therefore depends notably on:

- the actual presence of a common identifier;
- the level of granularity of the passport;
- the level of granularity of the identifier present in the commercial document;
- the retention of this identifier throughout the different stages of the transaction.

Technically possible cross-referencing is not established cross-referencing

None of the sources examined at this stage establish that approved platforms, the Public Invoicing Portal or the tax administration actually cross-reference identifiers present in invoices with data contained in Digital Product Passports.

Nor is it established that a DPP identifier or GTIN is systematically transmitted to the tax administration as part of the French electronic invoicing reform.

The presence of compatible identifiers across several infrastructures therefore constitutes a technical possibility for cross-referencing, not evidence of its use.

Interim conclusion

ESTABLISHED:

> The Digital Product Passport is based on structured identifiers and may notably include a GTIN or an equivalent identifier for the product or its parts S15.

ESTABLISHED:

> Electronic invoicing standards make it possible to provide a standard item identifier at invoice-line level, and Peppol standards also use standardized product identifiers, notably the GTIN, in various commercial documents S17.

TECHNICALLY DEDUCIBLE:

> When the same standardized product identifier is present in a Digital Product Passport and an electronic commercial document, it can technically serve as a key for cross-referencing the environmental information associated with the product with the information describing the commercial transaction.

TO BE ESTABLISHED:

> Do public or private actors actually use, experiment with or plan to use this correspondence between product identifiers in order to link Digital Product Passport data with order, invoicing, transaction or payment data?

3.4 Environmental footprint and carbon footprint

Status: ESTABLISHED

The existence of environmental information associated with products is not based solely on qualitative descriptions such as repairability or recyclability.

The European Union also has methods for quantitatively calculating the environmental impacts associated with certain products and their life cycle S18.

A European Product Environmental Footprint method

The European Commission has developed the Product Environmental Footprint (PEF) method, designed to measure and communicate the potential environmental impacts of a product throughout its entire life cycle S18.

This method is based on a structured analysis that notably takes into account the materials composing the product, manufacturing processes, energy used, transport and end of life S18.

The methodology also provides that certain data used in the study must be specific to the product examined. The bill of materials must notably correspond to the product concerned, and the modelling of manufacturing processes must be based on company-specific data under the conditions provided for by the method S18.

Specific rules may be established for certain product categories through Product Environmental Footprint Category Rules, or PEFCR S18.

The environmental footprint may therefore result from a structured calculation based on physical and industrial characteristics relating to the product and its life cycle.

Carbon footprint is an environmental parameter provided for by the ESPR Regulation

Regulation (EU) 2024/1781 provides that the information requirements applicable to certain product groups may cover various environmental parameters, including carbon footprint and environmental footprint S15.

Depending on the acts applicable to the product groups concerned, this information may notably be made accessible through the Digital Product Passport S15.

The ESPR framework therefore establishes the legal possibility of associating quantitative information relating to the environmental or carbon footprint with a digitally identifiable product.

It does not, however, mean that a carbon footprint will be mandatory for every product marketed in the European Union.

The case of batteries provides a concrete regulatory application

Regulation (EU) 2023/1542 concerning batteries provides a concrete example of the implementation of a regulatory carbon footprint associated with a product S19.

For certain categories of batteries, a carbon footprint declaration is progressively required S19.

This footprint is expressed in kilograms of CO_2 equivalent per kWh of the total energy delivered by the battery over its expected service life S19.

The regulation also provides for the footprint to be differentiated across several stages of the life cycle S19.

The calculation notably takes into account:

- raw material acquisition and pre-processing;
- production;
- distribution;
- own electricity production where applicable;
- end of life S19.

The regulatory methodology is based on the “climate change” impact assessment method derived from the Product Environmental Footprint S19.

A value linked to the model and production site

For the batteries concerned, the regulation provides that the carbon footprint declaration must be specific to a battery model produced at a particular manufacturing plant S19.

Battery-specific activity data must be used for the calculation under the conditions provided for by the regulation S19.

The regulation also provides that a change in the bill of materials or in the energy mix used to produce a battery model results in a new calculation of its carbon footprint S19.

Environmental information may therefore reach a level of precision combining a product reference, certain characteristics of its manufacturing process and a specific production site.

From environmental calculation to digital product data

The elements established since the beginning of this chapter now make it possible to identify several complementary components.

The Digital Product Passport makes it possible to associate structured data with an identifiable product S15.

The information that may be associated with the product can include its carbon or environmental footprint S15-[S16].

European methods make it possible to calculate the environmental impacts of a product using data relating to its life cycle S18.

Finally, the Batteries Regulation already provides an example in which a quantitative carbon footprint is calculated as a regulatory requirement for certain categories of products S19.

It is therefore established that the European Union has both infrastructures enabling products to be digitally identified and methodologies enabling quantified environmental indicators to be associated with certain products.

An essential distinction from the footprint of a purchaser

The carbon footprint of a product and the carbon footprint of a person are two different concepts.

The texts examined establish the existence of environmental data relating to products.

They do not establish that these values are added together based on purchases made by a person in order to automatically create an individual carbon footprint.

Such a mechanism would notably require a system capable of establishing a link between the products purchased, their environmental information and a specific purchaser.

This question therefore depends directly on the interconnection possibilities examined in the previous section and in the following sections.

Interim conclusion

ESTABLISHED:

> The European Union has a structured methodology for calculating the environmental footprint of products over their life cycle S18.

ESTABLISHED:

> The ESPR framework provides that information relating to the carbon or environmental footprint may form part of the information requirements applicable to certain product groups S15.

ESTABLISHED:

> The European Batteries Regulation already provides a concrete example in which a quantitative carbon footprint is associated with certain categories of products according to a regulatory methodology that notably takes into account the battery model, the production site and different stages of its life cycle S19.

TECHNICALLY DEDUCIBLE:

> When a product can be identified in a transaction and quantitative environmental data can be retrieved from its identifier, the two pieces of information can technically be cross-referenced in order to associate the product's environmental characteristic with the corresponding transaction.

TO BE ESTABLISHED:

> Are there systems, projects or experiments that actually use this possibility to automatically cross-reference a product's environmental data with order, invoice, payment or purchaser identification data?

3.5 Access to and circulation of data

Status: ESTABLISHED / TO BE ESTABLISHED

The Digital Product Passport is not based on a simple static digital document associated with a product.

Its architecture provides for different actors, different levels of access, identification and authorization mechanisms, as well as interfaces enabling the automated exchange of information between systems S15-S20.

A decentralized system

The Digital Product Passport system is based on a decentralized architecture S20.

The European registry does not necessarily contain all the detailed information present in each passport.

The complete passport data remain under the responsibility of the economic operator concerned and may be hosted directly by that operator or by a Digital Product Passport service provider S15-S20.

The European registry notably serves an indexing function and retains the unique identifiers, registration data and certain metadata provided for by the regulation S15-S20.

This architecture therefore distinguishes the central European registry from the systems in which the detailed information associated with products is stored.

Several categories of actors may access the data

Regulation (EU) 2024/1781 provides that different categories of actors may access passport information free of charge and easily, according to the rights granted to them S15.

These actors notably include:

- customers;
- manufacturers;
- importers;

- distributors and dealers;
- professional repairers;
- independent operators;
- refurbishers;
- remanufacturers;
- recyclers;
- market surveillance authorities;
- customs authorities;
- certain civil society organizations and trade unions;
- other relevant actors according to the applicable rules S15.

Access is therefore not necessarily identical for all users.

The rights to consult, enter, modify or update certain information depend on the actor's role and the rules applicable to the product group concerned S15.

An API enabling integration with operators' computer systems

The implementing regulation relating to the registry provides for an API enabling the registration of Digital Product Passports and the receipt of information from the registry S20.

The Commission specifies that this API allows economic operators, where appropriate, to integrate registration operations into their existing digital systems S20.

When a passport is registered, the registry generates a unique registration identifier that can be automatically communicated to the actor concerned through the user interface or directly in the API response S20.

The registry is therefore not designed solely for human use through a web portal: its architecture also enables automated exchanges between computer systems.

Identification, authorization and delegation

Economic operators wishing to interact with the registry must undergo a verification process S20.

Other actors in the value chain that may perform certain operations in the registry are also subject to a verification mechanism S20.

The system provides for user identification and authorization mechanisms, as well as the possibility for certain verified actors to delegate access rights to users acting on their behalf S20.

The regulation notably provides for the use of electronic identification mechanisms under the applicable European framework for electronic identification S20.

Integration with other Union information systems is envisaged by the legislation

The implementing regulation explicitly provides for the case in which the Digital Product Passport registry is integrated with another Union information system that has an equivalent or identical identity verification process S20.

In such a situation, an economic operator or another actor in the value chain already registered in that other system does not have to undergo a new identity verification procedure in the DPP registry S20.

ESTABLISHED:

> The regulatory framework therefore explicitly provides for the possibility of integrating the DPP registry with other Union information systems that share compatible mechanisms for verifying actors S20.

This provision does not, however, establish that the registry is currently integrated with any particular tax, banking or payment system.

The identification of the systems concerned and the integrations actually implemented must be investigated separately.

Logging and versioning

The registry includes an operation logging system S20.

The creation, modification and deletion of registration data must be recorded, and the registry supports data versioning as well as timestamping of updates S20.

The implementing regulation also provides, where no other specific retention period is defined by Union law, for the automatic deletion of certain passport registration data ten years after their registration S20.

There is therefore a regulatory mechanism for tracing operations performed in the registry, as well as rules relating to the retention period of certain registration data.

A public portal complements the access mechanisms

The ESPR Regulation also provides for a public web portal enabling stakeholders to search for and compare certain data contained in Digital Product Passports S15.

The information accessible remains determined by the rights granted to the different categories of actors S15.

The existence of this portal shows that certain information within the system is intended to be accessible beyond economic operators or public authorities alone.

An important limitation concerning customers' personal data

The ESPR Regulation also contains an important safeguard for the analysis conducted in this repository.

Personal data relating to customers must not be stored in the Digital Product Passport without their explicit consent, in accordance with European data protection rules S15.

ESTABLISHED:

> The DPP is therefore not designed, under its current regulatory framework, as a database automatically containing the identity of every purchaser of a product S15.

This restriction does not prevent a product from being identified in another system, for example a commercial document, but such cross-referencing constitutes a separate operation that cannot be inferred solely from the existence of the DPP.

Interim conclusion

ESTABLISHED:

> The DPP system is based on a decentralized architecture in which detailed information may be hosted by economic operators or specialized service providers, while a European registry notably handles the registration and indexing of passports S15-S20.

ESTABLISHED:

> The registry has an API, identification and authorization mechanisms, a semantic repository, a logging system and mechanisms enabling automated exchanges with actors' computer systems S20.

ESTABLISHED:

> The implementing regulation explicitly envisages the integration of the registry with other Union information systems that have equivalent or identical identity verification mechanisms S20.

ESTABLISHED:

> Personal data relating to customers must not be stored in the Digital Product Passport without their explicit consent S15.

TO BE ESTABLISHED:

> With which other Union information systems is the DPP registry currently integrated, or is its integration planned, experimented with or under consideration?

TO BE ESTABLISHED:

> Which systems operated by economic operators, DPP service providers, commercial platforms, financial actors or other intermediaries use DPP APIs and identifiers together with order, invoicing or payment data?

3.6 Potential link with transaction data

Status: ESTABLISHED / TECHNICALLY DEDUCIBLE / TO BE ESTABLISHED

The previous sections established that the Digital Product Passport can associate structured environmental information with an identifiable product and that certain commercial standards also make it possible to identify products within documents describing a transaction S15-S17.

The question is now whether these two categories of data remain strictly separate or whether infrastructures, projects or experiments already provide for their cross-referencing.

DPP data are intended to circulate throughout the value chain

The Digital Product Passport is designed to support the circulation of product-related information between different actors in its value chain S15.

Its architecture is based on structured identifiers, interoperable formats and interfaces enabling automated exchanges between systems S15-S20.

This circulation does not mean that transaction or payment data are automatically recorded in the DPP.

It does, however, allow different systems to retrieve information associated with a product when they have the necessary identifiers and access rights.

European projects already combine traceability and proof of transaction

The European e-Origin project provides a concrete example in which information relating to a commercial transaction is exchanged between several categories of public and private actors S21.

The pilot notably brings together VAT administrations, marketplaces, online sellers, customs brokers and customs authorities S21.

The infrastructure notably enables sellers and marketplaces to store and share proof of a commercial transaction and allows customs authorities to recognize this proof in order to facilitate certain customs clearance operations S21.

The project also provides mechanisms enabling information to be shared securely while maintaining control over sensitive and confidential data S21.

It is therefore established that European work is already underway on infrastructures enabling several categories of economic and administrative actors to exchange digital proofs relating to commercial transactions.

The Digital Product Passport appears within the same traceability trajectory

European documentation relating to e-Origin also indicates that the EBSI-ELSA project aims to develop traceability capabilities using the Digital Product Passport S21.

ESTABLISHED:

> The same European development environment therefore brings together work relating to digital proof of commercial transactions, actors responsible for VAT and customs, as well as the development of traceability capabilities based on the Digital Product Passport S21.

This element constitutes a more concrete documentary connection than merely comparing two technical architectures.

It does not, however, establish that environmental data contained in a DPP are currently linked to the tax data of a transaction or transmitted to an administration responsible for VAT.

Cross-referencing may also rely on the product identifier

As established in Section 3.3, the DPP may include a GTIN or an equivalent identifier S15.

Electronic commercial standards also make it possible to carry standardized item identifiers in different documents throughout the commercial chain S17.

TECHNICALLY DEDUCIBLE:

> When a proof of transaction or commercial document contains an identifier that makes it possible to retrieve the corresponding product in a DPP system, it becomes technically possible to associate the information describing the transaction with the environmental information accessible for that product.

This operation can be performed without information relating to the purchaser necessarily being recorded in the Digital Product Passport itself.

A system that separately has access to the identity of a party to the transaction and the product identifier can technically cross-reference the two sets of data.

Use of the DPP beyond the initial placing on the market is already being experimented with

European projects are already using the DPP as a traceability tool throughout the product life cycle S40.

The European CE-RISE project notably develops and experiments with the use of the DPP to enable material traceability and assess opportunities for product reuse, repair, refurbishment and recycling S40.

The European QUASAR project provides another concrete example: the DPP is used to help track photovoltaic panels at the end of their life and direct them towards reuse, repair or recycling operations, while second-life solutions are also being experimented with S41.

These examples establish that the use of the DPP is being experimented with beyond the initial placing on the market and may support different stages of a product's life cycle.

They do not, however, demonstrate that events associated with the product life cycle systematically constitute commercial transactions, that these transactions are centralized by a tax administration, or that they are linked to the permanent identity of their users.

An important boundary: transaction, payment and identity are not equivalent

Transaction data can establish that a commercial exchange took place.

Payment data describe the corresponding financial settlement.

Identity data make it possible to identify a natural or legal person.

Finally, the DPP makes it possible to identify and document the product.

These four categories of information must be distinguished.

The technical possibility of cross-referencing them does not mean that they are currently brought together in a single database, nor that any particular actor necessarily has access to all of this information.

What is now established

The elements examined nevertheless make it possible to move beyond the hypothesis that the DPP is necessarily isolated from the infrastructures used for commercial exchanges.

The DPP is based on identifiers and interoperability mechanisms S15-S20.

Commercial standards also allow the use of structured product identifiers S17.

Finally, European work already brings together, within the same development environment, digital proof of commercial transactions, administrative actors responsible notably for VAT and customs, secure data sharing and the development of traceability capabilities using the DPP S21.

Interim conclusion

ESTABLISHED:

> European projects are developing infrastructures enabling digital proofs of commercial transactions to be stored and shared between sellers, marketplaces and public authorities S21.

ESTABLISHED:

> The e-Origin project notably brings together actors responsible for VAT and customs, while the developments associated with EBSI-ELSA provide for the use of the Digital Product Passport to strengthen traceability capabilities S21.

TECHNICALLY DEDUCIBLE:

> When a transaction system and a DPP system have a common identifier enabling them to identify the same product, the economic data of the transaction can technically be cross-referenced with the environmental data associated with that product.

TO BE ESTABLISHED:

> Is there currently a system in which environmental data contained in or referenced by a Digital Product Passport are actually associated with an electronic invoice, a tax declaration or payment data?

TO BE ESTABLISHED:

> Do European projects ultimately provide for direct interoperability between DPP infrastructures, electronic invoicing systems, tax systems or payment infrastructures?

3.7 What is technically deducible

Status: TECHNICALLY DEDUCIBLE

The previous sections separately established several characteristics of the Digital Product Passport and the digital infrastructures used in commercial exchanges.

It is now possible to examine what their combination makes technically possible, without confusing this possibility with the actual existence of processing or interconnection.

Associating environmental data with an identifiable product

The Digital Product Passport is based on a unique and persistent identifier and may, depending on the applicable requirements, be defined at the model, batch or individual item level S15.

It may contain or provide access to structured environmental information relating to the product, notably its carbon or environmental footprint where the applicable rules provide for it S15-[S16].

European methodologies also make it possible to quantitatively calculate certain environmental impacts of products S18, and the Batteries Regulation already provides a concrete example of a regulatory carbon footprint associated with certain categories of products S19.

TECHNICALLY DEDUCIBLE:

> A system that has a product identifier and access to the corresponding data can technically retrieve the environmental characteristics associated with that product.

Associating a product with a commercial transaction

The standards used in electronic commercial exchanges make it possible to carry structured product identifiers in different commercial documents S17.

The DPP may also include standardized commercial identifiers, notably a GTIN or an equivalent identifier S15.

When the same identifier or a matching mechanism makes it possible to identify the product in both systems, it can constitute a key for cross-referencing.

TECHNICALLY DEDUCIBLE:

> A system that has a product identifier present in a commercial document can technically retrieve information corresponding to the same product in a DPP infrastructure.

This possibility does not mean that this identifier is necessarily provided in every invoice or transmitted to the tax administration.

Associating an environmental characteristic with a transaction

The combination of the two previous mechanisms makes it possible to identify an additional possibility.

If a product present in a transaction can be identified and environmental information can be retrieved from that identifier, a system with access to the necessary data and access rights can technically associate the product's environmental characteristic with the corresponding transaction.

The cross-referencing can be represented in simplified form as follows:

```
Commercial transaction
   ↓
Product identifier
   ↓
Match with the product
   ↓
Digital Product Passport
   ↓
Environmental data
```

TECHNICALLY DEDUCIBLE:

> Associating product environmental data with a commercial transaction does not necessarily require the environmental data to be directly recorded in the invoice: a common identifier or a matching table can make it possible to retrieve this information from a separate system.

The purchaser's identity constitutes an additional step

The ESPR Regulation provides that personal data relating to customers must not be stored in the Digital Product Passport without their explicit consent S15.

The DPP therefore does not, under its current framework, constitute a database that automatically assigns each product to its purchaser.

This does not, however, prevent another system from separately holding information relating to the parties involved in a transaction.

TECHNICALLY DEDUCIBLE:

> If a separate system has both information enabling a party to a transaction to be identified and the identifier of the product concerned, the identity does not need to be stored in the DPP for a technical correspondence between the transaction and the product information to be established.

This technical possibility demonstrates neither the existence nor the legality of such processing.

From successive transactions to a set of environmental information

When a system contains multiple transactions to which identifiable products can be associated, the same cross-referencing mechanism can technically be repeated.

It then becomes possible, from a purely technical perspective, to associate the corresponding environmental characteristics of the products concerned with multiple transactions.

If these characteristics include compatible quantitative values, statistical or aggregation operations can technically be performed on those values.

TECHNICALLY DEDUCIBLE:

> From a set of transactions involving identifiable products and quantitative environmental data accessible for those products, a system with the necessary information and access rights can technically calculate environmental aggregates corresponding to that set of transactions.

This deduction is important but must be strictly limited to its technical scope.

It does not demonstrate that an individual carbon footprint of purchases is currently calculated, that a public actor has access to all the necessary data, that such processing has a legal basis, or that a system for restricting purchases exists.

The infrastructures are designed to enable automated exchanges

The DPP uses structured, machine-readable data that can be transferred within an interoperable environment S15.

Its registry and architecture also enable automated exchanges between systems S20.

An automated interconnection with customs systems is explicitly provided for by the ESPR Regulation S15.

European projects such as e-Origin are also working on the circulation of proofs of commercial transactions between economic actors and administrations, while associated developments provide for traceability capabilities using the DPP S21.

The possibility of cross-referencing described in this section is therefore not based on the assumption that all information would have to be manually brought together in a single database.

It is based on architectures using identifiers, structured data and interoperability mechanisms that enable separate systems to exchange or retrieve information.

A technically feasible chain, but not established as an existing system

The elements examined make it possible to represent the following technical chain:

```
Identity or business
   ↓
Transaction
   ↓
Identifiable product
   ↓
Product identifier
   ↓
DPP data
   ↓
Environmental characteristics
   ↓
Quantitative environmental value
   ↓
Potential aggregation
```

Each link in this chain corresponds to a technically feasible computer operation when the systems concerned have the necessary identifiers, data, access rights and interoperability mechanisms.

This representation does not mean that this entire chain currently exists within a single system or that it is implemented by an administration.

It only makes it possible to precisely identify the components and correspondences that would be necessary to carry out such processing.

What is still missing to move from possibility to established use

To establish the actual existence of a system automatically linking transactions and environmental data, it would notably be necessary to identify:

- an actor that actually has access to both categories of data or is authorized to query them;
- a concrete mechanism for matching identifiers;
- an infrastructure or processing operation performing this task;
- a defined purpose for this processing;
- a legal basis where required;
- technical, regulatory, contractual, experimental or institutional documents demonstrating its implementation or preparation.

The simultaneous existence of the technical components is therefore not sufficient to demonstrate the existence of the complete system.

Interim conclusion

TECHNICALLY DEDUCIBLE:

> The infrastructures and standards examined technically make it possible to use a product identifier as a point of correspondence between a commercial transaction and the environmental information associated with that product.

TECHNICALLY DEDUCIBLE:

> When multiple transactions involve identifiable products associated with quantitative environmental values, these values can technically be cross-referenced and aggregated by a system with access to the necessary data and access rights.

ESTABLISHED:

> Interoperability and automated exchange mechanisms form part of the DPP's regulatory architecture, and an interconnection with customs systems is explicitly provided for S15-S20.

ESTABLISHED:

> European work already brings together digital proof of commercial transactions, administrative actors responsible notably for VAT and customs, and the development of traceability capabilities using the Digital Product Passport S21.

TO BE ESTABLISHED:

> Is there an actor, processing operation, project or infrastructure that actually implements or prepares all or a substantial part of the chain enabling transactions to be automatically associated with their environmental characteristics?

TO BE ESTABLISHED:

> Is there a system enabling this information to be aggregated at the level of an identified business or person, and if so, for what purpose and on what legal basis?

3.8 Limitations and elements remaining to be established

Status: TO BE ESTABLISHED

The elements examined in this chapter establish the existence of a European infrastructure enabling structured digital data to be associated with identifiable products, as well as the existence of methods for quantifying certain environmental impacts of those products S15-S18-S19.

They also establish the existence of interoperability mechanisms, standardized identifiers and automated exchanges that technically enable different systems to retrieve or cross-reference certain information relating to the same product S15-S17-S20.

These elements do not, however, establish that all the technical possibilities identified are currently implemented in a system automatically linking product, transaction, purchaser and environmental data.

Products actually covered by the DPP

The ESPR Regulation establishes the general framework for the Digital Product Passport, but its concrete application depends on the requirements adopted for the different product categories S15.

The presence of a DPP, its level of granularity and the nature of the information it contains must therefore not be considered identical for all products marketed in the European Union.

TO BE ESTABLISHED:

> Which product categories will actually be subject to a Digital Product Passport, according to what timetable, with what mandatory data and at what level of granularity: model, batch or individual item?

Generalization of the carbon footprint

The European framework allows the carbon or environmental footprint to form part of the information associated with certain products S15-[S16].

European methodologies already make it possible to quantitatively calculate certain environmental impacts S18, and the Batteries Regulation provides a concrete example of regulatory application S19.

These elements do not, however, establish that a quantitative carbon footprint will be calculated and recorded for every product marketed in the European Union.

TO BE ESTABLISHED:

> For which product categories will a quantitative carbon or environmental footprint become mandatory, according to which methods and with what level of precision?

Presence of identifiers in transactions

The DPP may include standardized product identifiers, and the standards used in electronic commercial exchanges also make it possible to carry item identifiers S15-S17.

This compatibility constitutes a technical possibility for cross-referencing.

It does not, however, establish that a common identifier is actually present in every invoice, every transaction or every passport.

TO BE ESTABLISHED:

> In which situations is an identifier enabling a product's DPP to be retrieved directly or indirectly actually retained in an order, an electronic invoice, transaction data or another commercial document?

Transmission of identifiers to the tax administration

Chapter 1 established the nature of the regulatory data transmitted to the administration under the French electronic invoicing framework.

The elements examined do not establish that the DPP identifier, GTIN or another identifier enabling a product's Digital Product Passport to be automatically retrieved is systematically transmitted to the tax administration.

This distinction is essential: the presence of an identifier in an invoice format does not necessarily mean that this identifier forms part of the regulatory data actually extracted and transmitted to the administration.

TO BE ESTABLISHED:

> Is an identifier enabling an invoice line to be linked to a product with a DPP transmitted, retained or accessible in the systems used by approved platforms, the Public Invoicing Portal or the tax administration?

Actual interconnection with invoicing systems

DPP infrastructures have interoperability mechanisms and interfaces enabling automated exchanges S15-S20.

Commercial standards also allow the use of structured product identifiers S17.

These elements make cross-referencing technically possible under certain conditions, but none of the sources examined establish the existence of a general interconnection between the DPP system and the French electronic invoicing infrastructure.

TO BE ESTABLISHED:

> Is there a project, experiment, specification, partnership or infrastructure explicitly providing for data exchange between DPP systems and electronic invoicing systems?

Interconnection with payment systems

The elements examined in this chapter do not establish that DPP data are automatically transmitted to a bank, payment service provider or monetary infrastructure when a purchase is paid for.

Nor do they establish that environmental information associated with a product currently plays a role in the authorization, refusal or conditions of execution of a payment.

TO BE ESTABLISHED:

> Are there projects, partnerships, experiments or infrastructures that actually link DPP identifiers or environmental data with payment data or payment mechanisms?

This question will be examined more specifically in the chapter devoted to payments and the digital euro.

Identification of the purchaser

The ESPR Regulation provides that personal data relating to customers must not be stored in the Digital Product Passport without their explicit consent S15.

The DPP therefore does not, under its current regulatory framework, constitute a registry that automatically assigns each product to its purchaser.

An association with a person or business could technically be made by a separate system simultaneously holding information relating to the transaction and the product identifier.

TO BE ESTABLISHED:

> Are there processing operations in which the identity of a purchaser, the products purchased and the corresponding environmental data are actually cross-referenced automatically?

Environmental aggregation of transactions

Section 3.7 established that it is technically possible, under certain conditions, to associate environmental values with multiple transactions and then perform aggregation operations on those values.

This technical possibility does not demonstrate the existence of a system that automatically calculates a cumulative environmental footprint based on the purchases of a business or a person.

TO BE ESTABLISHED:

> Is there a public or private system that uses product identifiers and transaction data to automatically calculate cumulative environmental indicators corresponding to the purchases of a business or a person?

Use of these data for a decision or restriction

None of the sources examined in this chapter establish that environmental information associated with products is used to authorize, refuse, limit or condition a person's purchases.

The existence of quantified environmental data and the technical possibility of associating them with a transaction are not sufficient to demonstrate the existence of a decision-making or restriction mechanism.

Such a system would require additional components, notably a decision-making mechanism, an infrastructure capable of acting on the transaction or payment, as well as a legal framework permitting such use.

TO BE ESTABLISHED:

> Are there texts, projects, experiments or infrastructures providing for the use of environmental data associated with products or transactions in order to automatically trigger a decision, condition or restriction?

Common actors and interconnection projects

The research identified European projects already combining digital traceability, proofs of commercial transactions, economic actors and public authorities S21.

The presence of actors or infrastructures in several systems does not, however, constitute, in itself, evidence of data exchange between those systems.

Partnerships, consortia, public procurement contracts, experiments, standards and technical documentation must therefore continue to be examined in order to identify any concrete interconnections.

TO BE ESTABLISHED:

> Which actors participate simultaneously in invoicing, environmental traceability, payment or digital identity infrastructures, and what data exchanges between these infrastructures are actually planned or carried out?

Interim conclusion

The elements remaining to be established no longer concern only the existence of digital environmental data or the technical possibility of associating them with identifiable products.

These elements are now documented.

The central question becomes that of the **connections actually implemented between the infrastructures**: the presence and circulation of identifiers, access to data, actors holding several categories of information, cross-referencing processes and associated purposes.

ESTABLISHED:

> Products can be associated with structured and quantitative environmental data, standardized identifiers can be used across several digital systems, and the DPP architecture provides for interoperability and automated exchange mechanisms S15-S17-S18-S19-S20.

TECHNICALLY DEDUCIBLE:

> When the necessary identifiers, data and access rights are available, a product's environmental characteristics can technically be cross-referenced with information describing a transaction and, under certain conditions, aggregated across multiple transactions.

TO BE ESTABLISHED:

> It remains to be determined which cross-referencing operations are actually carried out or being prepared, by which actors, for what purposes, on what legal bases and with what possibilities for acting on transactions or payments.

3.9 What this chapter establishes

The analysis of the regulatory texts, technical infrastructures and institutional projects examined in this chapter now makes it possible to distinguish several levels of certainty concerning environmental data associated with products and the possibilities for cross-referencing them with commercial data.

What is established

ESTABLISHED:

> The European Union has established a legal framework for the Digital Product Passport, based on structured, machine-readable and interoperable data associated with digitally identifiable products S15.

ESTABLISHED:

> Depending on the requirements applicable to the product group concerned, the Digital Product Passport may be defined at the model, batch or individual item level S15.

ESTABLISHED:

> The information that may be associated with certain products notably includes data relating to their composition, durability, repairability, recyclability, as well as their carbon or environmental footprint S15-[S16].

ESTABLISHED:

> The European Union has methods for quantitatively calculating certain environmental impacts of products over their life cycle S18.

ESTABLISHED:

> The European Batteries Regulation already provides a concrete example in which a quantitative carbon footprint is associated, as a regulatory requirement, with certain categories of products according to a defined methodology S19.

ESTABLISHED:

> The DPP may include standardized commercial identifiers, notably a GTIN or an equivalent identifier, while the standards used in electronic commercial exchanges also make it possible to carry standardized identifiers at item level S15-S17.

ESTABLISHED:

> The DPP architecture provides for interoperability mechanisms, automated exchanges, an API, identification and authorization mechanisms, as well as a European registry of Digital Product Passports S15-S20.

ESTABLISHED:

> The regulatory framework already provides for an automated interconnection with customs systems and envisages the integration of the DPP registry with other Union information systems that have compatible mechanisms for verifying actors S15-S20.

ESTABLISHED:

> European work already brings together digital proof of commercial transactions, economic actors, administrations responsible notably for VAT and customs, and the development of traceability capabilities using the Digital Product Passport S21.

What is technically deducible

The preceding elements make it possible to identify several technically feasible operations without having to assume the existence of a single database containing all the information.

TECHNICALLY DEDUCIBLE:

> When the same standardized identifier makes it possible to identify a product in a commercial document and in the DPP environment, this identifier can technically serve as a key for cross-referencing information relating to the transaction with environmental information associated with the product.

TECHNICALLY DEDUCIBLE:

> Environmental data do not need to be directly recorded in an invoice in order to be associated with a transaction: a system that has the product identifier and the necessary access rights can technically retrieve these data from a separate system.

TECHNICALLY DEDUCIBLE:

> Likewise, the purchaser's identity does not need to be stored in the DPP for cross-referencing to be technically feasible if another system separately holds information enabling the party to the transaction and the product concerned to be identified.

TECHNICALLY DEDUCIBLE:

> When multiple transactions involve identifiable products to which quantitative environmental values can be associated, a system with the necessary information and access rights can technically cross-reference and then aggregate these values.

The theoretical technical chain can therefore be represented in simplified form as follows:

```
Purchaser or business
   ↓
Transaction
   ↓
Identifiable product
   ↓
Product identifier
   ↓
Digital Product Passport
   ↓
Environmental data
   ↓
Quantitative environmental value
   ↓
Potential aggregation
```

This representation describes a possible architecture, not a system whose complete existence has been established.

What is not established

The sources examined do not establish:

- that an individual Digital Product Passport will be created for every product marketed in the European Union;
- that a quantitative carbon footprint will be mandatory for all products;
- that a GTIN, DPP identifier or equivalent identifier will be systematically present in every electronic invoice;
- that this identifier will be systematically transmitted to the tax administration;
- that approved platforms or the tax administration currently query DPP systems using information present in invoices;
- that product environmental data are currently cross-referenced with French invoicing or e-reporting data;
- that a bank or payment system automatically receives environmental information associated with purchased products;
- that an individual carbon footprint of purchases is currently calculated by an administration using these infrastructures;
- that purchases can currently be authorized, refused or limited on the basis of these environmental data.

These claims would require additional evidence that is not present in the sources examined.

An important safeguard concerning the identity of purchasers

The ESPR Regulation provides that personal data relating to customers must not be stored in the Digital Product Passport without their explicit consent S15.

ESTABLISHED:

> Under its current regulatory framework, the DPP therefore does not automatically constitute a nominative registry of products owned or purchased by each person.

This safeguard must be preserved in the analysis.

It does not, however, answer the separate question of possible cross-referencing performed by another system that separately holds identity, transaction and product identification data.

Chapter overview

This chapter establishes the existence of several distinct components:

- structured digital identification of products;
- a level of granularity that may, depending on the applicable rules, extend to the individual item;
- environmental data that can be associated with products;
- methods for quantifying certain environmental impacts;
- standardized identifiers that can be used in commercial chains;
- interoperability and automated exchange mechanisms;
- a European registry of Digital Product Passports that became operational on July 20, 2026, accompanied by a test environment S42;
- connections provided for by regulation with certain public infrastructures, notably customs infrastructures;
- European projects already bringing together digital traceability and proof of commercial transactions.

Taken separately, none of these elements demonstrates the existence of a system capable of automatically tracking the environmental footprint of a person's purchases.

Taken together, however, they establish that several technical components necessary to enable cross-referencing between **product, transaction and environmental data** already exist or are provided for in the infrastructures examined.

Chapter conclusion:

> **It is established that the European Union is developing an infrastructure enabling structured and, in certain cases, quantitative environmental data to be associated with digitally identifiable products. It is also established that this infrastructure is designed to be interoperable with other digital systems and that European projects are already working on environments combining traceability and proofs of commercial transactions S15-S20-S21.**

> **It is technically deducible that a common identifier or matching mechanism could make it possible to associate a transaction with the environmental data of the product concerned and, when multiple transactions are available, to aggregate the corresponding values.**

> **It is not established, however, at this stage, that such a mechanism is used by the tax administration to establish an environmental footprint of the purchases of a business or a person, nor that it is linked to a system capable of conditioning or restricting a payment.**

Chapter 4 — Digital Euro and Payment Infrastructures

Navigation: ← Back to the table of contents

This chapter examines the proposed architecture for the digital euro, the actors involved in its operation, the data necessary for the execution of payments, as well as the technical mechanisms enabling certain operations to be automated.

The objective is notably to determine what the digital euro infrastructure would technically enable, what data could be processed by the different actors, and what safeguards are provided concerning the programmability of money, data protection and the possibilities for conditioning payments.

An essential distinction must be made between:

- the programmability of the money itself;
- conditional payments;
- the automation of payment execution;
- the data used to verify a condition;
- the identification of the payer or beneficiary;
- the potential use of information originating from other digital systems.

The existence of a mechanism enabling a payment to be automatically triggered when a condition is met does not mean that the money itself is programmable.

Table of contents

4.1 General architecture of the digital euro

Status: ESTABLISHED / ONGOING PROJECT

The digital euro is a central bank digital currency project intended to complement cash and other existing means of payment in the euro area S22-S23.

It is not a crypto-asset or a currency issued by a private institution. Digital euro units would constitute a direct claim on the Eurosystem S23.

As of the date of the sources examined, the digital euro has not yet been issued. The project continues its technical development and remains dependent on the adoption of the corresponding European legislative

framework S23.

A central settlement infrastructure

The technical architecture currently envisaged is based on a centralized settlement platform operated by the Eurosystem S23.

The Eurosystem would process and verify settlements as well as digital euro holdings recorded within the infrastructure S23.

The ECB specifies that this architecture does not rely on blockchain or distributed ledger technology as the system's fundamental infrastructure S23.

It nevertheless incorporates certain technical principles used in distributed systems, notably to improve resilience and performance.

ESTABLISHED:

> The architecture currently envisaged for the digital euro is based on a central settlement infrastructure controlled by the Eurosystem S23.

Distribution through intermediaries

The existence of a central infrastructure does not mean that users would directly hold an account with the ECB for their day-to-day transactions.

The proposed regulation provides that digital euro payment services would be distributed through payment service providers S22.

These intermediaries would notably enable:

- access to and use of the digital euro;
- initiation and receipt of payments;
- provision of the instruments enabling these payments to be made;
- management of digital euro payment accounts;
- operations enabling the corresponding holdings to be funded or defunded S22.

The ECB also indicates that a user could access the digital euro through an account set up with their bank or a public intermediary S23.

The architecture therefore distinguishes at least two levels:

```
User
   ↓
Payment service provider
   ↓
Eurosystem infrastructure
   ↓
Settlement in digital euros
```

This separation between the relationship with the user and central settlement will become important in determining which data are accessible to the different actors.

Money recorded on the Eurosystem's balance sheet

Digital euros held by users would constitute direct liabilities of the Eurosystem S23.

This characteristic distinguishes the digital euro from commercial bank money usually held in a bank account.

The payment service provider would therefore manage the relationship with the user and provide the service, while the corresponding monetary value would remain a claim on the central bank.

ESTABLISHED:

> Intermediation by a bank or payment service provider does not transform the digital euro into private bank money: the corresponding holdings would remain a direct claim on the Eurosystem S23.

An infrastructure designed to operate at scale

The ECB envisages an architecture distributed across several geographical regions, each with multiple servers, in order to ensure service continuity and infrastructure resilience S23.

The objective is notably to enable the system to continue operating in the event of a failure affecting part of the infrastructure.

The digital euro is therefore envisaged as a European retail payment infrastructure intended to operate at scale, rather than as an experiment limited to a small number of actors.

Online and offline payments

The architecture provides for two main modes of use:

- online payments;
- offline payments S23.

The possibility of making offline payments is an important feature of the project.

In this situation, the ECB indicates that the transaction details would be known only to the payer and the beneficiary, in order to provide a level of privacy close to that of cash.

Online payments, by contrast, use the payment infrastructure and involve the intermediaries necessary for their execution.

The distinction between these two modes must therefore be preserved when examining the data accessible to the different actors.

A centralized architecture does not mean that the ECB directly knows users' identities

Centralized settlement does not mean that the ECB would automatically have access to the civil identity of the users corresponding to each transaction.

The ECB indicates that the information made available to the Eurosystem would be pseudonymized and that it should not be able to directly identify the user from the payment data it receives S23.

The intermediaries managing the relationship with the user would, however, have access to the information necessary to comply with their legal obligations.

This distinction will be examined more specifically in the section devoted to payment data.

An architecture still under development

The digital euro is not currently a currency in circulation S23.

The ECB is continuing the technical development of the system and indicates that it aims to be prepared for a potential first issuance in 2029, subject notably to the adoption of the European legislative framework S23.

The technical specifications therefore continue to evolve.

The elements examined in this chapter should be understood as describing the architecture currently proposed or being prepared, rather than the definitive operation of a system already deployed.

Interim conclusion

ESTABLISHED:

> The digital euro is designed as central bank money whose holdings would constitute a direct claim on the Eurosystem S22-S23.

ESTABLISHED:

> The architecture currently envisaged is based on a centralized settlement platform controlled by the Eurosystem, while distribution and the relationship with users are handled through payment service providers S22-S23.

ESTABLISHED:

> The infrastructure provides for online and offline payments, as well as specific technical mechanisms intended to ensure its resilience S23.

ESTABLISHED:

> The ECB indicates that the Eurosystem should not be able to directly identify users from the payment data to which it would have access, while intermediaries would retain the information necessary to comply with their legal obligations S23.

TO BE ESTABLISHED:

> What exact data circulate between the user, their payment service provider and the central infrastructure during the different types of transactions?

TO BE ESTABLISHED:

> Which technical components have access to the information required to initiate, verify, authorize, settle or potentially condition the execution of a payment?

4.2 Actors and payment infrastructures

Status: ESTABLISHED / ONGOING PROJECT

The architecture envisaged for the digital euro is not based on a single direct relationship between the user and the European Central Bank.

It involves several categories of actors performing distinct functions in access to the service, payment initiation, acceptance, control and settlement S22-S24.

This distribution of functions is important in determining what information is accessible to each actor and at what point in a transaction.

The Eurosystem

The Eurosystem constitutes the central level of the infrastructure.

As established in the previous section, the architecture currently envisaged provides for a central platform enabling, notably, the processing and settlement of digital euro transactions S23.

The Eurosystem also defines the common rules and specifications necessary for the operation of the system.

The digital euro rulebook notably describes:

- the actors participating in the system;
- the different use cases;
- end-to-end payment flows;
- the interfaces between the different components;
- the technical requirements applicable to payment service providers;
- data management mechanisms;
- data exchanges;
- risk and fraud management mechanisms;
- transaction settlement S24.

ESTABLISHED:

> The Eurosystem is therefore not only the issuer of the currency: it also provides the central infrastructure and defines the common technical rules enabling the different actors in the system to interact S23-S24.

Payment service providers

The proposed regulation provides that the distribution of the digital euro is based on payment service providers S22.

Users establish a contractual relationship with these providers rather than directly with the European Central Bank S22.

Payment service providers may notably enable users:

- to access the digital euro;
- to initiate and receive payments;
- to use digital euro payment instruments;
- to manage their digital euro payment account;
- to perform the funding and defunding operations provided for by the system S22.

Payment service providers therefore constitute an intermediary layer between the user and the central infrastructure.

The payer's payment service provider

In a transaction, the provider managing the relationship with the payer is involved in the initiation and processing of the payment S24.

It notably constitutes the point of contact between the user, their payment instrument and the services necessary for the execution of the transaction.

The system's technical documentation explicitly distinguishes the functions and requirements applicable to providers distributing the digital euro S24.

These providers must notably interact with the central services necessary for access to the system, liquidity management and transaction processing.

They also remain subject to the legal obligations applicable to payment service providers.

This position is important for the analysis of data: unlike the Eurosystem, which is intended to receive pseudonymized information in certain situations, the provider managing the relationship with the user has access to the information necessary to provide the service and comply with its regulatory obligations.

The beneficiary's payment service provider

A commercial transaction may also involve a provider on the beneficiary's side of the payment.

The rulebook thus distinguishes providers distributing the digital euro from providers performing the acquiring functions necessary for payment acceptance S24.

In a commercial transaction, the acquiring provider notably enables interaction between the merchant's acceptance device and the infrastructure necessary for processing the payment.

The architecture can therefore be represented in simplified form as follows:

```
Payer
   ↓
Payer's PSP
   ↓
Digital euro infrastructure
   ↓
Beneficiary's PSP / acquirer
   ↓
Merchant or beneficiary
```

This diagram is intentionally simplified: the technical flows may involve several additional common services.

Acceptance devices

The infrastructure is not limited to banks and the Eurosystem.

The rulebook also provides specifications relating to devices enabling digital euro payments to be accepted S24.

These devices may notably be involved in payments made to a merchant.

They constitute the technical point at which the information necessary for the transaction is presented, exchanged or captured before being transmitted to the other components of the system.

The acceptance device must therefore be distinguished from the central settlement system: it operates close to the commercial transaction, while monetary settlement is carried out in another layer of the infrastructure.

Common services between the different actors

The rulebook also provides for a category of common services that can be used by different participants in the system S24.

The technical specifications published by the ECB notably cover:

- access management;
- alias lookup and resolution;
- liquidity management;
- payment processing;
- risk and fraud management;
- data exchanges;
- transaction settlement S24.

The existence of these services shows that the execution of a payment does not simply correspond to a direct transfer between two wallets.

It involves several technical functions that may operate successively or simultaneously in the processing of a transaction.

Risk control, fraud prevention and compliance with legal obligations

Payment service providers remain responsible for the controls imposed on them by the applicable regulations.

The project's technical documentation notably provides for mechanisms relating to risk and fraud management S24.

The versions of the rulebook preparing the architecture also indicate that the payer's payment service provider must carry out, before the final execution of a transaction, the legally required controls relating to fraud, anti-money laundering and counter-terrorist financing, as well as, where applicable, controls relating to sanctions and embargoes.

The provider remains responsible for the execution or non-execution of the transaction in accordance with the applicable legal framework.

ESTABLISHED:

> The execution of a digital euro payment is therefore not designed as a technically blind operation: regulatory controls and risk and fraud management mechanisms are involved in the processing of transactions S24.

These controls correspond to existing legal obligations and do not, in themselves, constitute a general ability to condition payments according to any criterion.

Several actors may therefore be involved in the same transaction

The architecture makes it possible to distinguish several functions:

```
User
   ↓
Payment instrument or interface
   ↓
Distributing PSP / payer's PSP
   ↓
Common services
   ↓
Central infrastructure
   ↓
Acquiring PSP / beneficiary's PSP
   ↓
Acceptance device
   ↓
Beneficiary
```

Not all of these actors or components necessarily have access to the same information.

Knowledge of the payer's identity, the beneficiary's identity, the amount, the instrument used, the commercial context or the technical information necessary for settlement may be distributed across several components.

It is therefore necessary to distinguish the overall existence of information within the payment chain from its actual accessibility by a specific actor.

An essential distinction between knowledge and capacity to act

The presence of an actor in the processing of a transaction does not automatically mean that it has access to all the data relating to that transaction.

Conversely, an actor does not necessarily need to know the entire commercial context in order to perform a technical operation such as authentication, control, authorization or settlement.

This distinction will be particularly important when examining conditional payments.

A system may receive the result of an external verification without necessarily receiving all the data used to produce that result.

An architecture of this type can be represented as follows:

```
External system
   ↓
Result of a condition
   ↓
Payment component
   ↓
Execution or non-execution
```

This representation describes only a principle of computer architecture. It does not mean that an external system using environmental, tax or individual data is currently connected to the digital euro.

Interim conclusion

ESTABLISHED:

> The architecture envisaged for the digital euro distributes functions among several categories of actors and components, notably the Eurosystem, payment service providers, providers operating on the payer's or beneficiary's side, acceptance devices and various common services S22-S24.

ESTABLISHED:

> The rulebook provides distinct technical specifications concerning, notably, end-to-end flows, distributing and acquiring providers, acceptance devices, data management, data exchanges, risk and fraud, as well as settlement S24.

ESTABLISHED:

> Regulatory controls and risk and fraud management mechanisms may intervene before the final execution of a transaction, in accordance with the obligations applicable to payment service providers S24.

TECHNICALLY DEDUCIBLE:

> The distribution of functions among several components makes it possible for a decision or verification necessary for processing a payment to be produced in a separate system and then communicated to the component responsible for continuing or not continuing the operation, without that component necessarily having access to all the data used to produce that decision.

TO BE ESTABLISHED:

> What exact data are accessible to each of the actors involved in a digital euro transaction, and which data are exchanged between their different systems?

TO BE ESTABLISHED:

> Which services technically have the ability to block, suspend, defer or trigger a transaction, in what situations and according to what rules?

TO BE ESTABLISHED:

> Can information originating from systems external to the payment system be used by certain components of this architecture to determine whether an operation is executed, and if so, in which cases?

4.3 Data processed during payments

Status: ESTABLISHED / ONGOING PROJECT

The technical documentation published for the digital euro project makes it possible to go beyond a general description of the architecture and examine the categories of data provided for its operation S24-S25.

Rulebook v0.91 notably includes a data model, a data dictionary and specifications dedicated to data exchanges between the different components of the system S25.

These documents remain provisional and non-binding specifications. They nevertheless describe in detail the information currently provided for in the design of the system.

A structured model of users, accounts, devices and transactions

The data model distinguishes several categories of entities necessary for the operation of the digital euro S25.

It notably includes:

- users;
- business users;
- digital euro payment accounts;
- certain non-digital-euro payment accounts linked to the system;
- payment service providers;
- devices used;
- aliases;
- merchant interaction points;
- transactions;
- payers;
- beneficiaries;
- dispute-related data;
- risk and fraud data S25.

The document specifies that this model represents the entities, their essential attributes and the relationships between them.

It should not, however, be interpreted as a complete representation of all the databases in the system or as indicating that each actor retains all of this information.

ESTABLISHED:

> The current design of the digital euro is based on a structured data model linking, notably, users, accounts, devices, payment service providers and transactions S25.

Identifiers specific to users and accounts

The model provides for a unique digital euro user identifier as well as an identifier for the digital euro payment account, notably referred to as DEAN in the specifications S25.

It also provides for pseudonymous aliases.

The rulebook defines an alias as a pseudonymous identifier intended to protect the user's identity during payment processing. According to the specification, this alias can only be linked to an identifiable natural or

legal person by the payment service provider distributing the digital euro or by the user concerned S25.

The alias is intended to serve as a primary identifier that can be shared in certain transactions.

ESTABLISHED:

> The architecture therefore distinguishes between the identity known to the payment service provider and the pseudonymous identifier that may circulate in certain transaction processing operations S25.

This separation constitutes an important identity protection measure but does not mean that the user is anonymous to their payment service provider.

Detailed data describing the transaction

The model defines a transaction as the representation of a financial exchange between actors.

The examples mentioned notably include funding and defunding operations, recurring payments, reservations, payments, purchases, withdrawals and other operations S25.

The information provided for notably includes:

- a transaction identifier;
- an end-to-end transaction identifier known to the relevant providers;
- the transaction amount;
- the date and time of creation;
- the transaction direction;
- the currency;
- additional information that may be provided by the user during initiation;
- the transaction type;
- the initiation method;
- the transaction status;
- the environment in which it takes place S25.

The types and environments provided for notably make it possible to distinguish purchases, refunds, reservations, account-to-account payments, P2P transactions, e-commerce, mobile commerce, recurring payments or standing orders S25.

ESTABLISHED:

> A digital euro transaction is therefore not represented solely by a transferred amount: the technical model provides for several attributes enabling it to be identified, dated, categorized and tracked throughout its processing cycle S25.

Identification of the payer and beneficiary

The model provides for separate entities for the payer and the beneficiary S25.

The payer may be a natural person, a business, an administration or another public authority.

The beneficiary may also belong to these different categories.

The specifications provide for unique identifiers for the payer and the beneficiary within the data model S25.

This does not mean that their full civil identity is communicated to all components of the system.

As indicated previously, the architecture notably provides for the use of pseudonymous aliases and a distribution of information between providers and the central infrastructure.

ESTABLISHED:

> The data model technically makes it possible to distinguish and identify the parties participating in a transaction, while providing mechanisms intended to limit the circulation of their directly identifiable identity S25.

The devices used can also be represented

The model provides for information relating to the devices used to interact with the system S25.

A device may notably correspond to an application, a card or browser access.

The attributes provided for notably include:

- a device identifier;
- its type;
- its IP address where applicable S25.

This information may notably be involved in technical, security or risk management processes.

Its presence in the model does not necessarily mean that it is transmitted to all actors participating in the settlement of a transaction.

The commercial context can be categorized

The documentation also provides for data relating to the merchant and its activity S25.

It notably uses the **Merchant Category Code**, or MCC, based on the ISO 18245 classification.

This code makes it possible to classify a merchant according to the type of goods or services corresponding to its activity, for example transportation, retail or vehicle rental S25.

The model also provides for a merchant identifier as well as the identifier of its digital euro payment account.

ESTABLISHED:

> The currently documented architecture therefore makes it possible, in certain flows, to know not only the amount and the parties to a transaction but also a category corresponding to the beneficiary's commercial activity S25.

This data does not, however, describe the individual product purchased.

A Merchant Category Code classifies the merchant's activity; it does not constitute a GTIN, a DPP identifier or an item identifier.

This distinction is essential to avoid confusing **merchant category** with **detailed basket contents**.

The Merchant Category Code circulates in the payment request

The documentation goes further regarding the MCC.

It indicates that, among the information relating to the merchant's type of activity, **only the Merchant Category Code is transmitted in the payment request to the Digital Euro Service Platform (DESP) and to the distributing payment service provider**, and that it is transmitted in encrypted form S25.

ESTABLISHED:

> In the currently documented architecture, information categorizing the merchant's activity is therefore among the data that may circulate within the technical chain of a payment request S25.

The encryption of this information must be taken into account: its presence in a message does not mean that every intermediary component can necessarily read or use it.

It will therefore be necessary, for each processing operation, to distinguish the technical circulation of data from the actual ability of a specific actor to decrypt and use it.

Information relating to the point of interaction and its location

The model also describes the point of interaction, or POI, where a transaction may be carried out S25.

This may correspond to a physical location, such as a payment terminal in a store, or to a virtual location, such as an online payment page or mobile application.

The information envisaged notably includes:

- a point of interaction identifier;
- its type;
- a legal entity identifier;
- a local business identifier, for example a SIRET in France;
- an online identifier such as a domain name or IP address;
- a physical address;
- a city;
- a postal code;
- a country S25.

The documentation specifies, however, that several of these pieces of information must be managed **internally by the acquiring PSP**, notably for traceability, auditing, management of acceptance capabilities and, for certain data, management of pre-disputes or disputes S25.

ESTABLISHED:

> Information making it possible to characterize or locate a commercial point of interaction exists in the model, but the documentation provides that several of these pieces of information remain managed at the acquiring PSP level rather than necessarily being transmitted throughout the entire infrastructure S25.

Link with a non-digital-euro bank account

The model also provides for the possibility of linking a digital euro payment account to a non-digital-euro payment account S25.

For the latter, the documentation notably mentions:

- the IBAN;
- opening and closing dates;
- the balance;
- the date corresponding to the balance S25.

This relationship is notably involved in the mechanisms enabling digital euro holdings to be funded or defunded.

ESTABLISHED:

> The architecture therefore provides for a possible technical link between a user's digital euro account and a conventional bank payment account used notably for funding or defunding operations S25.

This link does not mean that the Eurosystem has unrestricted access to all the data from the traditional bank account: the distribution of data between the PSP and the DESP remains decisive.

Risk and fraud data

The payment model also includes data relating to risk and fraud assessment S25.

It notably provides for an entity corresponding to a **fraud and risk score**, as well as a type used to classify this score.

This information must be considered within the fraud prevention and detection function provided for by the payment architecture.

ESTABLISHED:

> The architecture therefore provides for the use of structured scores or indicators intended for risk and fraud assessment in payment processing S25.

The presence of a risk or fraud score does not demonstrate the existence of a general social, environmental or behavioral score.

None of the sources examined at this stage establish that environmental data or an environmental profile are included in the calculation of these scores.

Data that may be used for reports, queries and analyses

The data exchange service specifications provide for the DESP to make various reports and query mechanisms available to participants S25.

The documentation explicitly indicates that these functions are intended to meet the **operational, analytical and statistical** needs of participants.

The reports and queries provided for notably concern:

- transactions;
- accounts;
- certain reference data;
- disputes;
- the calculation of certain fees;
- risk and fraud management S25.

Some reports may be detailed, others aggregated, and access to them depends on the role of the provider concerned.

The documentation provides, for example, detailed transaction reports for eligible PSPs as well as a periodic aggregated report relating to the fraud risk situation S25.

ESTABLISHED:

> The infrastructure therefore provides not only for the immediate transactional processing of data but also for structured mechanisms enabling certain authorized participants to obtain reports and perform queries for operational, analytical or statistical purposes S25.

This capability remains governed by the roles and access rights defined within the system.

The model distinguishes the existence of data from its actual accessibility

One methodological point is essential.

The data model describes the information necessary for the different processes but specifies that it does not represent the entirety of an information system and does not automatically determine the information already managed in existing systems S25.

Similarly, the data exchange service provides that the reports and queries accessible to a PSP depend on its role and the data for which it is eligible.

Three levels must therefore be distinguished:

```
Data provided for in the model
   ↓
Data actually transmitted in a specific flow
   ↓
Data actually accessible and usable by a specific actor
```

These three levels must not be confused.

What the payment data do not yet establish

The elements examined make it possible to document a significant level of granularity in the information necessary for the operation of the system.

They do not, however, establish that the payment system systematically knows the individual product purchased.

At this stage, the data identified notably include the amount, date and time, parties, necessary accounts or aliases, transaction type and environment, certain technical elements, as well as the merchant's activity category.

None of the sources examined in this section establish that the payment request systematically contains:

- the GTIN of the product purchased;
- the identifier of its Digital Product Passport;
- its detailed description;
- its carbon footprint;
- the different line items making up the basket;
- the detailed tax data from an electronic invoice.

TO BE ESTABLISHED:

> Can data originating from the commercial system, an electronic invoice, a DPP or another external system be associated with the transaction identifier or used by another layer of the infrastructure without being directly contained in the payment message?

Interim conclusion

ESTABLISHED:

> The technical model currently published for the digital euro provides for structured data relating to users, accounts, devices, providers, payers, beneficiaries and transactions S25.

ESTABLISHED:

> Transactions have identifiers, including an end-to-end identifier, and notably include information relating to the amount, date and time, type, environment and status of the operation S25.

ESTABLISHED:

> The architecture provides for pseudonymous identifiers that limit the circulation of the user's directly identifiable identity, while their payment service provider retains the ability to link certain information to its customer S25.

ESTABLISHED:

> The Merchant Category Code makes it possible to categorize the beneficiary's commercial activity, and the documentation provides for its encrypted transmission in the payment request to the DESP and the distributing PSP S25.

ESTABLISHED:

> The model also includes information relating to points of interaction, certain location elements, devices and risk and fraud scores, with their management distributed among the different actors S25.

ESTABLISHED:

> The DESP provides for reports and query mechanisms intended for certain PSPs according to their rights and roles, notably for operational, analytical and statistical purposes S25.

NOT ESTABLISHED:

> The sources examined do not establish that the payment infrastructure systematically receives the precise identifier of the product purchased, its DPP, its GTIN, its environmental footprint or the complete details of the basket.

TO BE ESTABLISHED:

> What additional information can be associated with a transaction by PSPs, merchants or external systems through the transaction identifiers provided for in the architecture?

TO BE ESTABLISHED:

> What data are actually accessible to the DESP, distributing PSPs, acquiring PSPs and other technical services, in what form and for how long?

TO BE ESTABLISHED:

> In what situations can information describing the context of a transaction contribute to an automated decision concerning its processing?

4.4 Online and offline payments

Status: ESTABLISHED / ONGOING PROJECT

The architecture envisaged for the digital euro distinguishes two operating modes with different technical characteristics and levels of access to data:

- online payment;
- offline payment S23-S26.

This distinction is essential for the analysis of data processing possibilities.

An online payment uses the infrastructures and intermediaries necessary for its processing and settlement.

An offline payment, by contrast, is designed to enable the transfer of value without an Internet connection and without real-time intervention by the central infrastructure S26.

Online payment

In online operation, the different components examined in the previous sections are involved in processing the transaction.

Depending on the type of operation, this may notably involve:

- the payer's payment service provider;
- the beneficiary's payment service provider;
- the system's common services;
- the Digital Euro Service Platform;
- the Eurosystem's settlement infrastructure S24-S25.

The data necessary for processing the transaction may then circulate between different components according to the rules, roles and access rights provided for by the architecture.

As established in section 4.3, these data may notably include transaction identifiers, the amount, date and time, the type and environment of the operation, the pseudonymous identifiers necessary for processing, as well as certain information relating to the commercial context S25.

The ECB indicates, however, that the Eurosystem should not be able to directly identify the payer or beneficiary from the information received for online payments S23.

The link between the pseudonymized identifiers used within the infrastructure and the identity of users would remain known to their payment service providers in accordance with the applicable obligations S23.

ESTABLISHED:

> Online operation therefore involves a structured circulation of data necessary for payment, but the architecture provides for a separation between directly identifying information held by PSPs and pseudonymized information accessible to the Eurosystem S23-S25.

Offline payment

Offline operation is based on a different architecture.

The ECB provides that a payment can be made directly between the payer's and beneficiary's devices without an Internet connection at the time of the transaction S26.

In the technical work currently being conducted for the pilot, offline payments between individuals notably rely on proximity communication using NFC.

The value necessary for the payment is stored locally in a secure hardware environment on the device.

The ECB is notably examining the use of:

- embedded Secure Elements;
- eSIMs;
- other hardware components capable of protecting the values and cryptographic operations necessary for offline operation S26.

These components are intended notably to prevent the extraction of cryptographic keys, fraudulent modification of the balance or alteration of operations performed within the secure environment.

A direct transfer between devices

In offline mode, the transfer does not require the intervention of an online system at the time of payment S26.

The ECB describes the mechanism as a direct transfer of cryptographically secured values between two devices.

The operation can be represented simply as follows:

```
Payer's device
   ↓
Secure local communication
   ↓
Beneficiary's device
```

The central infrastructure therefore does not intervene in real time in the individual processing of this transaction.

ESTABLISHED:

> An offline digital euro payment is designed to be executed directly between the payer's and beneficiary's devices without transmitting the transaction to an online system at the time of payment S26.

Transaction details remain on the devices

The difference from online payment is particularly significant with regard to data.

The ECB indicates that, for offline payments, sensitive information relating to the transaction remains within the secure environment of the devices and is accessible neither to the Eurosystem nor to payment service providers S26.

The documentation notably specifies that information relating to:

- the goods purchased or the purpose of the payment;
- the location where the goods were purchased;
- the merchant from whom the purchase was made or the person who received the payment,

is not accessible to the ECB, banks or PSPs in the context of offline payment S26.

ESTABLISHED:

> Under the architecture currently announced, the personal details of an offline payment are designed to be known only to the payer and the beneficiary S23-S26.

This characteristic constitutes a major difference from the online operation examined previously.

A level of privacy comparable to cash

The ECB explicitly presents offline payment as being intended to offer a level of privacy comparable to that of cash S23-S26.

Offline operation prevents the Eurosystem from directly linking the transaction to a person.

But it goes further: unlike online payment, PSPs also do not receive the personal details of the transaction itself during or after its execution S26.

The difference can be summarized as follows:

Online payment

Transaction processed by the digital infrastructure:

- necessary data distributed among several components
- PSP able to identify its customer
- Eurosystem receiving information designed not to enable it to directly identify the user

Offline payment

Transaction executed locally between devices:

- personal details retained on the devices
- PSP not receiving the personal details of the transaction
- Eurosystem not receiving the personal details of the transaction

This distinction constitutes an important architectural safeguard in the analysis of payment tracking possibilities.

Funding and defunding operations remain distinct

The private nature of offline payment does not, however, mean that the user can obtain or convert digital euros offline without any interaction with their provider.

Operations enabling funds to be loaded into the offline functionality or converted back into other forms of money require the involvement of the payment service provider S26.

The ECB indicates that anti-money laundering controls are carried out by the PSP at the time of these funding and defunding operations, according to an approach comparable to the controls applicable to cash withdrawals and deposits S23-S26.

It is therefore necessary to distinguish:

Funding of funds → interaction with the PSP
Offline payment → local transfer between devices
Defunding of funds → interaction with the PSP

ESTABLISHED:

> The privacy of offline payment concerns the transaction carried out between users; it does not eliminate the regulated interactions with the PSP necessary for funds to enter and leave the offline functionality S23-S26.

Locally stored value requires specific technical protections

The ability to perform a transaction without a connection requires the device to be able to securely store and transfer the corresponding value.

The ECB's current work notably relies on the use of a secure hardware element S26.

This component notably protects:

- cryptographic keys;
- the available value;
- debit and credit operations;
- critical information necessary for the operation of the offline mechanism S26.

The objective is notably to prevent a user from artificially modifying their balance or duplicating the same value to make multiple payments.

Offline mode is therefore not simply an online mode that is temporarily disconnected: it requires a technical architecture specifically designed to enable a secure local transfer of value.

A protection that also limits certain interconnection possibilities

The safeguards of offline mode have an important consequence for the subject of this investigation.

If the details of a transaction remain exclusively on the payer's and beneficiary's devices and are transmitted neither to the PSP nor to the Eurosystem, external infrastructures do not automatically have the information necessary to link this individual payment to other databases.

TECHNICALLY DEDUCIBLE:

> The offline architecture currently described therefore constitutes a technical obstacle to systematic centralized cross-referencing between each individual payment and information originating from other infrastructures, since the personal details of the transaction are not transmitted to the central infrastructure.

This conclusion must, however, remain limited to offline operation as it is currently designed.

It does not establish that all interactions surrounding the payment are anonymous, since funding and defunding operations involve the PSP.

Nor does it establish that no usage limit, security rule or anti-fraud mechanism can be applied to the offline functionality.

These elements must be examined separately.

An architecture currently being tested

Offline operation is no longer merely a conceptual hypothesis.

The ECB is preparing a digital euro pilot scheduled to begin in the second half of 2027 and is currently continuing the work necessary to implement the offline functionality S26.

In August 2026, the ECB notably launched a technical consultation concerning the standards required to deploy offline mode in the secure hardware components of smartphones.

The work notably concerns embedded Secure Elements and eSIMs.

ESTABLISHED:

> The offline architecture is therefore currently the subject of concrete technical work concerning hardware components, security standards and preparation for the pilot S26.

It nevertheless remains a feature of a project that has not yet been deployed as a means of payment in general circulation.

What offline mode does not establish

The existence of an offline functionality does not mean that all digital euro payments will have the same level of privacy.

Online payments follow a different architecture.

Nor does it mean that offline mode will necessarily be usable without any limits on amount, holdings, frequency or security.

Finally, the fact that the personal details of an offline transaction are not transmitted does not establish that the merchant or beneficiary does not itself hold any information relating to the purchase in its own commercial systems.

A merchant may separately hold:

- a receipt;
- an order;
- a customer account;
- an invoice;
- a product identifier;
- or other commercial data.

NOT ESTABLISHED:

> The sources examined therefore do not establish that offline mode makes it impossible for cross-referencing to be performed independently by the merchant or by another system that separately holds the necessary commercial data.

This distinction is essential: the privacy of the **payment rail** does not necessarily mean the absence of data in the **commercial system** surrounding that payment.

Interim conclusion

ESTABLISHED:

> The digital euro is designed to enable online and offline payments based on different architectures S23-S26.

ESTABLISHED:

> An offline payment is intended to be executed directly between the payer's and beneficiary's devices without an Internet connection and without the intervention of an online system at the time of the transaction S26.

ESTABLISHED:

> The value and sensitive information necessary for offline payment must be protected within a secure hardware environment on the device S26.

ESTABLISHED:

> According to the architecture announced by the ECB, the personal details of offline transactions are accessible neither to the Eurosystem nor to PSPs and remain known to the payer and the beneficiary S23-S26.

ESTABLISHED:

> Operations enabling funds to be funded or defunded remain, however, linked to the PSP, which performs the corresponding regulatory controls S23-S26.

TECHNICALLY DEDUCIBLE:

> The absence of central transmission of the details of an offline payment significantly limits the possibility, at the payment infrastructure level, of systematically cross-referencing that transaction centrally with external tax, commercial or environmental data.

NOT ESTABLISHED:

> This protection does not establish that no cross-referencing can be performed independently within the beneficiary's commercial system when it holds data enabling the transaction, product or customer to be identified.

TO BE ESTABLISHED:

> What limits on amount, holdings, frequency or operation will ultimately be applied to offline payments?

TO BE ESTABLISHED:

> What information relating to funding and defunding operations will be retained by PSPs and for how long?

TO BE ESTABLISHED:

> Under what conditions can security, fraud prevention or limit management mechanisms prevent or defer an offline operation?

TO BE ESTABLISHED:

> Can an offline payment participate in a conditional payment mechanism, or do conditional mechanisms necessarily require an online component?

4.5 Programmable money and conditional payments

Status: ESTABLISHED / TECHNICALLY DEDUCIBLE / ONGOING PROJECT

The distinction between programmable money and conditional payments constitutes a central element of the architecture envisaged for the digital euro.

The European Central Bank explicitly excludes the digital euro becoming programmable money S22-S27.

At the same time, the architecture is designed to enable conditional payments, meaning payments whose execution can be automatically triggered when certain predetermined conditions are met S27.

These two mechanisms must not be confused.

Programmable money is explicitly excluded

The ECB defines programmable money as money whose use would be intrinsically limited according to certain rules.

Such money could, for example, be designed to:

- allow the purchase only of certain goods or services;
- be usable only during a specified period;
- be spendable only within a particular geographical area;
- or directly impose other restrictions on use attached to the monetary units S27.

The ECB explicitly indicates that such operation is incompatible with the principles adopted for the digital euro.

Digital euro units must remain fungible and retain the same value as other forms of the euro.

ESTABLISHED:

> The Eurosystem explicitly excludes digital euro units themselves containing rules limiting the goods, services, periods, locations or beneficiaries for which they can be used S22-S27.

The ECB presents this safeguard as a fundamental difference between money and a voucher restricted to a specific use.

A payment can nevertheless be conditional

The exclusion of programmable money does not mean that all payments must be executed immediately and without conditions.

The ECB defines conditional payments as payments executed automatically when predetermined conditions are met S27.

The condition does not alter the properties of the monetary units themselves.

It operates within the process determining **when a specific payment is to be executed**.

The distinction can be summarized as follows:

Programmable money

The rule is attached to the money itself.
Example: this monetary unit can only be used to purchase a specified category of goods.

Conditional payment

The money remains freely usable, but a specific transaction is executed only when the condition agreed for that transaction is met.
Example: payment for a product is released when its delivery is confirmed.

ESTABLISHED:

> The ECB therefore explicitly distinguishes a restriction attached to the money, which it excludes, from the conditional automation of a transaction, which is provided for in the digital euro architecture S27.

Funds reservation constitutes the basic mechanism

The envisaged architecture provides for a funds reservation functionality to support conditional payments S27.

When a conditional payment is initiated, the corresponding amount can be temporarily reserved in the payer's account.

The reserved amount then reduces the balance available for other spending, but it is not immediately transferred to the beneficiary.

The funds remain available to execute the payment when the specified condition is met.

The mechanism can be represented as follows:

```
Payment initiated
   ↓
Amount reserved
   ↓
Verification of the condition
   ↓
Condition met     → funds transferred to the beneficiary
Condition not met → reservation cancelled or expired
```

ESTABLISHED:

> The envisaged central infrastructure therefore provides a technical funds reservation capability enabling their transfer to be deferred until a condition has been verified S27.

A settlement layer separate from a conditionality layer

The preparation phase closure report explicitly describes a separation between two layers S27.

The first is the **settlement layer**, located in the back-end infrastructure and provided by the Eurosystem.

The second is a **conditionality layer**, developed by market actors.

The settlement layer handles monetary processing.

The conditionality layer determines whether the conditions specified for releasing the funds have been met.

The operation can be represented as follows:

Conditionality layer — market actors

```
Verification of an event or condition
   ↓
Result of the verification
   ↓
Funds reservation function / payment infrastructure
   ↓
Settlement layer – Eurosystem
   ↓
Transfer or release of funds
```

ESTABLISHED:

> The architecture currently described therefore technically separates the monetary settlement function from the logic used to determine whether a condition associated with a transaction has been met S27.

This separation is essential.

It means that the Eurosystem does not necessarily need to know or evaluate itself the data used to verify the condition.

External monitoring can trigger the condition

The ECB's preparation phase closure report specifies that this architecture must provide flexibility for **external monitoring capable of triggering the conditions** S27.

In the example provided by the ECB, a system can determine that a train has actually arrived.

When this information confirms that the specified condition has been met, the reserved funds are transferred to the beneficiary.

If the train does not arrive or if the specified condition is not met, the reservation can be cancelled or expire and the funds become available to the payer again S27.

ESTABLISHED:

> Information produced or verified outside the settlement layer can therefore technically contribute to triggering or not triggering a conditional payment S27.

This constitutes a first explicitly documented link between **data or an event external to monetary settlement** and **the execution of a transaction**.

Examples already identified and experimented

The work of the ECB and market actors has examined several categories of conditional payments S27.

The documented examples notably include:

- payment on delivery;
- pay-per-use;
- payments triggered by stages or milestones;
- automatic refunds;
- subscriptions;
- split payments;
- machine-to-machine payments;
- certain payments linked to energy consumption S27.

In the case of payment on delivery, the transaction can be finalized when delivery of the product is confirmed.

In a machine-to-machine payment, a machine can automatically contribute to triggering a payment when a specified event occurs.

The ECB and market actors have already tested the feasibility of several of these mechanisms in an environment simulating the digital euro back-end S27.

ESTABLISHED:

> Conditional payments are therefore no longer merely an abstract possibility described in a regulatory proposal: their technical feasibility has been experimented with market actors in the ECB's innovation environment S27.

These experiments did not, however, use actual digital euros and do not constitute the deployment of a production system.

The condition can be verified by a third party

Earlier ECB work also provides an example in which the triggering of a payment on delivery can depend on a third party other than the payer or beneficiary, such as the postal service responsible for confirming delivery of a product S27.

This architecture therefore potentially introduces a third actor into the technical decision enabling the payment to proceed.

```
Payer + beneficiary define or accept the condition
   ↓
Third party or external system verifies the event
   ↓
Confirmation of the condition
   ↓
Payment executed automatically
```

ESTABLISHED:

> Verification of a condition can therefore be carried out on the basis of information originating from an actor or system distinct from the payer, the beneficiary and the central settlement layer S27.

Market actors develop the conditional logic

The ECB considers supervised intermediaries and other market actors to be best placed to develop conditional payment services S27.

The digital euro infrastructure notably provides the fundamental funds reservation functionality.

Market actors can build value-added services on top of this infrastructure using their own logic and the information necessary for the relevant use cases.

In July 2026, the ECB also indicated that banks could use the digital euro infrastructure to automatically trigger payments when an agreed condition is met and develop new services by relying on the data available to them S27.

ESTABLISHED:

> Conditional logic is therefore not designed as a function exclusively defined and operated by the European Central Bank: banks, PSPs and other market actors can develop conditional services on top of the common infrastructure S27.

The first technical bridge with external data

The previous sections established that the payment architecture can process different information relating to transactions and that market actors have their own systems and data.

This section adds a further element: the conditionality layer can use the verification of an external event to determine whether the reserved funds should be transferred S27.

The general mechanism therefore becomes:

```
External data or event
   ↓
Verification of the condition
   ↓
Conditionality layer
   ↓
Instruction relating to the reserved funds
   ↓
Execution or non-execution of the payment
```

ESTABLISHED:

> The principle whereby information external to monetary settlement can trigger the execution of a conditional payment is explicitly provided for in the architecture examined S27.

This finding constitutes a **technical bridge between external information and the execution of a payment**.

It does not, however, establish that any information can be used as a condition.

This bridge does not demonstrate the use of environmental data

None of the sources examined in this section provide for a payment being conditioned by:

- the carbon footprint of a product;
- a Digital Product Passport;
- a GTIN;
- a cumulative environmental footprint;
- an individual environmental quota;
- tax data originating from electronic invoicing;
- or a user's behavioral profile.

The examples currently documented mainly concern events directly related to the performance of a contract or service: delivery, completion of a service, use of a service, timing, consumption or a verifiable event S27.

NOT ESTABLISHED:

> The existence of a conditionality layer capable of using external information does not demonstrate that it is currently designed to receive or use environmental data, tax data or individual profiles.

This distinction is fundamental to the analysis.

But the technical nature of the condition is not intrinsically monetary

The condition enabling the payment to be triggered may correspond to an event verified by a separate system.

The settlement system does not necessarily need to know all the information used to establish that this condition has been met.

TECHNICALLY DEDUCIBLE:

> A conditional payment architecture can technically use the result of a verification performed by an external system without the data used for that verification being directly integrated into the monetary infrastructure.

For example, the payment system could receive only a logical result:

```
Condition verified: YES
or
Condition verified: NO
```

without necessarily receiving all the data that led to that result.

This technical property means that an interconnection does not necessarily require the complete merging of the databases concerned.

Who decides the condition is a separate legal question

The technical ability to construct a condition does not mean that any actor can arbitrarily impose that condition on a user.

The ECB indicates that conditional payments are based on predetermined and agreed conditions and states that users remain free to choose whether to use these services S27.

In a January 2026 communication, the ECB also specified that the conditions of a payment could only be set by the payer and the beneficiary.

ESTABLISHED:

> Under the framework currently presented by the ECB, conditional payments are voluntary services based on conditions agreed between the parties and do not give the Eurosystem a general power to determine what a user may purchase S27.

This safeguard must be distinguished from the system's technical ability to automatically execute a transaction when the agreed condition has been met.

The exact boundary with an external restriction must remain under scrutiny

The conceptual distinction between programmable money and conditional payment is clear:

- programmable money imposes a restriction on the monetary unit itself;
- conditional payment applies logic to a specific transaction.

From the user's perspective, however, a condition may nevertheless have the practical effect that a specific payment is not executed until the specified criterion is met.

This observation does not establish that the system constitutes programmable money.

It merely shows that **the absence of programmability of the money does not imply the absence of programmable logic surrounding the execution of payments**.

TECHNICALLY DEDUCIBLE:

> An infrastructure can therefore simultaneously use fully fungible and non-programmable money while enabling external services to apply automated rules to the execution of specific transactions.

The determining question then becomes the governance of these rules: who can define a condition, with what consent, based on what data and within what legal framework?

Interim conclusion

ESTABLISHED:

> The ECB explicitly excludes the digital euro being programmable money that intrinsically limits the goods, services, periods, locations or beneficiaries for which the monetary units can be used S22-S27.

ESTABLISHED:

> The architecture nevertheless provides for conditional payments executed automatically when predetermined conditions are met S27.

ESTABLISHED:

> A funds reservation functionality is provided to temporarily retain the necessary amount until the condition has been verified S27.

ESTABLISHED:

> The ECB describes an architecture separating a settlement layer provided by the Eurosystem from a conditionality layer developed by market actors, with the possibility for an external verification to trigger the condition S27.

ESTABLISHED:

> Conditional payments have already been experimented in a simulated environment with market actors, notably for payment-on-delivery, pay-per-use, milestone payment and other automated service scenarios S27.

ESTABLISHED:

> The ECB indicates that banks and other providers will be able to develop conditional services on top of the common infrastructure and rely on the data available to them to offer innovative services S27.

TECHNICALLY DEDUCIBLE:

> Information originating from an external system can technically contribute to the execution or non-execution of a transaction without that information necessarily being stored in the money itself or fully transmitted to the settlement layer.

NOT ESTABLISHED:

> The sources examined do not establish that environmental data, DPPs, tax data or an individual profile are used as payment conditions in the architecture currently envisaged.

ESTABLISHED:

> Under the framework currently presented by the ECB, conditions are designed to be agreed between the parties, and the Eurosystem states that it does not have the power to block categories of purchases S27.

TO BE ESTABLISHED:

> What categories of external data can technically be used by services developing the conditionality layer?

TO BE ESTABLISHED:

> Which actors can provide the proof or result enabling a condition to be considered satisfied?

TO BE ESTABLISHED:

> What legal safeguards prevent a condition initially designed as voluntary or contractual from being imposed by an intermediary, regulation or another actor?

TO BE ESTABLISHED:

> Are there projects or experiments linking conditional payments to invoicing, product traceability or environmental data infrastructures?

4.6 External conditions and payment automation

Status: ESTABLISHED / TECHNICALLY DEDUCIBLE / TO BE ESTABLISHED

The previous section established that the architecture envisaged for the digital euro distinguishes between a settlement layer provided by the Eurosystem and a conditionality layer developed by market actors S27.

The work carried out within the innovation platform makes it possible to go further: market actors have actually connected their own platforms to an environment simulating the digital euro interfaces in order to experiment with conditional payments S28.

It therefore becomes possible to distinguish three components:

```
External system or platform
   ↓
Logic used to verify a condition
   ↓
Infrastructure enabling funds to be reserved and then transferred
```

This architecture has been the subject of technical experiments, even though the digital euro itself is not yet in circulation S28.

Participant platforms were connected to the simulated interfaces

As part of the "pioneers" workstream, the ECB provided participants with an environment simulating the digital euro back-end, as well as technical specifications and programming interfaces S28.

Participants were able to connect their own platforms to this environment through APIs.

In the experiment, they acted as providers developing their own services on top of the core functionalities provided by the Eurosystem.

ESTABLISHED:

> Platforms developed or operated by market actors were therefore effectively connected, on an experimental basis, to interfaces simulating the digital euro infrastructure S28.

This is not yet a connection to the future production system.

Nevertheless, this experiment demonstrates that the architecture is designed to enable external systems developed by market actors to use the functionalities provided by the common infrastructure.

The Eurosystem provides the monetary function, the market develops the condition

The distribution of responsibilities experimented follows the separation described previously S27-S28.

The Eurosystem provides the fundamental functions necessary for monetary processing, notably the reservation of funds.

PSPs and other market actors develop the layer determining the conditions necessary for their release.

The mechanism can be represented as follows:

```
**Eurosystem infrastructure**

funds reservation
   ↓
**PSP or market actor platform**

definition and management of the condition
   ↓
**Information enabling the condition to be verified**
   ↓
condition met
   ↓
instruction enabling the release of funds
```

ESTABLISHED:

> In the experiments carried out, the logic determining the condition was therefore not necessarily located within the Eurosystem's central infrastructure: it could be developed and managed by the platforms of market actors S28.

The condition can depend on an event external to the payment

Several scenarios examined show that the condition does not need to be information produced by the monetary system itself S27-S28.

In a payment on delivery, the determining information is confirmation of the product's delivery.

In a transport-related refund, it may be linked to the performance, delay or cancellation of the service.

In a pay-per-use payment, it may depend on the actual use of a service or equipment.

In a milestone payment, it may depend on the successive completion of predetermined objectives or milestones S28.

ESTABLISHED:

> The conditions examined can therefore depend on facts or events produced outside the monetary infrastructure and verified by the conditional layer developed by market actors S27-S28.

An external system does not necessarily need to transmit all its data

The separation between the conditional layer and the settlement layer allows an external system to perform certain verifications itself.

The monetary layer does not then necessarily need to receive all the information used to perform that verification.

The mechanism can be summarized as follows:

```
external system holds information
   ↓
external system verifies a rule
   ↓
result: condition met or not met
   ↓
conditional layer processes this result
   ↓
funds released or kept reserved
```

TECHNICALLY DEDUCIBLE:

> Data used to determine the execution of a payment therefore do not necessarily need to be stored within the monetary infrastructure or even transmitted to it in full: a verification result may technically be sufficient.

This property is important for the study of interconnections.

The absence of data from the digital euro data dictionary is not, by itself, sufficient to establish that such data could never indirectly contribute to the logic of a payment service developed around the infrastructure.

Machine-to-machine payments extend automation

The experiments also examined scenarios related to Industry 4.0 and machine-to-machine payments S28.

In these scenarios, equipment or digital systems can automatically participate in the initiation or triggering of financial operations.

One example examined involves a machine detecting by itself the need for a replacement part and participating in the automation of the corresponding commercial process.

These scenarios notably seek to reduce manual intervention and enable real-time settlements or settlements based on the actual use of a service S28.

ESTABLISHED:

> The experimental work is therefore not limited to payments manually triggered by a person: it also examines chains in which systems or machines can automatically participate in the initiation and processing of a transaction S28.

This automation does not mean that a machine can arbitrarily spend a user's money: it operates within a framework of service, mandate, authorization and predefined conditions.

Milestones can progressively determine the release of funds

The experiments examined payments based on stages or "milestones" S28.

In this type of scenario, the full amount of funds is not necessarily released at once.

Payment can be made progressively when different predefined objectives are considered to have been achieved.

One example examined concerns online training for which funds could be released progressively as the learner achieves certain objectives.

Another example concerns crowdfunding, in which funds could be released according to the progress of a project S28.

ESTABLISHED:

> An external condition can therefore not only determine whether a payment should be executed, but also contribute to determining the time or stage at which part of the funds should be released S28.

Pay-per-use payments rely on measurable data

Pay-per-use constitutes another category examined by the platform S28.

In this type of mechanism, the amount or timing of the payment depends on the actual use of a good or service.

The condition can therefore be supplied by information measuring that use.

This may notably concern mobility services, infrastructures or certain connected equipment.

TECHNICALLY DEDUCIBLE:

> When an external system is capable of measuring an event or quantity and communicating the corresponding result to the conditional layer, this information can technically contribute to the automation of the payment.

This is a general operating principle of conditional payments and not evidence that any category of data can be used without restriction.

Automation can also apply to refunds

The ECB's work does not focus solely on triggering a payment to a merchant S27-S28.

It also examines the automation of refunds when certain conditions are met.

In the transport sector, for example, a cancellation or delay may lead to the automation of a refund.

The same general principle applies:

```
external event
   ↓
verification of the situation
   ↓
automatic triggering
   ↓
payment or refund
```

ESTABLISHED:

> The use of an external condition can therefore affect different financial flows, notably the release of a payment or the triggering of a refund S27-S28.

Payment can be associated with additional commercial information

The innovation platform also examined complementary services such as electronic receipts S28.

The ECB presents e-receipts as a functionality that could be associated with digital euro payments, notably to enable users to track their spending and manage their warranties.

This functionality is distinct from monetary settlement.

It nevertheless shows that market actors are considering services in which a payment transaction can be associated with additional commercial information.

ESTABLISHED:

> The work of the innovation platform therefore also envisages associating a digital euro payment with commercial information external to the strict monetary transfer, notably through electronic receipts S28.

TO BE ESTABLISHED:

> What level of granularity could these electronic receipts contain, and could they notably include product references, purchase line items or standardized identifiers?

The link with the product becomes technically concrete in certain scenarios

The payment-on-delivery scenario already relies on a relationship between:

- an order;
- a purchased product;
- a delivery;
- a transaction;
- a condition;
- and the release of funds S27-S28.

The system must be able to determine that the verified event corresponds to the transaction for which the funds were reserved.

There is therefore necessarily, within the service developed around the payment, a mechanism enabling the verified condition to be matched with the transaction concerned.

ESTABLISHED:

> The scenarios experimented demonstrate that an external platform can technically associate a commercial event relating to an order or service with the transaction whose execution depends on that event S28.

This does not mean that the central infrastructure knows the details of the product.

The matching can be performed within the external platform, which then transmits only the information necessary for the payment to proceed.

The generic bridge between external data and payment is established

At this stage, several elements can be assembled.

Chapter 4 has established:

- that a transaction has structured identifiers S25;
- that a funds reservation architecture enables their transfer to be deferred S27;
- that a conditionality layer can be developed by market actors S27-S28;
- that external monitoring can trigger a condition S27;
- that participant platforms have actually been connected to the simulated digital euro interfaces S28;
- that commercial events external to settlement have been used in conditional payment scenarios S28.

The following chain is therefore now documented in principle:

```
event or data originating from an external system
   ↓
platform or service of the market actor
   ↓
verification of a condition
   ↓
association with the corresponding transaction
   ↓
use of the funds reservation functionality
   ↓
execution, release, retention or return of funds depending on the scenario
```

ESTABLISHED:

> The architecture and experiments examined therefore establish that a system external to the settlement layer can provide or verify information used by a conditional service to determine the execution of a specific transaction S27-S28.

This finding now goes beyond the mere abstract possibility of a computer architecture: the general mechanism has been the subject of technical experiments involving market actor platforms connected to an environment simulating the digital euro S28.

The specific bridge with environmental data is not established

This conclusion must not, however, be extended beyond what the sources demonstrate.

None of the experiments examined establish that a payment condition has been supplied by:

- a Digital Product Passport;
- a DPP identifier;
- a GTIN used to query a DPP;
- the carbon footprint of a product;
- a cumulative environmental footprint;
- data originating from the French electronic invoicing system;
- an individual environmental profile.

NOT ESTABLISHED:

> The generic bridge between an external system and a conditional payment is documented, but the specific bridge between environmental or tax data and the execution of a payment is not established at this stage.

This distinction constitutes an essential limitation of the investigation.

The combination with Chapter 3 nevertheless becomes technically analyzable

Chapter 3 separately established that a product can be associated with a digital identifier and structured environmental data and that, when compatible identifiers exist, this information can technically be matched with a commercial transaction.

The present chapter now establishes that information originating from an external system can be verified within a conditionality layer and contribute to the execution of a payment.

These two findings do not demonstrate that they are actually interconnected.

They nevertheless make it possible to identify precisely the technical connection that would be required:

```
transaction or order
   ↓
identifiable product
   ↓
external system holding information relating to the product
   ↓
rule or condition applied within an external service
   ↓
verification result
   ↓
payment conditionality layer
   ↓
execution or non-execution depending on the condition
```

TECHNICALLY DEDUCIBLE:

> If an authorized actor had environmental data relating to a product and if that data were used as a criterion for a payment condition, the architecture described for conditional payments would technically enable the result of that verification to contribute to the execution of the transaction without the environmental data being integrated into the money itself.

This proposition describes a technical possibility resulting from the combination of components documented separately.

It demonstrates neither the existence of such a service, nor its legal authorization, nor its use by an administration, bank or PSP.

An interconnection does not necessarily require a single database

The findings from Chapters 3 and 4 also show that a potential interconnection would not necessarily need to centralize all information within a single system.

A service could theoretically:

```
receive the identifier necessary for a transaction
   ↓
query an authorized external system
   ↓
verify a condition
   ↓
obtain a result
   ↓
transmit only that result to the system responsible for the payment
```

TECHNICALLY DEDUCIBLE:

> The absence of physical merging between environmental, commercial and monetary databases is therefore not sufficient to technically exclude a decision-making mechanism based on their interoperability.

This deduction is consistent with the architectures examined: they rely precisely on identifiers, APIs, access rights and exchanges between specialized components.

Consent and governance remain decisive

The technical ability to use an external condition does not determine who has the right to define that condition.

In the use cases currently presented by the ECB, conditional payments are services intended to meet a need of the payer and the beneficiary S27.

They do not constitute a general power granted to the Eurosystem to decide which purchases should be authorized.

A distinction must therefore be maintained between:

- a voluntary condition chosen within a service;
- a contractual condition imposed by the terms of use of a service;
- a regulatory condition imposed by law;
- a decision taken by an intermediary in accordance with its legal obligations;
- a restriction attached to the money itself.

These situations may produce similar technical effects on a transaction but are based on different legal grounds and decision-making actors.

TO BE ESTABLISHED:

> What safeguards prevent or regulate the use of the conditional layer for criteria other than those voluntarily accepted by the payer and the beneficiary?

Experiments continue in 2026

The work of the innovation platform did not end with the first experiment S28.

The ECB announced a new phase of collaboration with market actors in 2026.

This phase is intended notably to further explore conditional payments and other value-added services, such as electronic receipts, bill splitting and budgeting tools.

The ECB also indicates that it intends to continue exploring machine-to-machine payments, artificial intelligence applied to payments, micropayments and various B2B use cases.

ESTABLISHED:

> The integration of external services and payment automation therefore remain an active area of development and experimentation for the project in 2026 S28.

The final characteristics of the resulting services have not, however, yet been established.

Interim conclusion

ESTABLISHED:

> Market actors have connected their own platforms, through APIs, to an environment simulating the digital euro interfaces in order to test conditional payments S28.

ESTABLISHED:

> In the architecture experimented, the Eurosystem provides the fundamental monetary functionalities, while PSPs and other market actors can develop and manage the logic determining the conditions for releasing funds S27-S28.

ESTABLISHED:

> The conditions experimented can depend on events external to monetary settlement, notably delivery, use of a service, completion of a milestone or other verifiable events S28.

ESTABLISHED:

> Machine-to-machine scenarios have also been examined, enabling systems or equipment to automatically participate in certain commercial and payment processes S28.

ESTABLISHED:

> The generic mechanism enabling an external system to provide or verify information contributing to the execution of a conditional payment has therefore moved beyond the stage of a mere technical hypothesis and has been the subject of experiments in a simulated environment S27-S28.

TECHNICALLY DEDUCIBLE:

> External data do not necessarily need to be directly transmitted to or stored within the monetary infrastructure: the conditional layer can technically perform or receive a verification and communicate only the result necessary for the execution of the payment.

TECHNICALLY DEDUCIBLE:

> The combination with the infrastructures examined in Chapter 3 makes technically possible an architecture in which an environmental characteristic of a product would be verified in an external system and then used as a criterion for a conditional payment service.

NOT ESTABLISHED:

> None of the elements examined establish that a DPP, a GTIN, a carbon footprint, data originating from electronic invoicing or an individual environmental profile are currently used to trigger, prevent or modify a digital euro payment.

TO BE ESTABLISHED:

> Are there experiments, consortia, public procurement contracts, specifications or partnerships concretely linking product traceability, electronic invoicing or environmental data infrastructures to conditional payment services?

TO BE ESTABLISHED:

> Will the electronic receipts envisaged with the digital euro be able to carry product identifiers or other information enabling automated matching with commercial or environmental systems?

TO BE ESTABLISHED:

> Which actors are simultaneously involved in DPP, electronic invoicing and digital euro projects, and are they developing interfaces or services enabling these infrastructures to be linked?

4.7 Digital identity and payment infrastructures

Status: ESTABLISHED / ONGOING PROJECT

European digital identity constitutes an infrastructure distinct from the digital euro.

Official sources nevertheless establish an explicit connection between the European Digital Identity Wallet, or EUDI Wallet, and payment infrastructures S29.

The European Commission documents a use case specifically dedicated to payment authentication using the EUDI Wallet.

In parallel, the European Central Bank provides for providers participating in the digital euro pilot to be able to use this wallet as a strong authentication method for certain online transactions S29.

The link between digital identity and payment is therefore not merely technically deducible: it is explicitly provided for in the architectures examined.

The EUDI Wallet constitutes a European digital identity infrastructure

The European digital identity framework provides for wallets enabling natural and legal persons to identify themselves and present various digital attestations S29.

The wallet can notably contain or enable the presentation of:

- identity data;
- electronic attestations;
- verifiable credentials or attributes;
- elements necessary for authentication with public or private services.

The architecture relies on common formats and protocols enabling issuers, wallets and relying parties to cryptographically verify the information presented.

Its use is intended to be voluntary for the user.

The EUDI Wallet is explicitly provided for payments

The European Commission documents a use case entitled **Payment Authentication** enabling the EUDI Wallet to be used to authenticate online or in-store payments S29.

This architecture is designed to work with existing payment infrastructures, notably card payments and account-to-account payments.

The wallet therefore does not necessarily itself constitute the system transferring the funds.

It acts as a component notably enabling the payer to be authenticated and the evidence necessary for the transaction to be presented.

The general operation can be summarized as follows:

```
user
   ↓
EUDI Wallet
   ↓
presentation of evidence or an attestation
   ↓
bank / PSP / acquirer / merchant
   ↓
payment authentication
```

ESTABLISHED:

> A European digital identity infrastructure is explicitly designed to be able to intervene directly in the payment authentication process S29.

The wallet can be linked to a payer and an account

The documentation notably provides for strong authentication attestations issued by payment service providers S29.

These attestations make it possible to establish a verifiable link between:

- the wallet;
- a specific payer;
- and a specific payment account or instrument.

When a payment is initiated, the wallet can present the appropriate attestation to the party responsible for verifying it, for example a bank, an acquirer or a merchant.

ESTABLISHED:

> The EUDI Wallet can therefore act as a cryptographically verifiable component linking the user to the authentication of a payment transaction and to the instrument or account concerned S29.

This does not mean that all identity information contained in the wallet is transmitted with each payment.

Selective disclosure makes it possible to present an attribute without transmitting the entire identity

The EUDI Wallet architecture notably relies on a principle of selective disclosure S29.

The user can present only the information necessary for a given interaction rather than their entire identity or the entire document containing that information.

The Commission notably provides the following examples:

- age;
- residence;
- certain information from a driving licence S29.

In a purchase scenario subject to an age requirement, the system can therefore verify that the user meets the required criterion without necessarily receiving their full date of birth.

The principle can be represented as follows:

```
wallet containing verifiable information
   ↓
selection of the necessary attribute
   ↓
proof of the required criterion
   ↓
verifying service or merchant
```

ESTABLISHED:

> The infrastructure therefore technically enables an attribute relating to a person to be verified in the context of a payment without requiring the transmission of their entire identity S29.

Age already constitutes a concrete example of a criterion associated with a purchase

The official documentation specifically provides the example of a purchase requiring age verification S29.

In the flow presented by the Commission, the user makes an online purchase and uses their EUDI Wallet in the authentication process.

The wallet notably displays the merchant, the amount and the requested attributes.

The user can then present the necessary proof.

ESTABLISHED:

> A verifiable personal attribute originating from the digital identity infrastructure can therefore already be integrated into the technical flow surrounding a payment in order to verify a condition applicable to the purchase S29.

It is, however, essential to distinguish this mechanism from a conditional payment within the meaning examined in Sections 4.5 and 4.6.

In this example, age verification responds to a requirement related to access to or the sale of the product; it does not constitute evidence that the digital euro itself applies a purchase restriction.

The connection with the digital euro is explicitly provided for

The relationship between the EUDI Wallet and the digital euro is not merely a possibility resulting from the existence of two compatible European infrastructures.

The ECB documentation relating to the digital euro pilot explicitly states this S29.

PSPs participating in the pilot will be able to support the EUDI Wallet as a strong authentication method for online transactions when the user uses the PSP's digital instruments.

PSPs remain free to choose their authentication methods, subject to compliance with the applicable regulatory requirements.

ESTABLISHED:

> The use of the EUDI Wallet as an authentication method in the digital euro pilot is explicitly provided for by the European Central Bank S29.

The following connection is therefore officially documented:

```
EUDI Wallet
   ↓
strong authentication
   ↓
PSP
   ↓
digital euro payment
```

This connection is stronger than the hypothetical connections examined with other infrastructures: it is directly described by the ECB for the pilot.

European pilots have already experimented with identity and payment

The use of the EUDI Wallet in payments has also been the subject of European Large Scale Pilots S29.

European projects have notably tested:

- payment initiation;
- strong authentication;
- online payments;
- in-store payments;
- age verification associated with a payment.

ESTABLISHED:

> The connection between European digital identity and payment infrastructure has therefore moved beyond the stage of a mere conceptual specification: it has already been the subject of European pilots S29.

These experiments do not, however, constitute evidence of a generalized system automatically linking all identity information to all transactions.

The same infrastructure can present different types of attestations

The EUDI Wallet is not limited to basic civil identity.

Its architecture makes it possible to store and present different types of attestations issued by trusted sources.

This means that the same technical mechanism can be used to present different attributes depending on the service concerned.

TECHNICALLY DEDUCIBLE:

> A payment infrastructure using the EUDI Wallet for authentication or verification does not necessarily need to access all the data held by the wallet: it can request and receive only the attestation or attribute necessary for the process concerned.

From an architectural perspective, this logic is comparable to that examined for conditional payments: the component making a decision does not necessarily need to hold all the source data when the system can present it with verifiable proof.

The identity → payment connection is established, but its scope must be delimited

At this stage, the following chain can be considered documented:

```
verifiable attribute or identity
   ↓
EUDI Wallet
   ↓
presentation of proof
   ↓
PSP / bank / acquirer / merchant
   ↓
authentication or verification necessary for the payment process
```

And, within the digital euro pilot:

```
EUDI Wallet
   ↓
strong authentication
   ↓
PSP participating in the pilot
   ↓
digital euro transaction
```

ESTABLISHED:

> There is therefore an explicitly provided institutional and technical connection between the European digital identity infrastructure and payment infrastructures, including within the digital euro pilot S29.

This connection does not mean that a complete profile accompanies each payment

The existence of this connection should not lead to the conclusion that all data held in the EUDI Wallet is automatically communicated to the PSP or merchant.

On the contrary, the wallet's design is based on principles of data minimization and selective disclosure S29.

A verification may, for example, concern only whether a person meets an age requirement.

NOT ESTABLISHED:

> The sources examined do not establish that all attributes held in an EUDI Wallet can be accessed by a bank, PSP, merchant or the Eurosystem during a payment.

NOT ESTABLISHED:

> Nor do they establish that a general purchase history is recorded in the EUDI Wallet for individual profiling purposes.

The combination with conditional payments must be distinguished from authentication

Sections 4.5 and 4.6 established that external data can contribute to the verification of a condition triggering a conditional payment.

The present section establishes that an identity wallet can provide verifiable proof within the payment process.

These two mechanisms are technically compatible in principle, but their systematic combination has not been demonstrated.

TECHNICALLY DEDUCIBLE:

> A verifiable attestation provided by an identity infrastructure can technically constitute one of the pieces of information used by an external service to verify that a condition necessary for an operation has been met.

The example of age verification already shows that an individual attribute can be involved in a commercial process associated with a payment.

NOT ESTABLISHED:

> This does not demonstrate that an environmental, tax, social or behavioral attribute can currently be imposed as a general condition for using the digital euro.

The connection with the other infrastructures remains to be established

The previous chapters have now separately identified several mechanisms:

Chapter 1
structured data relating to transactions and invoicing

Chapter 3
identifiable products and structured environmental data

Chapter 4.5–4.6
external systems and conditions that can contribute to the automated execution of a payment

Chapter 4.7
verifiable identity or attribute that can directly contribute to the payment process

The separate existence of these four elements still does not demonstrate their overall interconnection.

It does, however, progressively reduce the number of purely hypothetical connections.

The connection:

> **digital identity → payment infrastructure**

is now **ESTABLISHED** S29.

The connection:

> **EUDI Wallet → payment authentication in the digital euro pilot**

is also **ESTABLISHED** S29.

The connection:

> **external system → condition → automated execution of a payment**

was established in the previous sections S27-S28.

By contrast, the connection:

> **invoicing data / DPP / environmental data → individual attribute → condition applied to a payment**

remains **TO BE ESTABLISHED**.

Interim conclusion

ESTABLISHED:

> The EUDI Wallet is explicitly designed to be used for the authentication of online and in-store payments S29.

ESTABLISHED:

> Attestations issued notably by PSPs can establish a verifiable link between a wallet, a payer and a payment account or instrument S29.

ESTABLISHED:

> The architecture enables the selective presentation of certain personal attributes, notably age or residence, without necessarily transmitting the user's entire identity S29.

ESTABLISHED:

> European pilots have already experimented with payments using the EUDI Wallet, including scenarios combining payment and age verification S29.

ESTABLISHED:

> The ECB explicitly provides for PSPs participating in the digital euro pilot to be able to use the EUDI Wallet as a strong authentication method for online payments S29.

TECHNICALLY DEDUCIBLE:

> Verifiable proof or an attribute originating from an identity infrastructure can technically be used in a verification process surrounding a transaction without all the source data being communicated to the payment system.

NOT ESTABLISHED:

> None of the elements examined establish that the EUDI Wallet is currently intended to provide an environmental, tax or behavioral profile used to authorize or refuse digital euro payments.

TO BE ESTABLISHED:

> What attributes other than those currently documented for authentication may be requested in future payment services using the EUDI Wallet?

TO BE ESTABLISHED:

> Under what legal conditions may a merchant, bank, PSP or other service request the presentation of an attribute before the execution of a transaction?

TO BE ESTABLISHED:

> Are there European infrastructures or projects enabling attestations held in an identity wallet to be linked to invoicing, product or environmental data?

4.8 Limitations and safeguards provided

Status: ESTABLISHED / ONGOING PROJECT / TO BE ESTABLISHED

The previous sections established that the architecture envisaged for the digital euro includes significant technical capabilities: structured processing of transactions, involvement of multiple providers, funds reservation, conditional payments, use of information originating from external systems and the possibility of using a digital identity infrastructure in the payment process S22-S24-S25-S27-S28-S29.

These capabilities cannot, however, be analyzed independently of the legal and technical safeguards provided to limit their use.

A distinction must notably be made between:

- what is explicitly prohibited;
- what is made more difficult by the architecture;
- what remains possible but is regulated by law;
- and what would depend on a future change to the legal framework.

The digital euro must not be programmable money

The most explicit safeguard concerns the programmability of money.

The proposed regulation excludes the digital euro being designed as money intrinsically subject to conditions limiting its use to certain goods, services, locations, persons or periods S22.

This prohibition is also consistently affirmed by the European Central Bank S23-S27.

ESTABLISHED:

> The Eurosystem must not be able to assign rules to certain digital euro units determining the goods or services for which they can be spent S22-S23-S27.

A digital euro unit must remain fungible with other units.

This safeguard therefore prohibits a scenario in which the money itself would carry, for example, a rule such as:

"this unit cannot be used to purchase this product."

This prohibition does not eliminate conditional payments

As established in 4.5 and 4.6, the prohibition of programmable money does not eliminate the possibility of building conditional services around payments S27-S28.

The legal and technical distinction is fundamental:

restriction attached to the money → explicitly excluded

condition attached to a transaction or service → provided for in the architecture

ESTABLISHED:

> The safeguard against programmable money therefore does not prohibit all automated logic surrounding the execution of a payment S22-S27.

This is precisely why the governance of the conditionality layer is important.

Conditions are presented as having to be agreed between the parties

In the model presented by the ECB, conditional payments correspond to services in which the conditions are determined or accepted by the parties to the transaction S27.

The Eurosystem provides the monetary infrastructure necessary for settlement and funds reservation but is not presented as the actor defining the commercial criteria enabling their release.

ESTABLISHED:

> Under the framework currently presented, the Eurosystem does not have a general power enabling it to define the goods or services that a user can purchase using the digital euro S22-S27.

This safeguard is important.

It does not, however, fully answer another question:

can a criterion become mandatory because it results not from the ECB but from a legal or regulatory obligation applicable to the PSP, merchant or user?

This question then concerns less the monetary design than the law applicable to the actor executing the payment.

TO BE ESTABLISHED:

> Under what conditions could a rule external to the monetary system legally require a PSP or another intermediary to verify a criterion before executing a transaction?

PSPs already have control and non-execution capabilities

The existence of non-programmable money does not mean that a payment service provider is technically required to execute every transaction presented to it.

As established in 4.2, PSPs remain subject to various regulatory obligations concerning notably:

- anti-money laundering and counter-terrorist financing;
- sanctions and embargoes;
- fraud prevention;
- security;
- certain tax obligations S22-S24.

In certain circumstances provided for by law, these obligations may result in an operation being prevented, suspended or refused.

ESTABLISHED:

> The prohibition of programmable money therefore does not amount to an absolute technical or legal impossibility of blocking a transaction: control and non-execution mechanisms already exist where a legal basis provides for them S22-S24.

The central question is therefore not only:

"can the payment be blocked?"

but also:

"who has the power to block it, for what reason and on what legal basis?"

Holding limits are provided for

The proposed regulation also provides for the possibility of applying limits to the amount of digital euros that a user can hold S22.

These limits are notably intended to preserve financial stability and prevent an excessive migration of bank deposits to central bank money.

PSPs participate in the application of these limits.

Mechanisms are also provided to verify that a user holding several digital euro accounts cannot circumvent the applicable overall limit S22.

ESTABLISHED:

> The architecture therefore already provides for quantitative rules that can be automatically verified and applied to digital euro holdings S22.

These limits concern the **holding** of digital euros and not the nature of the goods or services purchased.

They therefore do not constitute a restriction on consumption.

The infrastructure can verify a rule without knowing its full context

The verification of holding limits nevertheless illustrates a technical principle already encountered in the previous sections.

Several components can cooperate to determine that a rule is satisfied without each of them having all the information relating to the user.

This logic is consistent with that of conditional payments and digital identity:

```
data or attribute
   ↓
verification of a rule
   ↓
result usable by another component
```

TECHNICALLY DEDUCIBLE:

> The architecture therefore enables the automated application of certain rules without requiring a single actor to centralize all the data used to verify them.

This characteristic constitutes both a technical capability and, when based on pseudonymization or selective disclosure, a data protection mechanism.

The ECB must not be able to directly identify users from central data

The proposed regulation provides that data communicated to the ECB and national central banks must be organized in such a way as not to enable them to directly identify users S22.

The architecture notably provides for separation, pseudonymization and cryptographic protection mechanisms.

As established in 4.3, PSPs nevertheless retain the relationship with their customers and hold the information necessary for that relationship as well as for compliance with their regulatory obligations S22-S25.

ESTABLISHED:

> The current design therefore seeks to prevent the Eurosystem's central infrastructure from directly constituting a complete nominative database of individual payments S22-S23.

This does not mean that no actor in the chain can identify the user.

The protection relies precisely on a **distribution of information among different actors**.

Data separation constitutes a safeguard, but not an absence of processing

Pseudonymization does not mean that transactions cease to exist or become technically impossible to process.

It means that certain components use identifiers that do not directly enable the person concerned to be identified.

PSPs, in parallel, have the relationship enabling them to identify their own customers.

ESTABLISHED:

> The architecture therefore relies more on a separation of knowledge and responsibilities than on the complete absence of data S22-S25.

This distinction is important for the analysis of interconnections.

A distributed system can enable multiple forms of processing without a single central database containing all the information.

Offline mode constitutes the strongest architectural protection

The offline mode examined in 4.4 constitutes a different situation S23-S26.

The personal details of the payment are designed to remain on the payer's and beneficiary's devices and not be transmitted to PSPs or the Eurosystem.

ESTABLISHED:

> Under the architecture currently envisaged, offline mode therefore prevents the central infrastructure from systematically processing the individual details of each offline transaction S23-S26.

This protection constitutes a much greater technical obstacle to centralized matching than the mere pseudonymization of an online transaction.

Funding and defunding operations nevertheless remain visible to the PSP and subject to the corresponding regulatory controls.

Data minimization is also provided for digital identity

The EUDI Wallet notably relies on selective disclosure S29.

When a service needs to verify an attribute, the objective is to transmit only the necessary information.

For example:

"user over 18 years old: YES"

may be sufficient without transmitting the full date of birth.

ESTABLISHED:

> The interconnection between digital identity and payment therefore does not necessarily imply the transmission of the user's entire identity profile S29.

This architecture limits the amount of data exposed.

It nevertheless also confirms that a decision can technically be based on a personal attribute without the system making that decision knowing all the data used to produce the proof.

The safeguards rely partly on law and can therefore evolve with it

A fundamental distinction must be made between a technical impossibility and a legal prohibition.

Certain safeguards are deeply embedded in the architecture, notably the protection of offline mode.

Others rely on rules defining authorized purposes, access rights, PSP obligations or categories of permitted processing.

TECHNICALLY DEDUCIBLE:

> When a technical capability exists but its use is prohibited or limited by law, the safeguard depends on the continued existence of the legal framework governing that capability.

This does not mean that this framework is intended to be modified.

It simply means that a legal prohibition should not be presented as a technical impossibility.

This distinction is essential throughout this investigation.

The current safeguards prevent several excessive conclusions

Based on the sources examined, it would be incorrect to claim that:

- the ECB will be able to arbitrarily decide what a citizen can purchase;
- the digital euro will intrinsically include a carbon quota;
- each monetary unit will be restrictable to certain products;
- the ECB will necessarily have a complete nominative history of purchases;
- DPP data will automatically be transmitted with each payment;
- the EUDI Wallet will automatically transmit all personal attributes during a transaction;
- offline payments will enable centralized tracking identical to online payments.

NOT ESTABLISHED:

> None of the elements examined demonstrate the current existence of a system capable of assigning an environmental quota to a person and then automatically blocking their purchases when that quota is reached.

But the safeguards do not eliminate the documented technical capabilities

Conversely, it would also be incorrect to conclude that the prohibition of programmable money makes any automated decision surrounding a payment technically impossible.

The previous sections separately established:

```
structured and identifiable transactions [S25](#s25)
   ↓
funds reservation [S27](#s27)
   ↓
conditionality layer external to the Eurosystem [S27](#s27)-[S28](#s28)
   ↓
possible verification of events originating from external systems [S27](#s27)-
[S28](#s28)
   ↓
market actor platforms connected through APIs in the experiments [S28](#s28)
   ↓
verifiable identity and attributes that can contribute to the payment process
[S29](#s29)
```

ESTABLISHED:

> The safeguards surrounding the digital euro limit the authorized uses of these capabilities but do not eliminate the existence of the technical components enabling automation, condition verification and interaction with external systems S22-S27-S28-S29.

The central question therefore shifts to governance

After examining the safeguards, the question is no longer merely whether the infrastructure technically possesses the components enabling certain operations to be automated or conditioned.

Some of these components are now documented.

The question becomes:

```
who can define the rule?
   ↓
on what legal basis?
   ↓
based on what data?
   ↓
with what consent or obligation?
   ↓
which actor verifies the condition?
   ↓
which actor has the ability to act on the transaction?
```

This distinction between **technical capability** and **legal authority** will need to remain central in the chapters devoted to interconnections and legal safeguards.

Interim conclusion

ESTABLISHED:

> The digital euro proposal prohibits programmable money in the sense of monetary units intrinsically carrying restrictions relating to the goods, services, locations, persons or periods for which they may be used S22-S27.

ESTABLISHED:

> This prohibition does not prevent conditional payments, which rely on logic applied to a transaction or service rather than to the money itself S27-S28.

ESTABLISHED:

> PSPs remain able and, in certain situations, legally required to perform controls that may result in the non-execution of a transaction, notably in the areas of fraud, sanctions and anti-money laundering S22-S24.

ESTABLISHED:

> Digital euro holding limits can be defined and applied automatically, but they concern the amount held and not the categories of goods that can be purchased S22.

ESTABLISHED:

> The architecture provides for a separation between the identity known to PSPs and the pseudonymized information processed by the central infrastructure, while offline mode benefits from stronger protection preventing the central transmission of personal transaction details S22-S23-S26.

ESTABLISHED:

> The EUDI Wallet notably relies on data minimization and selective disclosure of the necessary attributes S29.

TECHNICALLY DEDUCIBLE:

> Legal safeguards governing a technical capability must not be confused with the absence of that technical capability.

NOT ESTABLISHED:

> None of the elements examined establish the existence of a current mechanism assigning an individual environmental quota and then using that quota to authorize or refuse payments.

TO BE ESTABLISHED:

> To what extent do the rules governing conditional payments legally prevent a condition from being imposed other than through the voluntary agreement of the payer and the beneficiary?

TO BE ESTABLISHED:

> Could a regulation external to the digital euro framework legally require a PSP, merchant or other intermediary to verify an attribute or condition before executing a transaction?

TO BE ESTABLISHED:

> What legal safeguards prevent data originating from other digital infrastructures from being used as decision-making criteria in a payment service?

TO BE ESTABLISHED:

> Which safeguards arise directly from the technical architecture and which depend primarily on a legal framework that may evolve?

4.9 What this chapter establishes

The analysis of the digital euro shows that it is not merely a new means of payment reproducing the functioning of cash in digital form.

The project relies on a structured infrastructure involving the Eurosystem, payment service providers, acceptance devices, common services and various interfaces enabling market actors to develop complementary services S22-S23-S24.

The technical documents and experiments examined also establish several important capabilities concerning data, payment automation and interaction with external systems.

These capabilities must, however, be distinguished from uses that are actually authorized or currently deployed.

A centralized settlement infrastructure is provided for

ESTABLISHED:

> The digital euro is designed as central bank money whose settlement relies on a centralized infrastructure operated by the Eurosystem and distributed to users through payment service providers S22-S23-S24.

This architecture does not rely on a blockchain or DLT infrastructure as the foundation of the system S23.

The user primarily maintains a relationship with their PSP, while the Eurosystem performs the central functions necessary for settlement and the operation of the infrastructure.

Online payments produce structured data

ESTABLISHED:

> The technical model currently published provides for structured data relating to users, accounts, devices, providers, payers, beneficiaries and transactions S25.

Transactions notably have identifiers, an amount, a date and time, a type, an environment and a status.

Certain information also makes it possible to characterize the commercial context.

The Merchant Category Code notably makes it possible to categorize the merchant's activity and is among the information provided for in certain payment flows S25.

This does not mean that the infrastructure systematically knows the exact product purchased or the detailed contents of the basket.

Data is distributed among several actors

ESTABLISHED:

> The architecture does not provide for a single actor to necessarily have all the information relating to a transaction S22-S24-S25.

PSPs know their customers in accordance with their obligations.

The central infrastructure notably uses pseudonymized identifiers and mechanisms intended to prevent the Eurosystem from directly identifying users from the information it receives S22-S23.

The presence of data somewhere in the chain therefore does not mean that it is accessible to all participants.

Offline mode constitutes a distinct architecture

ESTABLISHED:

> The digital euro is also designed to enable offline payments executed directly between the payer's and beneficiary's devices without real-time intervention by the central infrastructure S23-S26.

Under the model currently presented, the personal details of these transactions remain on the devices and are accessible neither to the Eurosystem nor to PSPs.

This architecture therefore constitutes an important limitation on the possibility of systematically matching offline payments with other data at a central level.

The digital euro must not be programmable money

ESTABLISHED:

> The proposed regulation and the European Central Bank explicitly exclude money whose units would intrinsically carry restrictions determining the goods, services, locations, beneficiaries or periods for which they may be used S22-S23-S27.

The digital euro must remain fungible.

Under the framework currently proposed, this safeguard therefore excludes a mechanism in which certain monetary units would be directly programmed to prohibit the purchase of a category of products.

Conditional payments are, however, explicitly provided for

ESTABLISHED:

> The prohibition of programmable money does not prevent the existence of conditional payments whose execution depends on predetermined conditions S27.

The infrastructure notably provides for a functionality enabling funds to be reserved and then transferred when the corresponding condition is considered satisfied.

The ECB therefore distinguishes between:

programming the money → excluded
programming the conditions surrounding a transaction → provided for

This distinction constitutes one of the central findings of the chapter.

Conditional logic can be located outside the Eurosystem

ESTABLISHED:

> The ECB describes a separation between a settlement layer provided by the Eurosystem and a conditionality layer that can be developed by banks, PSPs and other market actors S27-S28.

The external layer can verify that an event or condition has been satisfied and then use the functions provided by the infrastructure to continue processing the payment.

The Eurosystem therefore does not necessarily need to know all the data used to verify that condition.

An external event can contribute to the execution of a payment

ESTABLISHED:

> The ECB's work provides for external monitoring to be able to trigger a condition used by a conditional payment service S27.

The examples examined notably include:

- confirmation of a delivery;
- actual use of a service;
- completion of a milestone;
- certain events related to transport;
- machine-to-machine interactions S27-S28.

The following general principle is therefore established:

```
external system or event
   ↓
verification of a condition
   ↓
conditional service
   ↓
action on the transaction
```

This mechanism has been experimented

ESTABLISHED:

> Market actors have connected their own platforms through APIs to an environment simulating the digital euro interfaces in order to experiment with conditional services and payments S28.

PSPs and other participants were able to develop conditional logic on top of the fundamental functionalities provided by the simulated environment.

The generic bridge between an **external system** and the **conditional processing of a payment** therefore no longer constitutes merely a theoretical architectural possibility.

It has been the subject of technical experiments.

External data do not necessarily need to enter the monetary infrastructure

TECHNICALLY DEDUCIBLE:

> An external system can perform a verification based on its own data and then communicate only the result necessary for the conditional service.

The operation can therefore be:

```
data held in an external system
   ↓
verification of a rule
   ↓
verification result
   ↓
conditional service
   ↓
execution or non-execution of the transaction
```

This architecture means that a potential interconnection does not necessarily require the creation of a central database bringing together all the information concerned.

Digital identity also has an explicit connection with payment

ESTABLISHED:

> The EUDI Wallet is designed to be able to contribute to payment authentication and present verifiable attestations or attributes to the actors concerned S29.

The architecture notably enables the selective disclosure of an attribute without necessarily transmitting the user's entire identity.

Age verification already constitutes a documented example of an attribute that can contribute to a commercial process associated with a payment.

The connection between the EUDI Wallet and the digital euro is explicitly provided for

ESTABLISHED:

> The ECB provides for PSPs participating in the digital euro pilot to be able to use the EUDI Wallet as a strong authentication method for online payments S29.

The following chain is therefore directly documented:

```
digital identity or attestation
   ↓
EUDI Wallet
   ↓
PSP
   ↓
authentication
   ↓
digital euro payment
```

The connection between European digital identity and payment infrastructure therefore does not constitute merely a theoretical possibility.

Several previously separate capabilities can now be represented together

The findings of this chapter make it possible to represent the following general architecture:

```
User
   ↓
verifiable identity / attribute
   ↓
PSP or payment service
   ↓
structured and identifiable transaction
```

in parallel:

```
external system
   ↓
verifiable data or event
   ↓
conditionality layer
```

then:

```
funds reservation
   ↓
condition satisfied or not satisfied
   ↓
settlement or absence of settlement
```

ESTABLISHED:

> Each of the main components of this chain is documented in the architecture or in the experiments examined S22-S24-S25-S27-S28-S29.

TECHNICALLY DEDUCIBLE:

> These components technically make it possible to build services in which information originating from an external system contributes to an automated decision concerning a specific transaction, without making the money itself programmable.

The connection with environmental data remains the missing link

Chapter 3 separately established:

- the existence of the Digital Product Passport;
- the digital identification of products;
- the possibility of associating certain structured environmental data with these products;
- the existence of methods enabling certain environmental footprints to be quantified;
- interoperability mechanisms, APIs and registries;
- the technical possibility of matching a transaction with an identifiable product when the necessary identifiers and access rights exist S15-S18-S19-S20-S21.

Chapter 4 now separately establishes:

- the existence of structured payment transactions;
- funds reservation;
- conditional payments;
- an external conditionality layer;
- the possible use of information originating from external systems;
- APIs enabling market actor platforms to interact with the payment environment;
- and an explicit connection between digital identity and payment S25-S27-S28-S29.

The technical combination can therefore be represented as follows:

```
identifiable product
   ↓
external data associated with the product
   ↓
system capable of verifying a rule
   ↓
verification result
   ↓
conditionality layer
   ↓
transaction
   ↓
execution or non-execution
```

TECHNICALLY DEDUCIBLE:

> If environmental data relating to a product were made accessible to an authorized service and if that data became a valid criterion for a payment condition, the architecture examined would technically enable the result of that verification to be used to act on the execution of a transaction without programming the money itself.

This specific connection is not, however, established

NOT ESTABLISHED:

> None of the elements examined in this chapter demonstrate that data originating from a Digital Product Passport, a GTIN, a carbon footprint, electronic invoicing data or an individual environmental footprint are currently used as a condition for authorizing, refusing or modifying a digital euro payment.

Nor is it established that a French or European administration has a mechanism enabling an individual environmental quota to be automatically applied to a person's purchases.

The technical possibility resulting from the combination of several components must therefore not be presented as an existing or officially planned use.

The current safeguards must be incorporated into this conclusion

Several safeguards currently prevent an interpretation according to which the digital euro would directly constitute a general tool for controlling purchases:

- prohibition of programmable money S22-S27;
- payment conditions presented as agreed between the parties S27;
- pseudonymization and separation of the information accessible to the Eurosystem S22-S23;
- minimization and selective disclosure in the EUDI Wallet S29;
- enhanced privacy for offline payments S23-S26.

ESTABLISHED:

> The framework currently proposed therefore does not give the Eurosystem a general power enabling it to arbitrarily determine the goods and services that a user is authorized to purchase.

These safeguards must not be confused with a technical impossibility

The same sources establish, in parallel, the existence of:

- controls that may lead to the non-execution of certain transactions where a legal basis provides for them;
- quantitative rules automatically applied to holdings;
- conditional payments;
- external services capable of verifying conditions;
- APIs enabling interaction with market platforms;
- verifiable identity attributes that can be used in the payment process S22-S24-S27-S28-S29.

TECHNICALLY DEDUCIBLE:

> The current prohibition of certain uses therefore does not necessarily mean that the infrastructure would be technically incapable of implementing a comparable rule if a legal basis and the corresponding access rights existed.

The distinction between **technical capability** and **legal authority** thus constitutes one of the main conclusions of this chapter.

Conclusion of Chapter 4

The analysis makes it possible to rule out two opposing conclusions.

The first would be to claim that the digital euro already constitutes programmable money enabling an authority to control individual purchases.

The sources examined do not support this claim.

The second would be to claim that the architecture makes it technically impossible to use external data or conditions in the execution of a payment.

The sources examined establish, on the contrary, that such mechanisms exist in the envisaged architecture and have already been the subject of experiments.

The result can therefore be formulated as follows:

ESTABLISHED:

> The digital euro is not designed as programmable money.

ESTABLISHED:

> The infrastructure is nevertheless designed to support conditional payments.

ESTABLISHED:

> The logic determining a condition can be developed outside the Eurosystem by market actors.

ESTABLISHED:

> Information or an event originating from an external system can contribute to the verification of a condition.

ESTABLISHED:

> External platforms have already been connected through APIs to an environment simulating the digital euro in order to experiment with these mechanisms.

ESTABLISHED:

> European digital identity has an official connection with payment infrastructures and its use is explicitly provided for in the digital euro pilot.

TECHNICALLY DEDUCIBLE:

> Information originating from a distinct infrastructure can be verified externally and then used in the form of a result within a conditional service without the source data necessarily being integrated into the monetary infrastructure.

TECHNICALLY DEDUCIBLE:

> The components examined would therefore technically enable data relating to a product or another external characteristic to be used as a criterion for a conditional transaction if an authorized actor had access to that data and a basis permitting its use.

NOT ESTABLISHED:

> None of the elements examined currently demonstrate the use of a DPP, carbon data, electronic invoicing data or an individual environmental profile as a criterion for authorizing or refusing a payment.

TO BE ESTABLISHED:

> Are there actors, projects, standards, infrastructures, calls for tenders or experiments concretely linking electronic invoicing, Digital Product Passport, digital identity and payment systems?

TO BE ESTABLISHED:

> Are there identifiers, APIs or intermediary infrastructures enabling information to circulate or be verified between these different systems?

TO BE ESTABLISHED:

> Are actors participating in the development of the digital euro also involved in DPP, electronic invoicing or environmental data processing infrastructures?

TO BE ESTABLISHED:

> Do European projects currently under development explicitly provide for interoperability between these different infrastructures, even when their initial purposes remain distinct?

Chapter 5 — Interconnections

Navigation: ← Back to the table of contents

This chapter examines existing, planned or experimented interconnections between the infrastructures studied in the previous chapters.

The simultaneous existence of several digital infrastructures does not demonstrate their interconnection.

The analysis therefore looks for elements enabling concrete links between these infrastructures to be identified:

- common standards and identifiers;
- APIs and interoperability mechanisms;
- pilot projects and experiments;
- common consortia and actors;
- partnerships;
- public procurement contracts and calls for tenders;
- explicit references to other infrastructures in technical documentation.

The presence of the same actor in several projects is documented as such but does not, by itself, constitute proof of data exchange between these infrastructures.

An interconnection is classified as **ESTABLISHED** only when a source makes it possible to establish the actual or explicitly planned existence of the connection examined.

Table of contents

5.1 Mapping of already established connections

Status: ESTABLISHED / TECHNICALLY DEDUCIBLE / TO BE ESTABLISHED

The first four chapters separately examined several digital infrastructures relating to economic transactions, products, the environment, identity and payments.

Before looking for new interconnections, it is necessary to distinguish connections that are already established from those that remain only technically possible or still need to be demonstrated.

Electronic invoicing → tax administration

ESTABLISHED:

> The French electronic invoicing reform organizes the automated transmission to the tax administration of structured data relating to invoices, transactions and, in certain situations, payments S1-S2-S3-S4.

For certain B2B transactions, the data transmitted reaches invoice-line level and notably includes the description of the good or service, the quantity and the unit price excluding VAT.

The first connection is therefore directly established:

```
invoice / transaction
   ↓
approved platform
   ↓
tax administration
```

Tax data → economic analysis and public policy management

ESTABLISHED:

> The official objectives of the reform include, beyond combating fraud and pre-filling VAT returns, improving real-time knowledge of economic activity and the management of public policies S5-S6-S14.

The preparatory work also mentions the use of collected data to enrich certain analytical models.

The following connection is therefore also documented:

```
structured economic data
   ↓
processing and analysis
   ↓
knowledge of economic activity / public policy management
```

This does not make it possible to infer that all possible uses of these data would be authorized.

Product → Digital Product Passport

ESTABLISHED:

> The European Digital Product Passport framework makes it possible to associate a product, model or batch with a structured set of digital information through unique identifiers S15-S20.

This information may, depending on the product category and the applicable regulation, include various technical and environmental characteristics.

The following connection is therefore established:

```
identifiable product
   ↓
unique identifier
   ↓
Digital Product Passport
   ↓
structured data relating to the product
```

Product → environmental data

ESTABLISHED:

> Certain European regulations already allow or require quantitative environmental information, notably relating to carbon footprint, to be associated with certain categories of products S15-S18-S19.

The Batteries Regulation constitutes a concrete example of this association.

The connection:

```
identifiable product
   ↓
quantitative environmental data
```

is therefore established for the product categories to which the corresponding obligations apply.

It must not be generalized to all products placed on the market.

DPP → registry, APIs and external systems

ESTABLISHED:

> The Digital Product Passport architecture provides for a European registry, structured identifiers, interoperability mechanisms and interfaces enabling automated data exchange S15-S20.

The DPP registry is now operational and the Commission indicates that it notably relies on documented APIs and a semantic repository intended to facilitate interoperability between systems.

The architecture therefore does not merely constitute a set of digital records intended to be consulted manually.

It is designed to enable structured exchanges between information systems.

Commercial transactions → DPP / traceability

ESTABLISHED:

> European projects have already brought together evidence of commercial transactions, administrative actors responsible notably for VAT and customs, and traceability mechanisms intended to use the Digital Product Passport S21.

The e-Origin project notably makes it possible to store and share evidence of commercial transactions and have it recognized by customs authorities.

Its evolution within the EBSI-ELSA project provides for the development of traceability capabilities using the Digital Product Passport.

This establishes the existence of an institutional connection between several areas previously examined separately:

```
commercial transaction
   ↓
digital evidence of transaction
   ↓
traceability infrastructure
   ↓
administrative / customs actors
```

in parallel:

> development of traceability capabilities using the DPP

NOT ESTABLISHED:

> This project does not demonstrate that DPP data are transmitted to the French tax administration together with electronic invoicing data.

External system → payment condition

ESTABLISHED:

> The envisaged architecture for the digital euro provides for a conditionality layer developed by market actors and capable of using the verification of an event originating from an external system S27-S28.

The ECB explicitly indicates that this architecture enables external monitoring capable of triggering the conditions used in a conditional payment.

The following generic connection is therefore established:

```
external system
   ↓
information or event
   ↓
verification of a condition
   ↓
conditionality layer
   ↓
transaction processing
```

External platform → digital euro environment

ESTABLISHED:

> Market actors have connected their own platforms through APIs to an environment simulating the digital euro interfaces in order to experiment with conditional payments S28.

The scenarios examined notably include payment on delivery, pay-per-use or milestone payments, as well as certain machine-to-machine interactions.

The connection between an external platform and the conditional logic surrounding a payment therefore no longer constitutes merely a theoretical possibility.

It has already been the subject of technical experiments.

Digital identity → payment

ESTABLISHED:

> The European Digital Identity Wallet can contribute to payment authentication and enable the presentation of verifiable attestations or attributes S29.

The wallet notably makes it possible to selectively present certain attributes without necessarily communicating the user's entire identity.

The following connection is therefore established:

```
verifiable identity / attribute
   ↓
EUDI Wallet
   ↓
bank / PSP / acquirer / merchant
   ↓
payment process
```

EUDI Wallet → digital euro

ESTABLISHED:

> The European Central Bank provides for providers participating in the digital euro pilot to be able to use the EUDI Wallet as a strong authentication method for certain online transactions S29.

The following chain is therefore explicitly provided for:

```
EUDI Wallet
   ↓
strong authentication
   ↓
PSP
   ↓
digital euro payment
```

Transaction → product → environmental data

The previous chapters also identified a technically possible connection that requires certain conditions.

An invoice or transaction may contain an identifier enabling the product concerned to be determined.

The Digital Product Passport may also use a product identifier such as a GTIN or equivalent identifier S15-S17.

TECHNICALLY DEDUCIBLE:

> When a common identifier or matching mechanism exists and the necessary access rights are in place, a commercial transaction can technically be matched with the environmental data associated with the corresponding product.

The chain then becomes:

```
transaction
   ↓
identifiable product
   ↓
identifier or matching mechanism
   ↓
DPP or other environmental source
   ↓
environmental data
```

NOT ESTABLISHED:

> The sources examined do not demonstrate that the French tax administration currently performs this matching.

External data → automated decision concerning a payment

The work relating to conditional payments also establishes that an external system does not necessarily need to transfer all its data to the payment system.

It can itself verify a condition and then communicate only the result necessary for the conditional service.

TECHNICALLY DEDUCIBLE:

> Information originating from an external infrastructure can therefore contribute to an automated decision concerning a transaction without the source data necessarily being integrated into the monetary infrastructure.

This principle is important for the investigation of interconnections.

The absence of a central database bringing together all the information is not sufficient to demonstrate the absence of a connection between several infrastructures.

State of the chain after the first four chapters

The established connections can now be represented in simplified form:

```
**Electronic invoicing**
   ↓
structured economic data
   ↓
tax administration / economic analysis

**Identifiable product**
   ↓
Digital Product Passport
   ↓
structured data / environmental data

**Digital identity**
   ↓
EUDI Wallet
   ↓
payment authentication

**External system**
   ↓
verification of a condition
   ↓
conditional payment service

**Market actor platform**
   ↓
API
   ↓
experimental digital euro environment
```

These connections do not yet, by themselves, form a single chain.

Connections that remain to be investigated

After the first four chapters, several questions therefore become much more precise.

TO BE ESTABLISHED:

> Is there an infrastructure explicitly intended to connect invoicing or transaction data with the other European digital infrastructures examined?

TO BE ESTABLISHED:

> Is there a documented connection between the Digital Product Passport and a digital identity or wallet infrastructure used by businesses?

TO BE ESTABLISHED:

> Are electronic invoicing and DPP infrastructures explicitly envisaged as components of the same interoperable ecosystem?

TO BE ESTABLISHED:

> Do identifiers, attestations, APIs or intermediary services enable information to be transported or verified between these different systems?

TO BE ESTABLISHED:

> Are actors or consortia simultaneously involved in the development of product, invoicing, identity and payment infrastructures?

TO BE ESTABLISHED:

> Is there a concrete connection enabling environmental data relating to a product to reach, directly or indirectly, the conditionality layer of a payment service?

Interim conclusion

ESTABLISHED:

> Several connections between the infrastructures examined are already explicitly documented: invoicing to tax administration, product to DPP, DPP to interoperable systems, digital identity to payment, EUDI Wallet to the digital euro pilot, and external system to conditional payment.

ESTABLISHED:

> External platforms have already interacted through APIs with an environment simulating the digital euro in order to experiment with conditional services.

TECHNICALLY DEDUCIBLE:

> When an identifier or matching mechanism exists, a transaction involving an identifiable product can technically be matched with the corresponding environmental information.

NOT ESTABLISHED:

> None of the elements examined so far demonstrate an operational chain directly connecting French electronic invoicing data, the Digital Product Passport or environmental data to the decision to authorize or refuse a payment.

The chapter must now investigate the intermediary infrastructures capable of connecting these different systems.

The first of these appears in the European Commission's recent work: the **European Business Wallet**.

5.2 European Business Wallets: identity, invoicing and transaction data

Status: ESTABLISHED / ONGOING PROJECT / TO BE ESTABLISHED

In November 2025, the European Commission proposed the creation of **European Business Wallets**, a digital infrastructure intended for economic operators and public bodies S30.

Unlike the EUDI Wallet examined in Chapter 4, which is primarily oriented toward the digital identity of natural persons, the Business Wallet is designed to enable businesses and other economic operators to interact digitally with other businesses and public administrations.

It therefore constitutes a new intermediary infrastructure between several areas examined separately in the previous chapters.

An identification and data exchange infrastructure for businesses

ESTABLISHED:

> European Business Wallets are intended to enable economic operators to identify and authenticate themselves and securely exchange verifiable electronic data, documents and attestations with other economic actors and public administrations S30.

The system therefore does not merely constitute a wallet intended to store documents.

It is also intended to provide an interoperable digital exchange layer between organizations.

The general chain can be represented as follows:

```
business
   ↓
European Business Wallet
   ↓
identification / authentication / verifiable attestations
   ↓
recipient business or administration
```

Business Wallet → EUDI Wallet

The Business Wallet is built on the European digital identity framework.

The proposal notably provides for European Digital Identity Wallets and electronic attestations of attributes to be used for onboarding and access management for European Business Wallets S30.

ESTABLISHED:

> An explicit connection is therefore provided for between the EUDI infrastructure examined in Chapter 4 and European Business Wallets S30.

The chain becomes:

```
EUDI Wallet / electronic attestation
   ↓
authentication and access management
   ↓
European Business Wallet
```

This relationship is particularly important since Chapter 4 has already separately established a connection between the EUDI Wallet and payment infrastructures.

It does not, however, demonstrate that data contained in a Business Wallet are automatically transmitted to a payment system.

Tax and economic identifiers can be used as attributes

The proposal mentions several attributes that can be issued or verified through Business Wallets S30.

Examples notably include:

- VAT identification number;
- tax identification number;
- Legal Entity Identifier (LEI);
- EORI number used in the customs field;
- excise number.

ESTABLISHED:

> The Business Wallet is therefore explicitly designed to handle attributes enabling a business to be legally, fiscally or economically identified S30.

This creates an infrastructure capable of circulating verifiable evidence concerning the same entity across several administrative and economic contexts.

Business Wallet → ViDA → electronic invoicing

The proposal establishes a particularly important connection with **VAT in the Digital Age (ViDA)** S30.

ViDA modernizes the European VAT system and notably provides for the development of electronic invoicing and digital reporting.

The Commission indicates that European Business Wallets could enable the secure storage and verifiable exchange of VAT-related attestations and **transaction data**, in order to support real-time reporting and trusted invoicing S30.

ESTABLISHED:

> The Commission therefore explicitly provides for a connection between European Business Wallets, transaction data, VAT, digital reporting and electronic invoicing S30.

The following chain is no longer merely deducible:

```
business
   ↓
European Business Wallet
   ↓
VAT attestations / transaction data
   ↓
ViDA
   ↓
digital reporting / electronic invoicing
```

This is an institutional connection explicitly described in the Commission's proposal.

The Business Wallet is not limited to interactions with public administrations

The infrastructure must be usable in relationships between businesses as well as in interactions between businesses and public administrations S30.

ESTABLISHED:

> The same trusted environment is therefore designed to enable B2B and B2G exchanges.

This characteristic is important for the study of interconnections.

A verifiable attestation or data item can be used in several economic relationships without requiring the creation of a different infrastructure for each administration or business partner.

This does not, however, mean that data communicated in one context automatically become accessible in all others.

Access rights and purposes remain decisive.

The Business Wallet constitutes an intermediary layer

The infrastructures examined so far could appear to belong to separate domains:

- identity
- taxation
- invoicing
- customs
- products
- public administrations
- commercial transactions

The Business Wallet proposal specifically adopts a cross-cutting approach.

It provides a common infrastructure for identification, attestations and secure exchange, enabling different systems to communicate with the same economic operator S30.

ESTABLISHED:

> The European Union is therefore explicitly developing an infrastructure intended to facilitate interoperability between several previously distinct administrative and economic systems S30.

An important connection with our previous mapping

After Chapter 4, the following chain was already documented:

```
EUDI Wallet
   ↓
authentication
   ↓
payment infrastructures
```

The Business Wallet now adds another officially planned branch:

```
EUDI Wallet / European identity
   ↓
European Business Wallet
   ↓
business identity / verifiable attributes
   ↓
VAT / transaction data / invoicing / reporting
```

ESTABLISHED:

> The European identity infrastructure therefore now constitutes a documented common point between, on the one hand, mechanisms for identifying economic operators and invoicing and, on the other hand, the payment infrastructures examined in the previous chapter.

This finding is not sufficient to demonstrate a direct exchange of data between invoicing and payment.

It does, however, establish that these domains no longer necessarily rely on completely independent infrastructures.

An interconnection does not necessarily require a common central database

The envisaged operation relies on attestations, identifiers and verifiable exchanges between actors.

A business can therefore prove information to another system without a single central database necessarily bringing together all the information concerned.

This principle is consistent with several architectures examined previously:

```
information held by one system
   ↓
attestation or verifiable proof
   ↓
presentation to another system
   ↓
verification
   ↓
use of the result
```

TECHNICALLY DEDUCIBLE:

> Interoperability between several infrastructures can therefore rely on the exchange of attestations and verifiable proofs rather than on the centralization of all data in a common database.

What this connection does not demonstrate

The existence of European Business Wallets does not make it possible to claim that:

- French electronic invoicing data will automatically be copied into a Business Wallet;
- all transaction data will be accessible to all public administrations;
- information held in a Business Wallet will automatically be transmitted to a bank or the Eurosystem;
- environmental data will be used as a payment condition;
- the EUDI Wallet alone will make it possible to nominally link all economic transactions of a business or person.

NOT ESTABLISHED:

> None of the elements examined demonstrate at this stage an automatic transmission of invoicing or transaction data contained in or verified by a Business Wallet to the conditionality layer of a digital euro payment.

But the institutional separation between several infrastructures is narrowing

The result of this section is nevertheless important.

Before examining European Business Wallets, the infrastructures relating to identity, invoicing, tax data and payments could still be represented as several systems with essentially separate connections.

The Commission's proposal introduces a cross-cutting infrastructure specifically intended to enable the identification of operators and the secure exchange of data and attestations between several of these environments.

ESTABLISHED:

> European Business Wallet ↔ EUDI Wallet S30

ESTABLISHED:

> European Business Wallet ↔ business identity and tax attributes S30

ESTABLISHED:

> European Business Wallet ↔ ViDA S30

ESTABLISHED:

> European Business Wallet ↔ VAT attestations S30

ESTABLISHED:

> European Business Wallet ↔ transaction data S30

ESTABLISHED:

> European Business Wallet ↔ digital reporting / trusted invoicing S30

These connections are explicitly described in the Commission's documents.

Interim conclusion

ESTABLISHED:

> European Business Wallets are designed as a cross-cutting infrastructure enabling businesses and public administrations to identify and authenticate themselves and exchange verifiable data and attestations S30.

ESTABLISHED:

> Their architecture is explicitly connected to the EUDI framework and enables the use of verifiable tax and economic attributes S30.

ESTABLISHED:

> The Commission explicitly provides for their connection with ViDA as well as the storage and verifiable exchange of VAT attestations and transaction data in order to support real-time reporting and trusted invoicing S30.

TECHNICALLY DEDUCIBLE:

> This infrastructure therefore provides an intermediary mechanism enabling several economic and administrative systems to verify and reuse certain information relating to the same business without requiring a common central database.

NOT ESTABLISHED:

> None of the elements examined yet demonstrate that data originating from this infrastructure are used to condition a digital euro payment.

Another connection must now be examined.

The Commission also explicitly associates European Business Wallets with the **Digital Product Passport**.

5.3 Business Wallets, Digital Product Passport and European infrastructures

Status: ESTABLISHED / ONGOING PROJECT / TECHNICALLY DEDUCIBLE / TO BE ESTABLISHED

The analysis of European Business Wallets reveals an additional connection with the Digital Product Passport examined in Chapter 3.

This connection does not result solely from the technical compatibility of the two infrastructures.

The European Business Wallets proposal explicitly mentions the Digital Product Passport among the systems with which synergies are sought S30.

The European Single Market Strategy goes further by presenting the Digital Product Passport, eInvoicing, the future European Business Wallet and several other infrastructures as components of the same coherent ecosystem of digital solutions intended to create synergies S31.

Business Wallet → Digital Product Passport

The proposed regulation on European Business Wallets explicitly describes their connection with the Digital Product Passport S30.

The Commission notes that the DPP depends on reliable access to data relating notably to product compliance and sustainability.

It indicates that Business Wallets can notably:

- prove the legal identity of an economic operator;
- prove the access rights granted to it;
- enable the signing and sealing of declarations of conformity;
- enable the secure and verifiable exchange of product-related data between different actors and Member States S30.

ESTABLISHED:

> The Commission explicitly provides for a connection between European Business Wallets and the Digital Product Passport in order to enable the identification of operators, the verification of access rights and the secure and verifiable exchange of product-related data S30.

The following chain is therefore documented:

```
economic operator
   ↓
European Business Wallet
   ↓
legal identity / access rights
   ↓
Digital Product Passport
   ↓
compliance / sustainability / product data
```

The connection notably concerns sustainability data

This point is particularly important for the purpose of this investigation.

The connection between the Business Wallet and the DPP is not presented solely as a mechanism for identifying a business.

The Commission explicitly mentions access to **compliance and sustainability data** associated with the Digital Product Passport S30.

ESTABLISHED:

> The Business Wallet infrastructure is therefore explicitly envisaged as a mechanism that can contribute to secure and verifiable access to sustainability data associated with products in the DPP ecosystem S30.

This does not mean that all environmental data relating to a product are automatically transferred into the Business Wallet.

The wallet can notably act as an infrastructure enabling identity, access rights and the authenticity of exchanges to be proven.

Business Wallet → DPP and Business Wallet → ViDA

The previous section separately established:

```
European Business Wallet
   ↓
ViDA
   ↓
VAT attestations / transaction data / reporting / invoicing
```

The present section now establishes:

```
European Business Wallet
   ↓
Digital Product Passport
   ↓
product / compliance / sustainability data
```

ESTABLISHED:

> The same European infrastructure is therefore explicitly connected, on the one hand, with transaction and invoicing data and, on the other hand, with the Digital Product Passport and its product-related data S30.

This finding constitutes an institutional connection between two sets of systems examined separately in the previous chapters.

It does not yet demonstrate that a specific data item from an invoice is automatically matched with a specific data item from a DPP.

The Commission presents these infrastructures as part of the same digital ecosystem

The Single Market Strategy adopted in May 2025 makes it possible to go beyond the mere observation that several European projects are developing in parallel S31.

The Commission notably groups together:

- the Single Digital Gateway;
- the Once-Only Technical System;
- the Digital Product Passport;
- eInvoicing;
- the future European Business Wallet;
- the Business Register Interconnection System;
- the European Unique Identifier for companies;
- as well as other initiatives intended to simplify data exchange and digital reporting S31.

It indicates that these tools should collectively constitute a **coherent ecosystem of digital solutions** and create synergies facilitating economic activities within the European Union S31.

ESTABLISHED:

> The European Commission therefore does not present the DPP, eInvoicing and the Business Wallet as necessarily isolated infrastructures: it explicitly places them within the same digital ecosystem intended to create synergies S31.

This point changes the qualification of the analysis.

The existence of convergence between these infrastructures is no longer merely a deduction based on their technical compatibility.

ESTABLISHED:

> An institutional strategy of interoperability and the creation of synergies between several of these infrastructures is explicitly documented S31.

---

eInvoicing → data reuse

The strategy also identifies an obstacle to the full automation of economic processes: the limited reuse of data from electronic invoicing in other processes S31.

The Commission is therefore explicitly seeking to increase this reuse.

Its documentation relating to eInvoicing indicates that electronic invoicing should enable the automation of a broader set of processes, notably including:

- VAT reporting;
- certain customs procedures;
- environmental, social and governance, or ESG, reporting S31.

ESTABLISHED:

> Electronic invoicing data are therefore not envisaged solely for producing, transmitting and recording an invoice: their reuse in other digital processes is explicitly part of the European strategy S31.

---

eInvoicing → sustainability reporting

More specifically, the Commission plans to test the reuse of data from eInvoicing for **sustainability reporting** S31.

ESTABLISHED / PLANNED PROJECT:

> The European strategy provides for a pilot dedicated to the reuse of electronic invoicing data for sustainability reporting S31.

This connection is particularly important for the mapping examined in this investigation.

Until now, the following relationship was only technically deducible:

```
transaction data
   ↓
product
   ↓
environmental data
```

The strategy now introduces an additional institutional connection:

```
eInvoicing data
   ↓
reuse
   ↓
sustainability reporting
```

This does not mean that an individual carbon footprint is calculated from invoices.

It does, however, establish that the reuse of invoicing data for sustainability-related purposes is explicitly part of the work announced by the Commission.

---

eInvoicing → customs data

The same strategy also provides for improving customs transparency by linking eInvoicing data with customs data, in line with the development of the EU Customs Data Hub S31.

ESTABLISHED / PLANNED PROJECT:

> The Commission explicitly provides for a connection between electronic invoicing data and customs data S31.

The chain becomes:

```
eInvoicing
   ↓
structured transaction data
   ↓
connection with customs data
   ↓
EU Customs Data Hub
```

This connection is consistent with the elements examined in Chapter 3 relating to traceability infrastructures, the DPP and customs systems.

It does not, however, demonstrate that all these data are already brought together within the same system.

Several previously hypothetical connections become institutionally documented

After Sections 5.2 and 5.3, the mapping can now be expanded:

```
EUDI / digital identity
   ↓
European Business Wallet
```

```
European Business Wallet
   ↓
ViDA / VAT / transaction data / invoicing
```

```
European Business Wallet
   ↓
Digital Product Passport / product / compliance / sustainability data
```

```
eInvoicing
   ↓
planned reuse for sustainability reporting
```

```
eInvoicing
   ↓
planned connection with customs data
```

```
DPP + eInvoicing + Business Wallet + other infrastructures
   ↓
coherent digital ecosystem and creation of synergies
```

ESTABLISHED:

> The Commission's documents therefore now establish explicit institutional links between several infrastructures examined separately in the previous chapters S30-S31.

What this changes in the investigation

At the end of Chapter 3, the connection between transaction data and environmental data was primarily based on a technical possibility:

```
identify the product in a transaction
   ↓
retrieve its DPP
   ↓
access the corresponding environmental data
```

The elements examined in this section now add three distinct facts:

ESTABLISHED:

> The Commission provides for a connection between the Business Wallet and the DPP for identity, access rights and the secure exchange of product data, notably compliance and sustainability data S30.

ESTABLISHED:

> The same Business Wallet infrastructure is connected with ViDA, VAT attestations and transaction data S30.

ESTABLISHED / PLANNED PROJECT:

> The Commission plans to directly test the reuse of eInvoicing data for sustainability reporting S31.

The proximity between transaction data and sustainability data is therefore no longer merely the result of a theoretical combination made in this investigation.

ESTABLISHED:

> The European Commission is explicitly working on the reuse and interoperability of these categories of data within a common digital ecosystem S30-S31.

What this still does not demonstrate

These elements do not make it possible to claim that:

- each invoice line will automatically be matched with a DPP;
- each purchased product will be associated with its carbon footprint in a central database;
- an administration will calculate an individual environmental footprint from invoices;
- sustainability data will be transmitted to banks or the Eurosystem;
- environmental data from a DPP will be used as a condition for a payment;
- the envisaged sustainability reporting concerns an individual environmental profile of consumers.

NOT ESTABLISHED:

> The specific connection between environmental data relating to a product and the conditionality layer of a payment remains to be demonstrated.

An institutional chain nevertheless emerges

Without turning the preceding elements into evidence of a use that is not documented, a more precise institutional chain can now be represented:

```
eInvoicing / transaction data
   ↓
planned data reuse
   ↘ sustainability reporting
     ↘ **customs data / EU Customs Data Hub
```

in parallel:

```
      European Business Wallet
    ↙                         ↘
ViDA / transaction     DPP / product / sustainability
```

all of which is placed by the Commission within:

a coherent ecosystem of digital solutions intended to create synergies

ESTABLISHED:

> The existence of a strategy for connecting and reusing data between several of these infrastructures is now explicitly documented S30-S31.

TECHNICALLY DEDUCIBLE:

> An infrastructure capable of identifying the operator, verifying its access rights and exchanging product data can serve as an interoperability layer between transaction systems and systems containing sustainability information, when the applicable rules authorize such an exchange.

Interim conclusion

ESTABLISHED:

> European Business Wallets are explicitly connected with the Digital Product Passport and can contribute to the identification of operators, the verification of access rights and the secure and verifiable exchange of product-related data, notably compliance and sustainability data S30.

ESTABLISHED:

> European Business Wallets are also connected with ViDA, VAT attestations and transaction data S30.

ESTABLISHED:

> The Commission places the DPP, eInvoicing, the Business Wallet and several other infrastructures within the same coherent ecosystem of digital solutions intended to create synergies S31.

ESTABLISHED / PLANNED PROJECT:

> The Commission plans to test the reuse of eInvoicing data for sustainability reporting S31.

ESTABLISHED / PLANNED PROJECT:

> The Commission also plans to connect eInvoicing data with customs data in relation to the EU Customs Data Hub S31.

TECHNICALLY DEDUCIBLE:

> These mechanisms reduce the technical and institutional distance between data describing a transaction, data describing a product and data relating to its sustainability.

NOT ESTABLISHED:

> None of the elements examined yet demonstrate that environmental data originating from a DPP are transmitted to a payment infrastructure in order to authorize or refuse a transaction.

The question is therefore no longer merely whether these infrastructures can communicate.

The Commission itself documents their interoperability, their reuse and the synergies being pursued.

It remains to determine **through which identifiers, standards and APIs these connections can concretely be implemented**.

5.4 Common identifiers, standards and APIs

Status: ESTABLISHED / TECHNICALLY DEDUCIBLE / TO BE ESTABLISHED

The previous sections established that the European Commission is explicitly seeking synergies between several digital infrastructures relating to invoicing, businesses, products and their sustainability.

The existence of an intention to achieve interoperability is not, however, sufficient to demonstrate that data can actually be matched.

For an interconnection to work, several technical conditions generally need to be met: systems must be able to identify the objects or actors concerned, understand the data exchanged, verify access rights and have interfaces enabling automated exchanges.

The infrastructures examined already have several of these components.

---

eInvoicing → common semantic model

ESTABLISHED:

> The European EN 16931 standard defines a common semantic model enabling issuing and receiving systems to automatically understand and process the information contained in an electronic invoice S32.

The purpose of the standard is precisely to reduce differences between national formats and systems in order to enable interoperability.

The general technical chain is therefore:

```
invoicing system A
   ↓
data structured according to a common semantic model
   ↓
invoicing system B
```

The data are no longer intended solely to be read by a person.

They are structured so that they can be automatically interpreted by different systems.

EN 16931 is evolving toward other data uses

European standardization work no longer concerns only the traditional exchange of an invoice between supplier and customer.

The 2026 European standardization plan provides for keeping EN 16931 aligned with ViDA and integrating requirements arising from various European policies.

The areas explicitly mentioned include:

- tax reporting;
- sustainability reporting;
- customs;
- other automated processes.

ESTABLISHED:

> The evolution of the European invoicing standard explicitly takes into account requirements arising from tax reporting, sustainability reporting and customs procedures S32.

This evolution is consistent with the eInvoicing data reuse projects identified in the previous section.

It does not mean that all the data required for these uses are already present in every invoice.

DPP → unique and persistent product identifier

The European Ecodesign Regulation requires a Digital Product Passport to be linked to a **unique and persistent product identifier** S15-S32.

This identifier is associated with a data carrier providing access to the passport.

ESTABLISHED:

> The DPP therefore relies on a mechanism enabling different systems to persistently identify the same product, model or batch according to the applicable rules S15-S32.

The chain is:

```
product
   ↓
unique and persistent identifier
   ↓
Digital Product Passport
```

This mechanism constitutes an essential condition for any automated matching between a physical product and its digital information.

DPP → open standards and interoperable data

The regulation also requires Digital Product Passport data to rely on open standards and, depending on the case, to be:

- machine-readable;
- structured;
- searchable;
- transferable;
- accessible through an open and interoperable data exchange network S15-S32.

ESTABLISHED:

> DPP interoperability is therefore a regulatory requirement of its architecture and not merely an optional feature S15-S32.

The system is designed to enable the automated use of data by different authorized actors.

The DPP registry has an API

Implementing Regulation (EU) 2026/1778 specifies the architecture of the European Digital Product Passport registry S20-S32.

The registry notably includes:

- a secure user interface;
- an API enabling the registration of Digital Product Passports and the receipt of information from the registry;
- a verification platform;
- a user identification and authorization mechanism;
- a system generating unique registration identifiers;
- a semantic repository;
- a logging system S20-S32.

ESTABLISHED:

> The DPP registry therefore has a machine-to-machine interface explicitly designed to enable automated interactions with other systems S20-S32.

The following chain is directly provided for:

```
authorized external system
   ↓
API
   ↓
DPP registry
   ↓
registration / verification / information
```

The semantic repository facilitates understanding between systems

The DPP registry also includes a semantic repository intended to authoritatively define the meaning, structure, versions and interoperability requirements of passport data S20-S32.

ESTABLISHED:

> The system therefore does not merely provide a technical interface for transmitting data; it also provides a semantic layer enabling systems to consistently understand the information exchanged S20-S32.

Two conditions necessary for automated interconnection are thus met:

```
common technical interface
   +
common semantic understanding
```

The registry associates a product with a verified economic operator

The implementing regulation also requires the verification of economic operators and other value-chain actors interacting with the registry S20-S32.

When a DPP is registered, the registry can notably associate:

- the unique product identifier;
- the identity of the verified economic operator responsible;
- certain information necessary for registration;
- a unique registration identifier S20-S32.

Electronic proof of registration can also be generated.

ESTABLISHED:

> The DPP registry therefore establishes a verifiable relationship between an identifiable product and an identifiable economic operator S20-S32.

The chain becomes:

```
verified economic operator
   ↓
identifiable product
   ↓
DPP
   ↓
registration identifier / verifiable proof
```

Digital identity mechanisms can contribute to operator verification

The implementing regulation provides for several mechanisms enabling the identity of economic operators to be verified.

These notably include, depending on the circumstances, electronic identification means compliant with the eIDAS framework as well as electronic attestations of attributes S20-S32.

ESTABLISHED:

> The DPP infrastructure and the European digital identity infrastructure therefore share mechanisms enabling the identification or verification of economic operators S20-S32.

This does not yet necessarily constitute a direct connection with the EUDI Wallet in every situation.

But the use of the same European identity and attestation framework facilitates interoperability between these environments.

Business Wallet → verifiable attestations

European Business Wallets also rely on verifiable electronic data and attestations S30-S32.

These attestations can represent various attributes relating to the business, its representatives, its roles or its authorizations.

The architecture notably provides for:

- structured attribute formats;
- verification mechanisms;
- management of mandates and delegations;
- access controls;
- traceability of authorizations;
- cryptographically verifiable proofs S30-S32.

ESTABLISHED:

> Exchanges between infrastructures therefore do not rely solely on the transmission of raw data but can also rely on the presentation and verification of digital attestations S30-S32.

Business Wallet → interoperable access control

The proposal provides for mechanisms enabling real-time determination of whether an actor has the necessary rights to access data or perform a procedure S30-S32.

Authorizations must notably be:

- verifiable;
- auditable;
- revocable;
- traceable to their issuer;

- usable interoperably across Member States.

ESTABLISHED:

> The interoperability being pursued therefore also concerns the rights enabling access to data and services, and not only data formats S30-S32.

This point is essential for the analysis of interconnections.

A system may technically have an API providing access to data while preventing that access when the actor does not have the corresponding authorization.

Business Wallet → European Digital Directory → API

The European Business Wallets proposal also provides for the creation of a **European Digital Directory** S30-S32.

This directory is intended to include two interfaces:

- a portal intended for users;
- a machine-readable interface exposed through an API for automated communications between systems.

ESTABLISHED:

> The Business Wallet ecosystem therefore also provides for a machine-to-machine interface enabling automated discovery and interaction between actors and systems S30-S32.

The general structure becomes:

```
actor / system
   ↓
European Digital Directory
   ↓
API
   ↓
identification / discovery / interaction with the relevant actor
```

The same technical principles appear across several infrastructures

The systems examined do not necessarily rely on the same databases or on a single universal identifier.

They nevertheless use converging technical principles:

Infrastructure	Identification	Structured data	Semantics	API / automated exchange	Authorization
eInvoicing	businesses / transaction references	yes	EN 16931	electronic exchanges	depending on systems
DPP	product / operator	yes	semantic repository	registry API	yes
Business Wallet	business / roles / mandates	yes	attestations / vocabularies	API / interfaces	yes
EUDI	person / attributes	yes	verifiable attestations	exchange protocols	yes
digital euro	users / PSPs / transactions	yes	data model	payment interfaces	yes

ESTABLISHED:

> Several European infrastructures therefore simultaneously use structured identifiers, automatically interpretable data models, authorization mechanisms and interfaces intended for machine-to-machine exchanges S20-S25-S29-S30-S32.

The European Union explicitly seeks interoperability between these systems

This technical convergence is not merely accidental.

More broadly, the Commission indicates that it seeks to ensure cross-border interoperability between public digital solutions such as:

- eInvoicing;
- electronic signatures;
- electronic submissions;
- the Digital Product Passport.

At the same time, it presents the European Business Wallet as a central element enabling businesses to interact digitally with public administrations.

ESTABLISHED:

> The European strategy explicitly seeks interoperability between several categories of systems examined in this investigation S30-S31-S32.

Semantic convergence is also underway for Business Wallets

Technical work relating to European Business Wallets now includes the development of a semantic vocabulary for electronic attestations used across the different use cases.

This work notably relies on verifiable credential standards and formats intended to enable attribute interoperability.

ESTABLISHED / ONGOING WORK:

> The development of the Business Wallet ecosystem therefore also includes a layer intended to harmonize the meaning of data and attributes exchanged between systems.

This development brings its operation closer to the principle already observed in EN 16931 and in the DPP semantic repository.

Is there a universal identifier automatically connecting all infrastructures?

At this stage, the sources examined do not establish the existence of a single universal identifier that would simultaneously be present in:

```
invoice
   +
DPP
   +
Business Wallet
   +
identity
   +
payment
```

NOT ESTABLISHED:

> No universal identifier enabling all the infrastructures examined to be automatically joined has been identified.

This absence is important.

It prevents any claim that complete matching would be automatic or systematic.

A universal identifier is not, however, technically essential

An interconnection between systems does not necessarily require all of them to use exactly the same identifier.

Matching mechanisms can link multiple identifiers.

For example:

```
business identifier in system A
   ↓
identity or verifiable attestation
   ↓
matching with the business in system B
```

or:

```
product reference in a transaction
   ↓
matching mechanism
   ↓
unique DPP identifier
   ↓
product-related information
```

TECHNICALLY DEDUCIBLE:

> Attestations, registries or intermediary services can make it possible to resolve matches between multiple systems without requiring a universal identifier common to the entire architecture.

This is precisely one of the functions that identity infrastructures, registries or interoperability services can perform.

A single common API is no more necessary

The same distinction applies to interfaces.

It is not necessary for a single API to directly connect:

> invoicing → DPP → Business Wallet → payment

A distributed architecture can operate as follows:

```
system A
   ↓ API
intermediary service
   ↓ API
system B
   ↓ verifiable result
system C
```

This logic is already observed in the architectures examined previously.

TECHNICALLY DEDUCIBLE:

> The absence of a single API directly connecting all the infrastructures does not, by itself, make it possible to conclude that there is no interconnection.

The question of access rights remains decisive

The technical possibility of matching multiple data points does not mean that such matching is legally or operationally authorized.

The DPP, EUDI and Business Wallet architectures specifically include mechanisms intended to control access rights and the information that may be communicated.

ESTABLISHED:

> Technical interoperability and authorization to access data are two distinct questions S20-S29-S30-S32.

A chain may therefore be technically feasible while remaining legally prohibited or inaccessible to certain actors.

What this section now makes it possible to establish

After the previous sections, it was established that the Commission was seeking synergies between several infrastructures.

This section shows that the main technical components enabling such synergies to be implemented also exist:

```
**identifiers**
   ↓
identify actors, products and transactions
**semantic models**
   ↓
automatically understand the data
**verifiable attestations**
   ↓
prove information without necessarily transferring all the source data
**authorization mechanisms**
   ↓
determine who can access what
**APIs and machine-to-machine interfaces**
   ↓
enable automated exchanges
**registries and directories**
   ↓
find and verify actors, products or services
```

ESTABLISHED:

> These components exist in several of the infrastructures examined and are explicitly being developed with interoperability in mind S20-S30-S32.

Interim conclusion

ESTABLISHED:

> eInvoicing relies on a common European semantic model intended to enable the automated and interoperable processing of invoices S32.

ESTABLISHED:

> The DPP relies on unique persistent identifiers, structured and interoperable data, an API, a semantic repository, and identification and authorization mechanisms S15-S20-S32.

ESTABLISHED:

> European Business Wallets rely on verifiable attestations, interoperable authorization mechanisms and interfaces intended for automated communications between systems S30-S32.

ESTABLISHED:

> European standardization policies explicitly seek to align eInvoicing with requirements relating notably to tax reporting, sustainability reporting and customs S32.

TECHNICALLY DEDUCIBLE:

> The components necessary to build automated bridges between several infrastructures therefore exist: identification, matching resolution, common semantics, access control, verifiable attestations and APIs.

NOT ESTABLISHED:

> No universal identifier or single API automatically connecting invoicing, the DPP, identity and payment is established by the sources examined.

The search for an interconnection therefore cannot be limited to looking for a single database, identifier or API.

A distributed architecture can connect multiple systems through intermediary services, attestations, identifier matching and successive interfaces.

The next step is therefore to determine whether **the same actors, consortia and pilot projects are actually involved in several of these infrastructures**.

5.5 Common actors, consortia and experiments

Status: ESTABLISHED / INDICATION OF INTERCONNECTION / TO BE ESTABLISHED

The presence of common actors across several infrastructures does not, by itself, demonstrate that data circulate between those infrastructures.

It is nevertheless a relevant element when these actors are concretely involved in the design, integration or experimentation of several systems examined in this investigation.

The analysis of European projects relating to the digital euro, digital identity and Business Wallets shows that this work is not conducted solely by public institutions independently of one another.

It also involves banks, payment service providers, technology companies, economic operators, wallet providers and integrators operating across several ecosystems S33.

Digital Euro Innovation Platform → private actors

In 2025, the European Central Bank created an innovation platform bringing together around 70 market participants to experiment with features and use cases relating to the digital euro S28-S33.

The participants notably include:

- banks;
- payment service providers;
- fintechs;
- technology companies;
- commerce actors;
- providers of digital infrastructures and services.

ESTABLISHED:

> The design and experimentation of services that could be developed around the digital euro therefore directly involve private actors from several economic sectors S28-S33.

These actors are therefore not limited to observing the project.

As part of the "pioneers" workstream, they were able to connect their own platforms to the simulated environment provided by the ECB in order to experiment with various functionalities S28.

Several major financial and technology actors are participating in digital euro experimentation

The list published by the ECB notably includes:

- Accenture;
- CaixaBank;
- equensWorldline;
- KPMG;
- SAP Fioneer;
- Tata Consultancy Services;
- Infineon;
- several European banks and payment service providers S33.

A consortium called **Digi-Trade** is also participating in both workstreams of the Innovation Platform.

It brings together:

- Amazon;
- CargoX;
- Deutsche Bank;

- Stripe;
- Swift S33.

ESTABLISHED:

> Major actors in e-commerce, banking, payments, financial messaging and technology infrastructures are therefore jointly participating in the experimentation of services relying on the digital euro environment S33.

This participation does not demonstrate that their existing commercial infrastructures will automatically be connected to the digital euro.

It does, however, establish that they have direct access to the experimental work enabling the assessment and development of future services around this infrastructure.

WE BUILD → a cross-sector consortium

The **WE BUILD** Large Scale Pilot constitutes another important element S33.

This European project brings together more than 200 organizations from several dozen countries.

It notably includes:

- public authorities;
- business registries;
- tax administrations;
- banks and financial institutions;
- wallet and trust service providers;
- technology companies;
- SMEs;
- research organizations S33.

ESTABLISHED:

> The same European consortium therefore brings together public, tax, financial, technological and economic actors to develop and test interoperable infrastructures relying on the EUDI Wallet and European Business Wallets S33.

WE BUILD does not deal solely with identity

Official documentation relating to the Large Scale Pilots presents WE BUILD as a project dedicated to use cases relating to businesses **and payments** S33.

Its architecture divides the work into several domains.

These notably include:

Business
business identity / representation / data sharing

Supply Chain
processes relating to supply chains and electronic invoicing

Payments & Banking
secure payments / banking services / financial onboarding S33

ESTABLISHED:

> Use cases relating to electronic invoicing and use cases relating to payments and banking services are therefore being developed within the same European Large Scale Pilot and the same general interoperability architecture S33.

This finding does not demonstrate that an invoice is used as a condition for a payment.

It does, however, establish that both domains are being experimented with within the same technical program.

Business Wallet → supply chain → eInvoicing

The WE BUILD architecture blueprint explicitly mentions electronic invoicing among the processes covered in the Supply Chain domain S33.

The same project is also developing mechanisms relating to:

- business identity;
- mandates and representation;
- data sharing;
- relationships between buyers and suppliers;
- payments and banking services.

ESTABLISHED:

> Electronic invoicing, business identity, data sharing and payments are therefore no longer examined solely in separate European programs: they also appear as different use cases within the same experimental environment S33.

WE BUILD → tax administrations

The consortium also includes tax administrations S33.

The Finnish Tax Administration, for example, states that it is directly participating in WE BUILD to experiment with:

- the transmission of tax information through wallets;
- cross-border VAT declarations;
- the issuance and receipt of digital tax documents;
- various processes requiring tax attestations.

ESTABLISHED:

> Tax administrations are therefore directly participating in the experimentation of Business Wallets and the use of tax data and digital attestations within this environment S33.

The experimental chain thus includes:

```
business
   ↓
Business Wallet
   ↓
tax data / attestation
   ↓
tax administration
```

WE BUILD → payments

WE BUILD also includes work specifically dedicated to payments.

In 2026, the consortium created a dedicated payments community to present and discuss the technical solutions being experimented with around EUDI Wallets and Business Wallets for payments and banking services S33.

ESTABLISHED:

> EUDI Wallets and Business Wallets are therefore actually being experimented with in use cases relating to payments and banking services within the consortium S33.

The work notably covers regulatory requirements, standards, technical architectures and interactions with financial institutions and payment service providers.

Some actors appear in several environments

Analysis of the participants makes it possible to identify several overlaps between the ecosystems.

CaixaBank participates in the ECB's Digital Euro Innovation Platform S33.

The bank also appears in WE BUILD consortium work and events dedicated to wallets and payments.

Worldline, through equensWorldline, participates in the Digital Euro Innovation Platform S33.

The group also participates in Large Scale Pilots relating to the EUDI Wallet, notably WE BUILD, in work related to payments.

These overlaps can be represented as follows:

```
Digital Euro Innovation Platform
   ↕
banking actors / PSPs / integrators
   ↕
EUDI / WE BUILD
   ↕
Business Wallet / payments / banking services
```

ESTABLISHED:

> Certain financial and technology actors are therefore actually involved in several European initiatives relating to digital identity, wallets and payments S33.

The same actor in two projects does not prove a data exchange

This distinction is essential.

A company may simultaneously participate in several European projects for different reasons:

- technical expertise;
- regulatory preparation;
- business development;
- research;
- standardization;
- experimentation.

NOT ESTABLISHED:

> The presence of an actor in several projects does not make it possible to claim that this actor transfers data from one infrastructure to another.

For example:

```
actor A participates in project X
   +
actor A participates in project Y
```

does not automatically mean:

data from project X → actor A → project Y

To establish such a connection, it is necessary to identify a use case, an interface, a flow, an architecture or documentation actually describing this exchange.

The WE BUILD case is stronger than a simple overlap of actors

WE BUILD nevertheless presents an important difference.

It is not merely a matter of observing that the same companies participate separately in several projects.

The domains examined are brought together **within the same consortium and the same integration architecture**.

The project's blueprint explicitly distinguishes:

```
Business
   +
Supply Chain
   +
Payments & Banking [S33](#s33)
```

and provides for a common architecture intended to ensure interoperability between the different use cases.

ESTABLISHED:

> Business identity, data sharing, supply chains, electronic invoicing and payments are therefore being tested as different components of the same ecosystem of interoperable wallets S33.

This finding constitutes stronger evidence of interconnection than the mere presence of a common actor across several programs.

A European project now explicitly connects Business Wallet and payments

The European Business Wallets examined in Section 5.2 had primarily emerged as an infrastructure for identity, attestations and data exchange for businesses.

WE BUILD shows that this infrastructure is also being experimented with in banking and payment use cases S33.

The chain therefore becomes:

```
business identity
   ↓
European Business Wallet
   ↓
attestations / business data
   ↓
banking services / payments
```

ESTABLISHED:

> The functional connection between the Business Wallet and the banking or payment environment is therefore already being experimented with in a Large Scale Pilot funded by the European Union S33.

Invoicing and payment are now found within the same experimental environment

Combining only the elements explicitly documented in WE BUILD:

```
European Business Wallet
   ↓
identity / representation / data sharing
```

in parallel:

```
Supply Chain
   ↓
electronic invoicing
```

in parallel:

```
Payments & Banking
   ↓
payments / financial services
```

ESTABLISHED:

> Electronic invoicing and payments therefore now appear within the same European wallet experimentation program S33.

NOT ESTABLISHED:

> None of the elements examined yet make it possible to claim that data originating directly from an electronic invoice are used as a criterion for authorizing or refusing a payment in WE BUILD.

Work brings digital identity and payment even closer together

Experiments relating to the EUDI Wallet are not merely conceptual.

Work conducted within the Large Scale Pilots has already addressed payment authentication using the wallet.

WE BUILD is now continuing this trajectory with use cases dedicated to payments and banking services.

ESTABLISHED:

> Digital identity and payment infrastructures are therefore being jointly experimented with, involving banks, payment service providers, wallet providers and technology companies S29-S33.

The mapping of actors becomes cross-sectoral

The projects examined reveal several categories of actors present at different levels of the ecosystem:

```
**European institutions**
European Commission / ECB
   ↓
**national administrations**
registries / tax administrations / public authorities
   ↓
**banks and PSPs**
   ↓
**wallet and trust service providers**
   ↓
**integrators and technology companies**
   ↓
**businesses and merchants**
```

ESTABLISHED:

> The infrastructures examined are therefore being developed within a common institutional and industrial environment simultaneously involving public actors, tax administrations, banks, payment service providers and technology companies S33.

This still does not demonstrate any centralization of data between all these actors.

It does, however, establish the existence of a common space for design, standardization and experimentation.

What this changes in the investigation

At the beginning of Chapter 5, several infrastructures were still connected primarily through their technical characteristics.

The previous sections have progressively established:

```
DPP + eInvoicing + Business Wallet
→ same European interoperability strategy

eInvoicing
→ planned reuse for sustainability reporting

Business Wallet
→ DPP / product / sustainability data

Business Wallet
→ ViDA / transaction data

EUDI Wallet
→ payment

external system
→ conditional payment

WE BUILD
→ Business + Supply Chain + eInvoicing + Payments & Banking
```

ESTABLISHED:

> Several domains previously examined separately are now found within common strategies, architectures and experimental programs S30-S31-S32-S33.

What this still does not make it possible to claim

Even with these new elements, it is not established that:

- French electronic invoicing data are transmitted to payment infrastructures;
- DPP data are transmitted to a bank;
- a carbon footprint is used in a payment decision;
- a tax administration can automatically order the refusal of a purchase based on environmental data;
- participants common to the different projects organize a data exchange between these infrastructures.

NOT ESTABLISHED:

> The specific operational connection from environmental data to a payment condition remains to be demonstrated.

Interim conclusion

ESTABLISHED:

> The Digital Euro Innovation Platform brings together banks, PSPs, technology companies, fintechs and commercial actors to experiment with services that could be developed around the digital euro S28-S33.

ESTABLISHED:

> Certain financial and technology actors participate in several initiatives relating to digital identity, wallets and payments S33.

ESTABLISHED:

> WE BUILD brings together more than 200 public and private organizations and develops use cases relating to businesses, supply chains and payments within the same program S33.

ESTABLISHED:

> Electronic invoicing appears among the Supply Chain use cases, while payments and banking services have their own domain within the same project S33.

ESTABLISHED:

> Tax administrations, banks, financial institutions, wallet providers and technology companies participate in the same experimental environment S33.

ESTABLISHED:

> The functional connection between the Business Wallet, business identity and banking or payment services is being experimented with S33.

INDICATION OF INTERCONNECTION:

> The presence of several infrastructures and categories of actors within the same program further reduces the institutional and technical separation between the domains examined, without by itself demonstrating that data actually circulate from one to another.

NOT ESTABLISHED:

> No operational flow directly connecting environmental data originating from a product to a condition determining the execution of a payment has yet been established.

The common actors exist.

The common programs exist.

The integration architectures exist.

Use cases relating to invoicing and payments are now found within the same experimental environment.

The next step is therefore to stop examining the components separately and reconstruct the **end-to-end interconnection chains that are actually documented**.

5.6 Documented interconnection chains

Status: ESTABLISHED / EXPERIMENTED / TECHNICALLY DEDUCIBLE / TO BE ESTABLISHED

The previous sections separately identified interoperable infrastructures, identifiers, APIs, wallets, common actors and experimental programs bringing together invoicing, identity and payment.

It is now possible to look not only for compatible components, but for chains in which several of these components actually intervene during the same transaction or process.

The work conducted within WE BUILD makes it possible to document several such chains.

Business identity → bank account → payment → proof of transaction

In September 2026, the WE BUILD consortium presents a B2B chain using the European Business Wallet as a common trust infrastructure S34.

The described journey follows a business from its identification through to proof of the transaction.

It notably includes:

```
business
   ↓
identity / cross-border KYC / KYB
   ↓
European Business Wallet
   ↓
bank account opening or identification
   ↓
verifiable IBAN attestation
   ↓
payment using the verified IBAN
   ↓
eReceipt
   ↓
proof of the transaction
```

ESTABLISHED / EXPERIMENTED:

> WE BUILD therefore documents a chain in which digital business identity, verified banking data, payment and electronic proof of transaction are involved in the same B2B journey S34.

This connection goes beyond the mere presence of distinct use cases within the same consortium.

Here, the components are used successively within the same transactional process.

EUDI Wallet → payment authentication

The PA4 use case documented by a participant in the consortium provides an additional level of detail S34.

An employee acts on behalf of a business.

Their EUDI Wallet makes it possible to present the elements required for authentication and authorization.

The payment can be made from an account or card associated with the journey.

The transaction notably contains:

- the amount;
- the currency;
- the beneficiary;
- the selected payment method.

The user confirms the transaction data and the bank processes the payment.

The experimented chain becomes:

```
authorized person
   ↓
EUDI Wallet
   ↓
strong authentication
   ↓
transaction data
   ↓
bank
   ↓
payment settlement
```

EXPERIMENTED:

> The connection between digital identity, authorization of the person acting on behalf of the business and payment is therefore materialized in a technical demonstration journey S34.

Payment → automatic issuance of verifiable proof

Once the payment is confirmed, the seller issues an eReceipt in the form of a verifiable credential S34.

This proof is sent directly to the European Business Wallet of the purchasing business.

The chain becomes:

```
confirmed payment
   ↓
seller / Business Wallet
   ↓
eReceipt generation
   ↓
verifiable credential
   ↓
purchaser's European Business Wallet
```

EXPERIMENTED:

> An event originating directly from the payment process can therefore trigger the issuance and automated transfer of a structured transactional document to the business's wallet S34.

The payment → structured transaction data connection is therefore no longer merely theoretical in this use case.

The proof contains the economic details of the transaction

The eReceipt used in the demonstration is not merely proof indicating that an overall amount has been paid.

According to the technical documentation published by the project participant, it notably contains:

- the identity of the seller;
- its VAT number;
- the purchase lines;
- the amounts excluding VAT and including VAT;
- VAT subtotals by rate;
- the payment reference S34.

EXPERIMENTED:

> The same digital object can therefore establish a verifiable link between the payment and the detailed economic content of the transaction S34.

The chain becomes:

```
payment
   ↓
payment reference
   ↓
verifiable eReceipt
   ↓
purchase lines + amounts + VAT + seller
```

This point is important for the investigation.

In this experimental case, the transactional layer and the details of the goods or services purchased are no longer necessarily two sets without a technical relationship.

Verifiable proof can serve as a bridge between them.

Proof → accounting

The Business Wallet can also be connected to the systems used by the business.

In the PA4 demonstration, a connector transmits the eReceipts to the accounting system in order to automatically record expenses S34.

The chain becomes:

```
payment
   ↓
verifiable eReceipt
   ↓
Business Wallet
   ↓
connector
   ↓
accounting
```

EXPERIMENTED:

> Data originating from the transaction can therefore be automatically reused by a system external to the wallet without manual re-entry S34.

This mechanism confirms the role of interoperability layer attributed to wallets in the previous sections.

Proof → tax administration

The experimental use case described by the participant goes even further.

The verified proofs can be communicated to a demonstration tax service.

It notably verifies:

- the signature of the proof;
- the trust placed in its issuer;
- its revocation status.

The system can then use the VAT information contained in the proofs to perform VAT reconciliation S34.

The complete experimental chain becomes:

```
B2B purchase
   ↓
payment
   ↓
verifiable eReceipt
   ↓
European Business Wallet
   ↓
detailed transaction data
   ↓
accounting system
```

and:

```
verifiable eReceipt
   ↓
demonstration tax service
   ↓
verification
   ↓
VAT reconciliation
```

EXPERIMENTED — PARTICIPANT SOURCE:

> A WE BUILD participant therefore documents a technical demonstration connecting payment, structured proof, business wallet, accounting and tax processing from end to end S34.

LIMIT:

> This demonstration does not constitute evidence that a national tax administration currently uses this chain in production.

Payment and taxation can therefore belong to the same technical chain

This distinction is important compared with the previous chapters.

Until now, the investigation had separately established:

```
payment
→ payment data

invoicing / transaction
→ tax data

Business Wallet
→ attestations and business data
```

The pilot now makes it possible to represent a single experimental chain:

```
business identity
   ↓
identity / delegation of the person
   ↓
EUDI Wallet
   ↓
account or card
   ↓
payment
   ↓
verifiable eReceipt
   ↓
European Business Wallet
   ↓
transaction details / VAT
   ↓
accounting
   ↓
experimental tax processing
```

EXPERIMENTED:

> The technical connection payment → structured proof → tax data → tax processing has therefore been demonstrated end to end within the WE BUILD ecosystem S34.

This connection does not depend on a single central database

The journey also confirms a principle identified previously.

The information does not need to be brought together in a single central database.

The different components can successively exchange verifiable proofs or credentials.

For example:

```
bank
→ payment confirmation

seller
→ issuance of the proof

wallet
→ storage / presentation of the credential

accounting
→ use of the proof

tax service
→ verification of the proof
```

ESTABLISHED / EXPERIMENTED:

> An interconnection chain can therefore operate end to end through several distributed systems without requiring a central actor to hold all the data from every stage S34.

This distributed architecture makes the analysis of interfaces and access rights particularly important, rather than focusing solely on the search for a central database.

Electronic invoicing and payment: another chain examined within the same program

WE BUILD does not limit its work to eReceipts.

The program documentation also lists among its use cases:

- Business Payments;
- eInvoicing;
- Foreign Tax Declaration S33-S34.

Interoperability workshops have also addressed business payments, invoicing and digital proofs within the EUDI Wallet and Business Wallet environments.

ESTABLISHED:

> Business payment, electronic invoicing and tax processing are therefore among the domains actually being experimented with within the same European program S33-S34.

NOT ESTABLISHED:

> The elements examined do not yet make it possible to claim that the PA4 chain relating to eReceipts directly constitutes the future ViDA electronic invoicing mechanism or the French electronic invoicing mechanism.

An important bridge is now closed

At the beginning of Chapter 5, several connections remained separate:

- identity → payment
- transaction → taxation
- Business Wallet → business data

The WE BUILD use case now makes it possible to bring them together experimentally:

```
identity
   ↓
payment
   ↓
structured proof of transaction
   ↓
Business Wallet
   ↓
tax data
   ↓
tax processing
```

EXPERIMENTED:

> There is therefore at least one European use case in which these domains are technically connected from end to end.

This does not demonstrate any purpose of controlling purchases.

It does, however, demonstrate that their technical interconnection is no longer merely an abstract possibility.

The environmental connection remains

Chapter 3 separately established:

```
identifiable product
   ↓
DPP
   ↓
product data
   ↓
sustainability / environmental data
```

Sections 5.2 and 5.3 then established:

```
Business Wallet
   ⇔
DPP / product / sustainability data
```

and:

```
Business Wallet
   ⇔
transaction / VAT / invoicing
```

The present section now experimentally establishes:

```
payment
   ↓
proof containing purchase lines
   ↓
Business Wallet
   ↓
accounting / tax processing
```

It therefore becomes possible to place the two documented chains side by side:

```
DPP / sustainability data
   ↕
European Business Wallet
```

and:

```
payment
   ↓
eReceipt / purchase lines
   ↓
European Business Wallet
```

TECHNICALLY DEDUCIBLE:

> When a purchase line makes it possible to identify the corresponding product and the necessary access rights exist, the Business Wallet or an interconnected service technically has the components required to match the proof of transaction with the corresponding information contained in the DPP ecosystem.

This matching is no longer deduced solely from the theoretical compatibility of two formats.

It is now based on the documented existence of a wallet environment connected, on the one hand, to product and sustainability data and, on the other, to detailed proofs originating from a payment.

The final connection to conditional payment remains distinct

Chapter 4 established another chain:

```
external system
   ↓
verification of a condition
   ↓
conditionality layer
   ↓
payment
```

The ECB's work also experimentally demonstrated that platforms operated by market actors could communicate via API with an environment simulating the digital euro S27-S28.

We therefore now have two sets:

Set A

```
product / DPP / sustainability
   ↕
Business Wallet
   ↕
detailed transaction / eReceipt
   ↕
payment
```

Set B

```
external system
   ↓
external condition
   ↓
conditionality layer
   ↓
payment
```

TECHNICALLY DEDUCIBLE:

> The documented architectures therefore contain the components necessary for information originating from an external system to be verified and used in a process surrounding the execution of a payment.

NOT ESTABLISHED:

> None of the elements examined demonstrate, however, that environmental data from the DPP are currently used as a condition in a digital euro payment or in another payment system.

The difference between "possible", "experimented" and "planned"

At this stage of the investigation, three levels must be strictly distinguished.

EXPERIMENTED:

> identity → payment → structured proof → Business Wallet → accounting / tax processing.

ESTABLISHED / PLANNED:

> Business Wallet ↔ DPP / product and sustainability data.

ESTABLISHED / EXPERIMENTED:

> external system → verification of a condition → conditional payment.

But:

NOT ESTABLISHED:

> environmental data → condition determining the execution of a payment.

This final arrow must not be artificially added to the chain as long as no source documents it.

What this section changes in the demonstration

At the beginning of the investigation, it would have been possible to argue that the different systems examined had no connection with one another:

"the invoice is tax-related";

"the DPP is environmental";

"the wallet is used for identity";

"payment belongs to banks";

"the digital euro is a separate monetary infrastructure".

The sources examined now make it possible to rule out such an absolute version of this separation.

ESTABLISHED:

> The Commission explicitly seeks synergies between several of these infrastructures S30-S31.

ESTABLISHED:

> Standards, APIs, attestations and interoperability mechanisms enable interactions between them S20-S30-S32.

ESTABLISHED:

> European programs bring together identity, invoicing, taxation and payment within the same experimental environments S33-S34.

EXPERIMENTED:

> An end-to-end chain connecting identity, payment, detailed proof, Business Wallet, accounting and tax processing has been demonstrated by WE BUILD participants S34.

NOT ESTABLISHED:

> The use of environmental data as a payment criterion remains unproven.

Interim conclusion

ESTABLISHED / EXPERIMENTED:

> A wallet infrastructure can participate in a chain connecting the identity of a business and its representative, an account or card, a payment and structured proof of the transaction S34.

EXPERIMENTED:

> This proof can contain the purchase lines, amounts, VAT information and a payment reference, then be automatically transmitted to the European Business Wallet of the business S34.

EXPERIMENTED:

> Connectors then enable the proof to be reused by an accounting system and, in the demonstration case examined, by a tax service performing VAT reconciliation S34.

ESTABLISHED:

> The same Business Wallet ecosystem is also connected with the Digital Product Passport and its data relating to products and their sustainability S30.

ESTABLISHED / EXPERIMENTED:

> A separate conditional payment architecture also enables a condition verified by an external system to intervene in the execution of a transaction S27-S28.

TECHNICALLY DEDUCIBLE:

> The infrastructures examined therefore make it possible to construct a technical chain in which a detailed transaction can be linked to an identifiable product, the product to external data, and the result of an external verification to conditional logic surrounding a payment.

NOT ESTABLISHED:

> None of the documents examined demonstrate, however, that this chain is currently assembled in order to use environmental data to authorize, refuse or limit a payment.

The number of missing connections has therefore been considerably reduced.

It now remains to examine precisely **the final connection in the chain: environmental data → payment**, looking not only at whether it is technically possible, but whether a project, pilot, standard or documentation exists that experiments with it or explicitly provides for it.

S35 CEN/TS 16931-8:2024 — eReceipts, DPP identifier and environmental product information

Organization: European Committee for Standardization (CEN)

Document: CEN/TS 16931-8:2024 — Electronic invoicing — Part 8: Semantic data model of the elements of an e-receipt

Date: 2024

Used in: Chapter 5

Established elements: European semantic model relating to electronic receipts; description of a process in which the buyer selects a payment method, makes or initiates the payment and then receives an eReceipt generated by the seller; possibility of including, in certain environments, specific information relating to the product; explicit mention of the Digital Product Passport for the product categories concerned; use of a DPP identifier enabling the receipt to be linked to verified information relating to the product; mention among this information of the sustainability of materials as well as the social and environmental impacts associated with the materials, production, use and end of life of the product.

Methodological precaution: the existence of a field or mechanism enabling an eReceipt to be linked to the DPP demonstrates the standardized possibility of establishing this connection. It does not demonstrate that every eReceipt will contain a DPP identifier, that the corresponding environmental data will be systematically retrieved, or that they will be used by a payment system.

Reference: CEN/TS 16931-8:2024

5.7 The environmental data → payment connection

Status: ESTABLISHED / EXPERIMENTED / TECHNICALLY DEDUCIBLE / NOT ESTABLISHED

The previous sections have progressively reduced the number of missing connections between the infrastructures examined.

At the end of Section 5.6, two distinct chains had been established.

The first now experimentally connects payment to the economic details of the transaction:

```
payment
   ↓
eReceipt
   ↓
purchase lines
   ↓
European Business Wallet
```

The second connects information originating from an external system to the execution of a conditional payment:

```
external system
   ↓
verification of a condition
   ↓
conditionality layer
   ↓
payment
```

The question addressed in this section is therefore deliberately limited to a single arrow:

> **Is there a documented mechanism enabling environmental information relating to a product to be linked to the transaction or to the condition determining the execution of the payment?**

---

eReceipt → Digital Product Passport

An additional element appears in European standardization work relating to electronic receipts S35.

The CEN/TS 16931-8:2024 model describes the economic process in which the buyer selects a payment method, makes or initiates the payment, and then receives an eReceipt generated by the seller.

The same document provides that, in certain environments, specific information relating to the product may be associated with the receipt.

For product categories subject to the Digital Product Passport, the standard explicitly mentions the use of a **DPP identifier enabling the receipt to be linked to verified information relating to the product** S35.

ESTABLISHED:

> A European standard relating to eReceipts therefore explicitly provides for a connection between the receipt for a transaction and the Digital Product Passport of the corresponding product S35.

The chain becomes:

```
purchase
   ↓
payment
   ↓
eReceipt
   ↓
DPP identifier
   ↓
Digital Product Passport
```

This connection is more precise than the mere possibility of subsequently matching a commercial reference with a product identifier.

The mechanism for linking to the DPP is directly envisaged in the receipt model.

The connection provides access to environmental information

The same standard explains the purpose of this relationship with the DPP.

The identifier makes it possible to link the product to verified information concerning its life cycle.

The information explicitly mentioned notably includes:

- the sustainability of material sourcing;
- the social impacts of the materials used;
- the environmental impacts of the materials used;
- production;
- use;
- the end of life of the product S35.

ESTABLISHED:

> The eReceipt → DPP identifier connection therefore does not lead solely to an administrative reference for the product: it can lead to verified information including characteristics relating to its sustainability and environmental impacts S35.

The following chain is thus explicitly documented at the semantic model level:

```
transaction
   ↓
eReceipt
   ↓
DPP identifier
   ↓
product
   ↓
verified information
   ↓
sustainability / environmental impacts
```

Payment → eReceipt → DPP → environment

This new element can be considered alongside the chain experimented with in WE BUILD.

Section 5.6 established:

```
payment
   ↓
verifiable eReceipt
   ↓
purchase lines / transaction information
```

The CEN/TS 16931-8 standard adds:

```
eReceipt
   ↓
DPP identifier
   ↓
verified product information
   ↓
environmental information
```

ESTABLISHED / EXPERIMENTED DEPENDING ON THE LINK:

> The documented components therefore now make it possible to construct a chain in which a payment is linked to an electronic receipt and in which an electronic receipt can itself be linked, by means of a DPP identifier, to verified environmental information relating to the product S34-S35.

The complete chain can be represented as follows:

```
payment
   ↓
eReceipt
   ↓
identifiable product
   ↓
DPP identifier
   ↓
Digital Product Passport
   ↓
sustainability / environmental data
```

LIMIT:

> This representation combines two connections documented in different contexts. It does not demonstrate that the entire chain is currently used end to end within the same operational system.

The transaction → environment connection is therefore no longer merely hypothetical

At the beginning of the investigation, the link between a purchase and the environmental characteristics of the product was based on a deduction:

```
transaction
   ↓
identify the product
   ↓
look up its DPP
   ↓
retrieve the environmental data
```

The standard relating to eReceipts provides an additional element.

ESTABLISHED:

> The European model directly provides that a DPP identifier may be associated with the receipt in order to link the purchase to verified information relating to the product S35.

It is therefore no longer necessary to assume that matching would necessarily have to be performed after the transaction using independent databases.

The receipt itself can carry the mechanism enabling access to the product passport.

Another convergence exists with electronic invoicing

This relationship must also be considered alongside the elements established in Sections 5.3 and 5.4.

The Commission provides for:

```
eInvoicing
   ↓
data reuse
   ↓
sustainability reporting
```

and standardization work relating to EN 16931 explicitly takes into account requirements arising from sustainability reporting S31-S32.

The standard relating to eReceipts now adds:

```
eReceipt
   ↓
DPP identifier
   ↓
environmental product information
```

ESTABLISHED:

> Several distinct European initiatives therefore organize the connection between data describing a transaction and information relating to sustainability or the environment S31-S32-S35.

This still does not demonstrate the establishment of an individual environmental profile.

Conditional payment accepts a condition originating from an external source

At the other end of the chain, the ECB's work establishes that conditional logic does not need to be integrated into the money itself.

The system examined separates:

```
settlement infrastructure
   +
market-developed conditionality layer
```

This layer can use external monitoring to verify that a condition is satisfied S27-S28.

Once this condition has been verified:

```
condition satisfied
   ↓
release of funds
```

or, if it is not:

```
condition not satisfied
   ↓
cancellation / expiration of the reservation
```

ESTABLISHED / EXPERIMENTED:

> The current design therefore enables information verified outside the settlement infrastructure to intervene in the decision to execute a conditional payment S27-S28.

The nature of the condition is not technically limited to delivery

The examples most frequently presented by the ECB concern the delivery of a product, the arrival of a train, the use of a service or the completion of a step.

These examples describe use cases.

They do not constitute a technically exhaustive list of the only information that can be verified by a conditionality layer.

Experimental work shows that service providers can develop the conditional logic and that external platforms can intervene in its verification S27-S28.

TECHNICALLY DEDUCIBLE:

> A condition originating from an environmental infrastructure could technically be processed according to the same principle if a service provider developed such a service, if the corresponding data were accessible and if such use were legally authorized.

For example:

```
DPP identifier
   ↓
external service
   ↓
reading of an environmental characteristic
   ↓
evaluation of a rule
   ↓
verification result
```

The payment system would not necessarily need to receive the entire DPP.

It could technically receive only a result:

```
condition satisfied
   or
condition not satisfied
```

The final technical connection can therefore be represented

By combining only the documented capabilities:

```
purchased product
   ↓
eReceipt
   ↓
DPP identifier
   ↓
Digital Product Passport
   ↓
environmental data
   ↓
external verification service
   ↓
result of a condition
   ↓
conditionality layer
   ↓
payment
```

TECHNICALLY DEDUCIBLE:

> No architectural obstacle identified in the sources examined requires the data verified by the external system to be delivery data rather than other data accessible to that system.

But this deduction must immediately be distinguished from evidence of actual use.

The search for an environmental use case in the ECB's work

The Digital Euro Innovation Platform documents make it possible to determine whether this possibility has already been turned into an environmental use case.

The documented scenarios notably concern:

- delivery;
- pay-per-use payments;
- milestone payments;
- mobility and transport;
- e-commerce;
- financial services;

- certain industrial applications;
- machine-to-machine interactions S28.

Work relating to eReceipts also mentions an environmental benefit resulting from reduced paper use.

NOT ESTABLISHED:

> The Digital Euro Innovation Platform documents examined do not, however, describe a scenario in which the carbon footprint, environmental performance, DPP or other sustainability data relating to a product constitute the condition triggering or preventing a payment S28.

This negative finding is important.

It prevents the technical possibility from being turned into a claim about a currently documented project.

The digital euro cannot be used as programmable money

Another limitation must remain explicitly stated.

The proposed regulation on the digital euro excludes **programmable money** S22.

This means that units of digital euro must not intrinsically contain restrictions determining:

- the categories of goods that can be purchased;
- the merchants with whom they can be used;
- the period during which they can be spent;
- or other limitations undermining their full fungibility.

ESTABLISHED:

> The Eurosystem therefore does not plan to encode within the monetary units themselves a rule such as "this euro cannot purchase a product whose carbon footprint exceeds X" S22-S27.

Conditional payment and programmable money nevertheless remain two different mechanisms

The exclusion of programmable money does not eliminate conditional payments.

The European proposal separately defines a conditional payment transaction as a transaction executed automatically when predetermined conditions agreed between the payer and the payee are fulfilled S22.

The ECB also provides for payment service providers to develop the conditionality layer S27-S28.

The distinction is therefore:

```
**PROGRAMMABLE MONEY**
rule embedded in the monetary unit
→ excluded

versus:

**CONDITIONAL PAYMENT**
rule applied to the transaction process
→ provided for / experimented
```

ESTABLISHED:

> The prohibition of programmable money therefore does not constitute a general prohibition of all automated logic surrounding the execution of a payment S22-S27-S28.

The conditions are presented as agreed between the parties

This limitation is also essential.

In the legislative proposal, the conditions of a conditional payment are defined as predetermined conditions **agreed between the payer and the payee** S22.

The additional services examined by the ECB are also presented as services developed by market actors and used voluntarily by users.

ESTABLISHED:

> The documents examined therefore do not grant the ECB or the Eurosystem a general power to unilaterally impose an environmental condition on users' purchases.

NOT ESTABLISHED:

> No mechanism has been identified that would enable an administration to directly transform individual environmental data into a payment prohibition imposed on the payer.

The technical chain and the legal chain must be kept separate

The result of the analysis can therefore be represented in two different ways.

TECHNICAL CAPABILITY:

```
transaction
   ↓
eReceipt
   ↓
DPP identifier
   ↓
environmental data
   ↓
external service
   ↓
condition
   ↓
conditional payment
```

TECHNICALLY DEDUCIBLE:

> The components required to construct this chain exist separately, and the interfaces necessary for several of its connections are documented.

But:

ESTABLISHED USE:

```
environmental data
   ↓
imposed environmental condition
   ↓
authorization / refusal of payment
```

NOT ESTABLISHED:

> No institutional project, regulation, pilot or technical documentation examined currently demonstrates the use of environmental data relating to a product in order to authorize, refuse or limit a payment.

An important difference nevertheless emerges compared with the beginning of the investigation

At the beginning of the analysis, almost the entire chain had to be reconstructed by hypothesis:

```
invoice
   ?
product
   ?
environment
   ?
identity
   ?
payment
```

At this stage, the documented connections are much more numerous:

```
invoicing / transaction
   ↓
structured data

product
   ↓
DPP
   ↓
environmental data

eReceipt
   ↓
DPP identifier

Business Wallet
   ↔
DPP / sustainability

Business Wallet
   ↔
transaction / taxation

identity
   ↓
wallet
   ↓
payment

payment
   ↓
detailed eReceipt

external system
   ↓
condition
   ↓
conditional payment
```

The point that remains unproven is therefore no longer the existence of the necessary infrastructures.

It is now much more precise:

> **the existence of a rule or use case actually using environmental data as a condition determining the execution of a payment.**

The current documentary boundary

The boundary between what is established and what is not can now be precisely defined.

ESTABLISHED:

> A product can be linked to environmental data through the Digital Product Passport S15-S19.

ESTABLISHED:

> An eReceipt can contain an identifier enabling the purchase to be linked to the DPP and its verified information relating to the product S35.

EXPERIMENTED:

> A payment can be linked to an eReceipt containing the economic details of the transaction S34.

ESTABLISHED / EXPERIMENTED:

> An external system can verify a condition used by a conditionality layer surrounding a payment S27-S28.

TECHNICALLY DEDUCIBLE:

> Environmental data accessible through the DPP could be verified by an external service and its result used as a technical condition according to the same architecture.

NOT ESTABLISHED:

> The sources examined do not demonstrate that such an environmental service is currently planned or being experimented with to determine the execution of a payment.

Interim conclusion

ESTABLISHED:

> The European standard relating to eReceipts explicitly provides that a DPP identifier can link a transaction receipt to verified product information, including information relating to its sustainability and environmental impacts S35.

EXPERIMENTED:

> European work has also demonstrated a chain connecting payment, detailed eReceipt and Business Wallet S34.

ESTABLISHED / EXPERIMENTED:

> The conditional payment architecture enables an external system to verify a condition whose result intervenes in the execution of the payment S27-S28.

TECHNICALLY DEDUCIBLE:

> The documented components therefore technically make it possible to construct a chain payment ↔ identifiable transaction ↔ product ↔ DPP ↔ environmental data, as well as a chain external data → condition → payment.

NOT ESTABLISHED:

> No element identified demonstrates, however, that these two chains are currently connected so that environmental data determine the authorization, refusal or limitation of a payment.

ESTABLISHED:

> Under the proposed legal framework for the digital euro, the conditions of a conditional payment are presented as predetermined and agreed between the payer and the payee, while programmable money intrinsically limiting the goods or services that can be purchased is explicitly excluded S22.

The search for the environmental data → payment connection therefore leads to a nuanced but precise result:

> **the technical chain can be reconstructed using components and connections that are now largely documented; its environmental use as a payment decision mechanism remains unestablished.**

This boundary must be preserved in the conclusion of the investigation.

The following section must now examine the **limitations of the demonstration**, in order to definitively distinguish what the architecture enables, what has been experimented with and what no source yet makes it possible to claim.

5.8 Limitations of the demonstration

Status: ESTABLISHED LIMITATIONS / NOT ESTABLISHED

The previous sections have made it possible to identify numerous connections between the infrastructures examined.

These connections must not, however, be interpreted beyond what the sources actually demonstrate.

This section therefore establishes the limitations of the demonstration before presenting its synthesis.

Interoperability does not mean systematic data exchange

The infrastructures examined use identifiers, standards, APIs, verifiable attestations and authorization mechanisms enabling their interoperability S20-S30-S32.

ESTABLISHED:

> Several of these systems are technically designed to be able to exchange or verify information originating from other systems.

But:

NOT ESTABLISHED:

> This interoperability does not mean that all their data are automatically pooled, transmitted or centralized.

A possibility of interconnection must therefore be distinguished from an actually activated flow.

A connection between two systems does not demonstrate a complete chain

Several connections have been documented separately:

- transaction → eReceipt
- eReceipt → DPP
- DPP → environmental data
- identity → payment
- external system → condition → payment

The existence of each of these connections is not sufficient to demonstrate that they are all used simultaneously within the same process.

NOT ESTABLISHED:

> No operational system identified in the sources examined currently connects environmental data originating from the DPP end to end with a decision authorizing or refusing a payment.

A planned standard does not mean systematic use

The standard relating to eReceipts provides for the possibility of linking a receipt to the Digital Product Passport by means of a DPP identifier S35.

This demonstrates the existence of a standardized mechanism enabling this connection.

But:

NOT ESTABLISHED:

> Not all eReceipts will necessarily contain a DPP identifier, and not all products will necessarily be subject to the same digital passport requirements.

The standardized possibility of including data therefore does not demonstrate its systematic use.

A pilot project does not mean a deployed system

The WE BUILD experiments and those of the Digital Euro Innovation Platform make it possible to demonstrate the feasibility of several technical chains S28-S33-S34.

They constitute evidence of experimentation.

They do not necessarily constitute evidence of operational deployment.

NOT ESTABLISHED:

> The processes experimented with in these pilots must not be presented as mechanisms already generalized to all European businesses, administrations, banks or users.

This distinction is particularly important for demonstrations using simulated tax services or experimental payment environments.

A legislative proposal does not mean definitively adopted law

The European Business Wallets examined in this chapter are notably based on a proposed regulation presented by the European Commission S30.

At the date of the analysis, this proposal is still going through the European legislative procedure.

ESTABLISHED:

> The proposal makes it possible to establish the proposed direction, the envisaged functionalities and the intended architecture.

But:

NOT ESTABLISHED:

> Not all the provisions examined can be presented as already constituting the definitive applicable law in their current wording.

The final text may still evolve during the legislative procedure.

Technical possibility does not mean legal authorization

An infrastructure may technically enable two systems to communicate without all actors being legally authorized to access the corresponding data.

The DPP notably provides for differentiated access rights depending on the data and product categories S15-S20.

The EUDI and Business Wallet architectures also rely on authorization mechanisms and selective presentation of information S29-S30.

ESTABLISHED:

> Technical access to an infrastructure and the right to access particular data are two different questions.

Consequently:

TECHNICALLY DEDUCIBLE:

> A chain may be architecturally feasible.

without this making it possible to claim:

> that a specific actor legally has the right to use it for a specific purpose.

The DPP is not an individual consumption profile

The Digital Product Passport describes the product, its model, batch or item according to the applicable rules S15.

The regulation also provides that personal data relating to customers must not be stored in the DPP without their explicit consent S15.

ESTABLISHED:

> The DPP is an infrastructure relating to the product and is not, by its nature, a database intended to establish the individual profile of its purchaser.

NOT ESTABLISHED:

> The existence of the DPP therefore does not demonstrate the existence of a centralized European registry associating each individual with all the products they purchase.

Matching with a transaction or identity would require additional mechanisms as well as an appropriate legal basis or consent, depending on the case.

Business Wallet does not mean an individual consumer wallet

European Business Wallets are intended for economic operators and professional or administrative interactions S30.

They must be distinguished from the EUDI Wallet intended for natural persons.

ESTABLISHED:

> The B2B chains documented in WE BUILD do not demonstrate that an identical mechanism is automatically applied to the personal purchases of every consumer.

This distinction prevents a B2B pilot from being directly transposed to a scenario of individual consumption control.

Tax data does not mean exhaustive knowledge of individual purchases

Chapter 1 showed that the data transmitted under the French electronic invoicing and e-reporting framework differ depending on the transactions.

B2C transactions do not necessarily result in the transmission to the tax administration of individualized details of every product purchased by every consumer S1-S2-S3-S4.

NOT ESTABLISHED:

> The French electronic invoicing reform therefore cannot, on the basis of the sources examined, be presented as creating by itself an exhaustive nominative registry of every individual's purchases.

This limitation remains even if other infrastructures separately hold more detailed information about certain products or transactions.

Available environmental data does not mean an individual carbon profile

The DPP and other European regulations enable or require, depending on the products concerned, the availability of data relating to sustainability or certain environmental impacts S15-S18-S19.

Technical matching between a transaction and this information can also be envisaged or standardized S31-S35.

But:

NOT ESTABLISHED:

> No general mechanism automatically establishing an individual carbon footprint based on all of a person's purchases has been identified in the sources examined.

Such a purpose would notably require the identification of the relevant transactions, their attribution to a person, the retrieval of the corresponding environmental data and a method enabling their aggregation.

Conditional payment does not mean programmable money

Chapter 4 established a fundamental distinction S22-S27-S28.

The digital euro must not be designed as programmable money whose units would be restricted to certain goods, merchants, locations or periods.

However, conditional payment services are provided for and being experimented with.

The distinction is:

programmable money
rule embedded in the monetary unit
→ excluded

and:

conditional payment
rule applied to the process surrounding the transaction
→ provided for / experimented

ESTABLISHED:

> The existence of conditional payments therefore does not make it possible to claim that the digital euro itself can be programmed to prohibit certain categories of purchases S22-S27-S28.

A technically possible condition does not mean an imposed condition

Conditional payments are presented as relying on predetermined conditions involved in the transaction process S22-S27-S28.

Market actors can develop services using this conditionality layer.

TECHNICALLY DEDUCIBLE:

> Data accessible to an external system could technically be used to verify a condition if a corresponding service were developed.

But:

NOT ESTABLISHED:

> No general power enabling an administration to impose an environmental condition on all users' payments has been identified in the sources examined.

The ECB has not documented an environmental payment condition

The Digital Euro Innovation Platform experiments include various conditional payment scenarios S28.

The use cases examined notably concern delivery, the use of a service, contractual milestones, transport or machine-to-machine processes.

NOT ESTABLISHED:

> The documents examined do not present the carbon footprint, the DPP or another environmental characteristic of the product as a condition determining the execution of a payment.

This absence currently constitutes the main documentary limitation of the chain examined.

A common actor does not mean data exchange

Several banks, payment service providers, technology companies and integrators participate in different European projects S33.

These overlaps make it possible to identify a common industrial environment.

But:

NOT ESTABLISHED:

> The participation of the same organization in several projects does not demonstrate that it transfers data between these projects or their infrastructures.

An interconnection must be established on the basis of a flow, an interface, a use case or documentation actually describing the connection.

Distributed infrastructure does not mean a central surveillance database

The chains examined can operate by means of:

- APIs;
- verifiable attestations;
- wallets;
- registries;
- intermediary services;
- external verification mechanisms.

Information can therefore be verified without necessarily being copied in full into every system involved in the process.

NOT ESTABLISHED:

> The sources examined do not demonstrate the existence of a central European database simultaneously bringing together individual identity, complete purchase history, environmental data, tax data and payment data.

The possibility of distributed interconnection must therefore be distinguished from the hypothesis of complete data centralization.

Stated purpose and technical capability are two different levels

The investigation documents two categories of elements that should not be confused.

On the one hand:

> **explicitly stated purposes**

For example:

- combating fraud;
- administrative simplification;
- tax reporting;
- product information;
- sustainability;
- digital identity;
- interoperability;
- innovation in payments.

On the other hand:

> **technical capabilities resulting from the architecture**

For example:

- matching multiple identifiers;
- querying a registry;
- verifying an attestation;

- linking a receipt to a product;
- retrieving environmental information;
- verifying an external condition;
- automating certain stages of a transaction.

TECHNICALLY DEDUCIBLE:

> A capability may exist before a particular purpose is assigned to it.

But:

NOT ESTABLISHED:

> The existence of this capability does not constitute evidence that European or national institutions intend to use it for an undocumented purpose.

This distinction constitutes one of the central methodological limitations of the investigation.

The boundary of the demonstration

After all the research conducted in Chapter 5, the boundary can be precisely defined.

ESTABLISHED OR EXPERIMENTED:

> invoicing / transaction → structured data

> product → DPP → environmental data

> eReceipt → DPP identifier → product information

> identity → wallet → payment

> payment → detailed eReceipt

> Business Wallet ↔ transaction / tax data

> Business Wallet ↔ product / sustainability ecosystem

> external system → verification of a condition → conditional payment

But:

NOT ESTABLISHED:

> environmental data → imposed rule → authorization / refusal of a payment

and:

NOT ESTABLISHED:

> all of these infrastructures → centralized system for individual consumption control

---

Interim conclusion

The research conducted in this chapter therefore makes it possible to go much further than simply observing the parallel existence of several digital infrastructures.

Institutional, standardization and technical connections genuinely exist.

Some are already provided for by legal texts.

Others are standardized.

Still others have been experimented with in European pilots.

But several limitations remain essential:

> **interoperable** does not mean **permanently interconnected**;

> **interconnected** does not mean **centralized**;

> **technically possible** does not mean **legally authorized**;

> **experimented** does not mean **deployed**;

> **environmental data accessible** does not mean **individual carbon profile**;

> **conditional payment** does not mean **programmable money**;

> **technical capability** does not mean **political intention**.

Finally, the main documentary boundary remains unchanged:

> **the infrastructures enabling transaction, product, environmental data and a conditionality mechanism to be linked exist or can be technically connected, but none of the sources examined currently demonstrate that environmental data are used to authorize, refuse or limit a user's payment.**

5.9 What this chapter establishes

Chapter 5 aimed to determine whether the infrastructures examined previously should be considered independent systems or whether concrete interconnections between them could be documented.

The research now makes it possible to provide a more precise answer.

The systems do not form a single centralized infrastructure.

However, they are not entirely independent of one another either.

Institutional, standardization and technical connections exist between several of them. Some are provided for by legal texts, some are standardized and others have already been experimented with.

A common European ecosystem is explicitly being pursued

The European Commission no longer presents some of these infrastructures solely as isolated projects.

Its Single Market Strategy notably brings together:

- the Digital Product Passport;
- eInvoicing;
- European Business Wallets;
- the Single Digital Gateway;
- the Once Only Technical System;
- European identification and data exchange systems.

The Commission indicates that these tools should collectively form a **coherent ecosystem of digital solutions** intended to create synergies between the different systems S30-S31.

ESTABLISHED:

> The existence of a European strategy aimed at interoperability and the creation of synergies between several infrastructures examined in this investigation is explicitly documented.

This institutional convergence does not, however, demonstrate that all the data from these systems are exchanged between them.

Electronic invoicing → other uses of data

Electronic invoicing is not merely a mechanism for transmitting a document between seller and buyer.

In France, structured data notably feed the tax administration S1-S2-S3-S4.

At the European level, the Commission also plans to develop the reuse of eInvoicing data for other functions S31.

The explicitly documented directions include:

```
eInvoicing
   ↓
VAT reporting
```

but also:

```
eInvoicing
   ↓
sustainability reporting
```

and:

```
eInvoicing
   ↓
customs data / EU Customs Data Hub
```

ESTABLISHED:

> The reuse of electronic invoicing data beyond the sole production of the invoice is part of the documented European directions S31.

Transaction → product → environment

Chapter 3 established the existence of an infrastructure enabling a product to be associated with a Digital Product Passport containing, depending on the categories concerned, information relating to its sustainability or environmental characteristics S15-S18-S19-S20.

Chapter 5 identified an additional connection.

The European model relating to eReceipts provides that a receipt may contain an identifier enabling the purchased product to be linked to its Digital Product Passport S35.

The chain becomes:

```
transaction
   ↓
eReceipt
   ↓
DPP identifier
   ↓
product
   ↓
sustainability / environmental data
```

ESTABLISHED:

> A standardized mechanism enabling a transaction receipt to be linked to the Digital Product Passport and to verified product information is documented S35.

LIMIT:

> This does not mean that all products or all receipts will systematically use this mechanism.

Business Wallet → identity, transaction and product data

European Business Wallets constitute another important connection point.

The documents examined provide for their use to:

- identify and authenticate economic operators;
- manage verifiable attestations;
- exchange information relating to VAT and transactions;
- support invoicing-related processes;
- interact with the Digital Product Passport and certain data relating to products and their sustainability S30.

The institutional chain can therefore be represented as follows:

```
business identity
   ↕
Business Wallet
   ↔ tax / transaction data
   ↔ invoicing
   ↔ DPP / product data
```

ESTABLISHED:

> The Business Wallet is designed as a cross-cutting infrastructure enabling several categories of business data to be presented, verified or exchanged within an interoperable environment S30-S32.

LIMIT:

> The legislative proposal relating to European Business Wallets has not yet been definitively adopted in its current wording.

Identity → payment

The connection between digital identity and payment is also explicitly documented.

The EUDI Wallet can be used for payment authentication and the selective presentation of certain attestations S29.

Work relating to the digital euro also provides for its use as a possible authentication mechanism for certain transactions S22-S29.

The chain:

```
digital identity
   ↓
EUDI Wallet
   ↓
authentication
   ↓
payment
```

is therefore:

ESTABLISHED / EXPERIMENTED:

> European digital identity and payment infrastructures are already the subject of common connections and experiments S29.

Payment → detailed transaction → Business Wallet

The experiments examined in WE BUILD provide an additional connection.

A B2B journey connects:

```
business identity
   ↓
authorized person
   ↓
wallet
   ↓
account or card
   ↓
payment
   ↓
verifiable eReceipt
   ↓
purchase lines / VAT / payment reference
   ↓
European Business Wallet
```

The receipt can then be reused by accounting systems and, in the demonstration examined, by a tax service for VAT reconciliation S34.

EXPERIMENTED:

> A chain connecting identity, payment, detailed transaction receipt, Business Wallet and accounting or tax processing has therefore been the subject of a technical demonstration S34.

This chain must not, however, be presented as a system already generalized or deployed by European tax administrations.

External system → condition → payment

Work relating to the digital euro also establishes that a conditional payment can depend on a condition verified outside the settlement infrastructure S22-S27-S28.

The architecture can be represented as follows:

```
external event or information
   ↓
verification service
   ↓
condition satisfied / not satisfied
   ↓
conditionality layer
   ↓
execution of the payment
```

ESTABLISHED / EXPERIMENTED:

> External systems can intervene in the verification of a condition used by a conditional payment service S27-S28.

The conditional logic can be developed by market actors without being integrated into the monetary unit itself.

The main documented chains

At the end of Chapter 5, the connections can be summarized as follows:

```
**INVOICING / TRANSACTION**
structured data
   ↓
taxation
   ↓
planned reuse for other reporting purposes
```

```
**TRANSACTION / PRODUCT**
eReceipt
   ↓
DPP identifier
   ↓
Digital Product Passport
   ↓
product / sustainability / environmental information
```

```
**BUSINESS**
identity
   ↓
European Business Wallet
   ⇿ attestations
   ⇿ transaction / VAT / invoicing
   ⇿ product environment / DPP
```

```
**IDENTITY / PAYMENT**
EUDI Wallet
   ↓
authentication
   ↓
payment
```

```
**PAYMENT / RECEIPT**
payment
   ↓
verifiable eReceipt
   ↓
transaction details
   ↓
Business Wallet
   ↓
accounting / experimental tax processing
```

```
**CONDITIONAL PAYMENT**
external system
   ↓
verification of a condition
   ↓
conditionality layer
   ↓
payment
```

The technically reconstructible chain

These connections now make it possible to reconstruct a much more complete chain than the one available at the beginning of the investigation:

```
identity
   ↓
wallet
   ↓
transaction / payment
   ↓
structured receipt
   ↓
identifiable product
   ↓
Digital Product Passport
   ↓
environmental data
```

In parallel:

```
external data
   ↓
verification service
   ↓
result of a condition
   ↓
conditional payment
```

TECHNICALLY DEDUCIBLE:

> The documented architectures technically enable information relating to a product to be retrieved from an external infrastructure, evaluated by a service and transformed into a result that can be used by automated logic surrounding a transaction.

This conclusion does not require the existence of a central database bringing together all the information.

The different systems can operate by means of identifiers, APIs, wallets, verifiable attestations and intermediary services S20-S30-S32.

The connection that was not found

Despite the research conducted across the different infrastructures, none of the documents examined makes it possible to add the following arrow as an established element:

```
environmental data
   ↓
environmental condition
   ↓
authorization / refusal / limitation of payment
```

NOT ESTABLISHED:

> No regulation, institutional project, standard or pilot identified in this investigation currently demonstrates that environmental data originating from the DPP or an equivalent infrastructure are used to determine the execution of a payment.

The conditional payment examples examined concern other events or conditions S27-S28.

The presence of the necessary components therefore does not constitute evidence that they are assembled for this purpose.

What nevertheless changes compared with the initial hypothesis

At the beginning of the investigation, a possible representation would have been:

```
invoicing
   ?
product
   ?
environment
   ?
identity
   ?
payment
```

After analysis of the official sources, the situation is different.

Several question marks can be replaced by documented connections:

```
transaction
   → eReceipt
   → DPP
   → environmental data
```

and:

```
identity
   → wallet
   → payment
```

as well as:

```
payment
   → detailed eReceipt
   → Business Wallet
```

and:

```
external system
   → condition
   → conditional payment
```

Finally, the Commission itself documents a strategy aimed at creating synergies between several digital infrastructures examined in this investigation S30-S31.

ESTABLISHED:

> The hypothesis that all these infrastructures are necessarily designed and operated as completely independent systems is therefore not consistent with the documents examined as a whole.

But the opposite claim would also be excessive.

NOT ESTABLISHED:

> The sources do not demonstrate the existence of a single infrastructure bringing together all these data, nor of a European system for individual environmental control of payments.

Summary table

Connection examined	Status
Electronic invoicing → tax administration	**ESTABLISHED**
Tax data → economic analysis / public policy	**ESTABLISHED**
Product → Digital Product Passport	**ESTABLISHED**
DPP → sustainability / environmental data	**ESTABLISHED**
DPP → registry / API / external systems	**ESTABLISHED**
eReceipt → DPP identifier	**ESTABLISHED**
eReceipt → environmental information via DPP	**ESTABLISHED**
eInvoicing → reuse for sustainability reporting	**PLANNED / ESTABLISHED**
eInvoicing → matching with customs data	**PLANNED / ESTABLISHED**
Business Wallet → business identity	**ESTABLISHED IN THE PROJECT**
Business Wallet → VAT / transaction / invoicing data	**ESTABLISHED IN THE PROJECT**

Connection examined	Status
Business Wallet → DPP / product data	**ESTABLISHED IN THE PROJECT**
EUDI Wallet → payment authentication	**ESTABLISHED / EXPERIMENTED**
EUDI Wallet → digital euro	**PLANNED / EXPERIMENTED**
Payment → detailed eReceipt → Business Wallet	**EXPERIMENTED**
eReceipt → accounting / tax processing	**EXPERIMENTED**
External system → condition → payment	**ESTABLISHED / EXPERIMENTED**
Transaction → product → environmental data	**ESTABLISHED / DEDUCIBLE DEPENDING ON ACTUAL LINKAGE**
Environmental data → external verification service	**TECHNICALLY DEDUCIBLE**
Environmental data → payment condition	**TECHNICALLY DEDUCIBLE**
Environmental data → actual refusal or limitation of payment	**NOT ESTABLISHED**
Generalized individual carbon profile based on purchases	**NOT ESTABLISHED**
Central database combining identity + purchases + taxation + environment + payment	**NOT ESTABLISHED**
Institutional control of purchases according to their environmental impact	**NOT ESTABLISHED**

Conclusion of Chapter 5

Chapter 5 makes it possible to rule out two opposing conclusions.

The first would be to claim:

> **"These infrastructures have no connection with one another."**

This claim is contradicted by the sources.

Connections exist between invoicing, transaction data, digital identity, Business Wallets, the Digital Product Passport, sustainability data, taxation and payment.

Some connections are provided for in legal texts or standards.

Others form part of European strategies explicitly dedicated to interoperability.

Others have already been implemented in experiments.

The second excessive conclusion would be to claim:

> **"A European system already uses all these infrastructures to monitor individual environmental footprints and authorize or block purchases."**

The sources examined do not support this claim.

The documentary findings lie between these two positions.

ESTABLISHED:

> The European Union is developing several interoperable digital infrastructures capable of linking identity, businesses, transactions, products, tax data and, depending on the systems concerned, environmental information.

ESTABLISHED:

> The European Commission explicitly seeks synergies and data reuse between several of these infrastructures.

ESTABLISHED / EXPERIMENTED:

> Chains connecting identity, payment, detailed receipts, Business Wallets and tax processing have already been experimented with.

ESTABLISHED:

> A European standard provides that an electronic receipt can be linked to the Digital Product Passport and to verified environmental information relating to the product.

ESTABLISHED / EXPERIMENTED:

> Conditional payment architectures enable an event or information verified by an external system to intervene in the execution of a transaction.

TECHNICALLY DEDUCIBLE:

> These components make it possible to construct an architecture in which environmental data relating to a product could be queried by an external service and the result used in conditional logic surrounding a payment.

NOT ESTABLISHED:

> None of the elements examined demonstrate that this environmental use of conditional payment is currently planned, experimented with or deployed.

NOT ESTABLISHED:

> None of the elements examined demonstrate the existence of a centralized system assigning each individual a comprehensive environmental consumption profile used to control their payments.

The conclusion of the chapter is therefore not that the scenario examined exists.

It is more precise:

> **a significant part of the architecture that would make it technically possible to interconnect transaction, product, environmental, identity and payment data is now documented; several connections are explicitly provided for or experimented with; but the decisive connection transforming environmental data into an imposed rule authorizing or refusing a payment has not been established.**

Chapter 6 — Legal Safeguards

Navigation: ← Back to the table of contents

The previous chapters identified the data collected, the infrastructures concerned and several documented possibilities or mechanisms for interconnection between invoicing, taxation, products, environmental data, digital identity and payment.

However, the existence of a technical capability for interconnection does not mean that its use is legally authorized.

This chapter therefore examines the legal safeguards that may regulate, limit or prohibit certain processing operations or data cross-referencing identified during the investigation.

The analysis notably examines:

- the legal bases enabling processing;
- the purposes for which data may be collected and reused;
- the principle of purpose limitation;
- the principle of data minimization;
- the conditions applicable to cross-referencing data originating from different systems;
- the rules relating to profiling and automated decision-making;
- the rights of data subjects;
- transparency obligations;
- retention and access rules;
- the powers and positions of supervisory authorities, notably the CNIL;
- the requirements of necessity and proportionality;
- any specific safeguards provided for digital identity, the DPP and payment infrastructures;
- the possibilities and conditions for future changes to purposes or legal bases.

The objective is not to presume that a violation exists.

It is to determine, for each capability identified in the previous chapters, whether current law:

> **explicitly authorizes it;**

> **authorizes it under certain conditions;**

> **limits it;**

> **appears to prohibit it;**

> **or does not yet allow a conclusion to be reached.**

Particular attention will be paid to the difference between a protection established in current law and a technical impossibility.

A legal rule may currently limit processing that the architecture would technically enable.

Conversely, the existence of a technical infrastructure does not make it possible to presume that a legal development authorizing new uses will subsequently occur.

The chapter will therefore seek to identify both existing protections and their limitations, without transforming the possibility of legal evolution into an established institutional intention.

Table of contents

6.1 Applicable legal framework

Status: ESTABLISHED LEGAL SAFEGUARDS / IDENTIFIED POINTS OF VIGILANCE

The previous chapters focused primarily on the existence of the data, their circulation and the possibilities for interconnection between different infrastructures.

Chapter 6 raises a different question:

> **is the fact that processing is technically feasible and pursues an objective of general interest sufficient to make it legally permissible?**

The answer is no.

Several levels of law govern the processing operations examined.

The GDPR applies to personal data used within the system

The General Data Protection Regulation applies when information relates to an identified or identifiable natural person S36.

Not all data contained in an invoice therefore necessarily constitute personal data.

An invoice concerning a company may mainly contain information relating to a legal entity.

However, invoicing systems may also contain information that makes it possible to identify natural persons directly or indirectly.

This point is no longer merely theoretical with regard to the use of data originating from the reform for tax purposes.

The CNIL explicitly describes data originating from electronic invoicing and added to the CFVR processing system as **personal data collected** S37.

ESTABLISHED:

> At least some of the data originating from the electronic invoicing reform fall within the scope of personal data protection.

The system therefore does not fall outside the GDPR merely because it primarily concerns economic transactions between businesses.

The reform has a legal basis

A first argument must immediately be ruled out.

The transmission of data to the administration is not implemented without a legal basis.

It results notably from the French General Tax Code and from legislative and regulatory provisions governing electronic invoicing and e-reporting.

The decree governing the system itself explicitly refers to the GDPR and was adopted after consultation with the CNIL S38.

INSUFFICIENT ARGUMENT:

> "The collection is mandatory and carried out without consent, therefore it necessarily violates the GDPR."

The GDPR does not rely solely on consent.

Processing may notably be based on a legal obligation or be necessary for the performance of a task carried out in the public interest provided for by law S36.

The absence of consent from the businesses or persons concerned is therefore not, in itself, sufficient to make the reform unlawful.

The existence of a legal basis does not, however, grant an unlimited right of use

This is where a first important legal distinction appears.

The GDPR requires data to be:

> collected for specified, explicit and legitimate purposes;

and:

> not further processed in a manner incompatible with those purposes S36.

It also requires data to be:

> adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed S36.

Therefore:

```
legal basis
   ≠
general authorization for reuse
```

and:

```
legally mandatory collection
   ≠
unlimited ability to cross-reference data for any future public policy
```

ESTABLISHED LEGAL SAFEGUARD:

> Any subsequent reuse of personal data must remain compatible with the applicable legal framework, notably the purposes and the principles of necessity, proportionality and minimization.

This distinction becomes particularly important in light of the interconnections examined in Chapter 5.

An important finding: invoicing data do in fact feed an algorithmic tax-targeting system

Chapter 2 had left open the question of the automated processing actually applied to data originating from the reform.

The documentation published in 2026 now makes it possible to provide a precise answer.

The CNIL examined the integration of data originating from electronic invoicing into the automated **CFVR — fraud targeting and query enhancement** processing system S37.

This development was subsequently incorporated into the regulatory framework by the Order of 10 July 2026 amending the order establishing CFVR S45.

Data originating from electronic invoicing are therefore now among the categories of data integrated into the CFVR system.

The CNIL further states that part of the CFVR data, together with data originating from electronic invoicing, are to feed the DGFiP's secure data platform so that they can be processed there, notably because of their volume S37.

It notes that:

> their addition substantially increases the volume of data processed;

and that the volume concerned is approximately:

> **2 to 3 billion electronic invoices per year** S37.

The results produced by the processing carried out on this platform can then feed CFVR and be cross-referenced with other information in order to contribute notably to the identification of anomalies and businesses presenting certain tax risks S37.

ESTABLISHED:

> The integration of data originating from electronic invoicing into the CFVR processing system is now based on an adopted regulatory text S45.

ESTABLISHED:

> These data are intended to be processed on a large scale within the DGFiP's data analysis infrastructure for purposes related to tax control and targeting S37-S45.

ESTABLISHED LEGAL SAFEGUARD:

> This integration does not exempt the processing carried out from the applicable principles of purpose limitation, minimization, security, necessity and proportionality S36-S43-S44.

The data are cross-referenced with other analysis results

The CNIL opinion provides a second important element.

The data processed on the platform are intended to produce results that can be cross-referenced with other information used by CFVR in order to obtain, notably, lists of businesses considered to present certain tax risks S37.

The CNIL also indicates that, ultimately, all data from the CFVR processing system are intended to feed the secure data platform.

The actually documented chain therefore becomes:

```
electronic invoicing data
   ↓
DGFiP secure data platform
   ↓
algorithmic processing
   ↓
cross-referencing with other data / results
   ↓
anomaly detection
   ↓
identification of businesses presenting certain risks
   ↓
possible targeting of tax audits
```

ESTABLISHED:

> The cross-referencing and automated analysis of data originating from electronic invoicing with other tax information are no longer merely a technical possibility.

They form part of the documented uses of the CFVR system S37.

The processing extends beyond businesses alone

The history of CFVR described by the CNIL is also worth noting.

Initially developed for business taxpayers, the system was subsequently extended to natural persons involved in the operation of businesses, and then to private individuals S37.

This does not mean that every piece of electronic invoicing data will be associated with every individual.

But it demonstrates that the analytical infrastructure into which these data are now being integrated is not inherently limited to legal entities alone.

POINT OF VIGILANCE:

> The large-scale integration of data originating from electronic invoicing into an infrastructure that already uses different categories of data relating to professionals and natural persons reinforces the importance of rules governing purpose limitation, minimization, authorization and proportionality.

Exchanges with other administrations are also documented

The same CNIL deliberation describes exchanges between the DGFiP and social security bodies within the framework of CFVR S37.

These exchanges have a specific legal basis and are limited to certain purposes.

The CNIL considers these purposes legitimate under the legal framework currently provided for.

ESTABLISHED:

> Legal mechanisms already enable certain administrative data to circulate between public bodies for specified purposes.

However, the CNIL specifically emphasizes:

- data minimization;
- restriction to authorized agents;
- the need-to-know principle;
- the retention period;
- information provided to data subjects;
- the proportionality of exchanges S37.

This observation is essential for the remainder of the investigation.

ESTABLISHED LEGAL SAFEGUARD:

> Interconnection between administrations is not legally unrestricted: it must be based on a legal basis and comply with specified purposes and safeguards.

First area of vulnerability: the progressive expansion of purposes

The reform is initially based notably on tax-related objectives: modernization of VAT collection, combating fraud, pre-filling and improving knowledge of economic activity.

The use of data for tax targeting therefore has a direct connection with several stated purposes.

INSUFFICIENT ARGUMENT AT THIS STAGE:

> The current use of invoicing data by CFVR necessarily constitutes purpose diversion.

The sources examined do not support this conclusion.

Combating fraud and tax control are precisely part of the framework within which this processing is organized.

However, the issue would become legally much more sensitive if the same data were subsequently reused for a substantially different purpose.

For example:

```
collection for a tax purpose
   ↓
retention of a detailed transaction infrastructure
   ↓
reuse for another public policy
   ↓
cross-referencing with other categories of data
```

Such a development would have to be examined in light of purpose limitation, its legal basis, necessity and proportionality S36-S43.

POTENTIAL VULNERABILITY:

> The technical capability to reuse data does not constitute a legal basis allowing new purposes to be freely assigned to them.

Second area of vulnerability: data volume and proportionality

The CNIL itself notes the substantial increase in the volume of data caused by the integration of electronic invoicing into CFVR S37.

The announced volume reaches several billion invoices per year.

However, case law relating to the protection of privacy and personal data requires a balance to be struck between:

> the objective of general interest pursued

and:

> the nature, scope and sensitivity of the data processed, as well as the seriousness of the interference S39-S44.

The relevant legal question is therefore not simply:

> "is combating fraud a legitimate objective?"

It is.

The question is:

> **"are the precise scope of the data collected, their level of detail, their retention period, their cross-referencing and the ways in which they are processed necessary and proportionate to that objective?"**

It is on this ground that legal scrutiny becomes genuinely relevant.

Third area of vulnerability: data protection by design and by default

The principle of minimization does not apply solely to the initial choice of categories of data collected.

Article 25 of the GDPR also requires the controller to implement technical and organizational measures enabling the effective application of data protection principles by design and by default S43.

The Regulation specifies that this requirement notably concerns:

- the amount of personal data collected;
- the extent of their processing;
- their retention period;
- their accessibility.

This provision is particularly relevant to an infrastructure expected to process several billion electronic invoices per year and enable their processing within a platform with significant computing capabilities S37.

The legal question therefore does not concern only the existence of a legal basis allowing the integration of the data.

It also concerns the concrete design of the infrastructure:

> what data are actually necessary?

> for how long?

> for what processing operations?

> accessible to which agents?

> with what level of granularity?

> and what measures technically prevent their use beyond the authorized purposes?

The CNIL specifically requires the secure data platform to maintain strict segregation, that the data transferred to it be processed solely for the intended purposes and that its use not provide access to new recipients who were not originally provided for S37.

ESTABLISHED LEGAL SAFEGUARD:

> The GDPR requires data protection and minimization to be integrated into the very design of the processing and that, by default, only the data necessary for each specific purpose be processed S43.

POINT OF VIGILANCE:

> An increase in technical storage, computing or cross-referencing capabilities does not in itself constitute justification for expanding the data accessible or the processing carried out.

LEGAL QUESTION TO BE DOCUMENTED:

> Do the technical and organizational measures actually implemented in CFVR and in the secure data platform demonstrate, with regard to data originating from electronic invoicing, the effective application of the principles of data minimization and data protection by design and by default?

Fourth area of vulnerability: access control

The CNIL also emphasizes the need to restrict access to a limited number of agents and strictly on a need-to-know basis S37.

It requires the secure platform to:

> maintain strict segregation of data;

> allow their processing only for the intended purposes;

> not provide access to new recipients who were not originally provided for.

This requirement is particularly important for our investigation.

It means that an infrastructure technically capable of hosting several categories of data cannot legally become a general-purpose environment for data reuse without a new legal framework.

ESTABLISHED LEGAL SAFEGUARD:

> The segregation of purposes and access currently constitutes a legally significant safeguard against generalized data reuse.

POINT OF VIGILANCE:

> Any extension of the categories of persons with access, the purposes or the data being cross-referenced must be examined separately in order to determine whether the existing legal basis and safeguards remain sufficient.

A fundamental distinction emerges

The result of this initial analysis differs from two extreme positions.

It would be legally incorrect to claim:

> **"The reform violates the GDPR because the data are transmitted without consent."**

A legal basis exists, and consent is not the only basis on which processing may be carried out.

But it would also be incorrect to claim:

> **"Since the collection is provided for by law, the administration can then do whatever it wishes with the data."**

The GDPR and constitutional and European requirements for the protection of privacy continue to govern:

- the purposes;
- the categories of data;
- their necessity;
- their proportionality;
- their retention;
- their recipients;
- their cross-referencing;
- automated decisions;
- security measures.

First legal conclusion

ESTABLISHED:

> The reform is based on a legal and regulatory framework and has been subject to consultation with the CNIL.

ESTABLISHED:

> Data originating from electronic invoicing include personal data subject to the safeguards of the GDPR.

ESTABLISHED:

> These data are intended to feed a DGFiP infrastructure enabling their large-scale algorithmic processing for tax targeting.

ESTABLISHED:

> The CNIL itself notes a substantial increase in data volume and identifies risks relating to minimization, access, retention, security, algorithmic bias and automation.

ESTABLISHED:

> Certain exchanges and cross-referencing between administrations are legally possible when provided for by law and when their purposes are specified.

ESTABLISHED LEGAL SAFEGUARD:

> Legally established data collection does not permit unlimited reuse of the data for any purpose.

POTENTIAL VULNERABILITY:

> Any substantial extension of the purposes, categories of data, recipients or matching mechanisms must be able to satisfy the requirements of a legal basis, necessity, minimization and proportionality.

TO BE ESTABLISHED:

> The exact scope of the safeguards surrounding each processing operation resulting from the reform and the possibility of legally challenging certain extensions or methods of processing must be examined in the following sections.

What 6.1 changes in the investigation

An element that remained partially unresolved in the earlier chapters can now be clarified.

The following chain is documented:

```
electronic invoicing
   ↓
personal and economic data on a very large scale
   ↓
DGFiP secure data platform
   ↓
algorithmic processing
   ↓
cross-referencing / analysis
   ↓
anomaly detection and tax targeting
   ↓
possible human decision to initiate an audit
```

The legal question is therefore no longer whether invoicing data **can technically be processed and cross-referenced on a large scale**.

Such processing is now documented in the tax domain.

The question becomes:

> **how far can this processing legally go before it encounters the principles of purpose limitation, minimization, necessity, proportionality and protection against certain automated decisions?**

It is this boundary that the following sections must seek to identify.

6.2 Purposes of processing and data reuse

Status: ESTABLISHED LEGAL SAFEGUARDS / IDENTIFIED LEGAL LATITUDE / BOUNDARIES TO BE ESTABLISHED

The principle of purpose limitation constitutes one of the main legal safeguards applicable to the architectures examined in the previous chapters.

But its scope must be described precisely.

An overly simplistic interpretation would be to consider that:

> **"any new use of data for a purpose different from the one stated when it was collected is prohibited."**

The GDPR does not establish such an absolute prohibition.

On the contrary, it provides several mechanisms allowing, under certain conditions, certain further processing operations S36-S43-S46.

A purpose must be specified, explicit and legitimate

The initial principle remains clear.

Personal data must be collected for specified, explicit and legitimate purposes and must not be further processed in a manner incompatible with those purposes S36-S43.

This rule prevents, in principle, an infrastructure established for a specific purpose from becoming, solely by virtue of its technical existence, a general repository of data that can be used for any future purpose.

It therefore requires a distinction between:

```
technical capability for reuse
   ↓
legally defined purpose
   ↓
legal basis
   ↓
necessity / proportionality
   ↓
authorized processing
```

The first step is never sufficient to demonstrate the subsequent ones.

LEGAL SAFEGUARD:

> The technical availability of data does not, in itself, constitute a purpose or a legal basis allowing its use.

A new purpose is not, however, automatically prohibited

Article 6(4) of the GDPR explicitly provides for cases in which data are further processed for a purpose other than the one that justified their initial collection S46.

Where such further processing is based neither on the data subject's consent nor on a relevant provision of Union or Member State law, the controller must notably determine whether the new purpose is compatible with the initial purpose.

The Regulation provides several criteria for this assessment:

- the link between the initial purpose and the further purpose;
- the context in which the data were collected;
- the nature of the data;
- the possible consequences of the new processing for the individuals concerned;
- the safeguards implemented, notably encryption or pseudonymization S46.

There is therefore, in legal terms, a:

> **purpose compatibility test.**

LEGAL LATITUDE:

> Data collected for a specified purpose may, under certain conditions, be subject to further processing compatible with that purpose.

This means that:

```
new use
   ≠
automatic illegality
```

But also that:

```
new use
   ≠
automatic compatibility
```

Compatibility must be assessed in light of the processing actually envisaged.

A second route exists: intervention through law

Article 6(4) reveals a second important possibility for this investigation.

The compatibility test mechanism it describes concerns cases in which further processing is not based, notably, on Union or Member State law constituting a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 of the GDPR S46.

In other words, the evolution of uses does not depend solely on compatibility with the initial purpose.

The law may also provide a framework for certain new processing operations or certain restrictions under the conditions laid down by the GDPR.

LEGAL LATITUDE:

> The legal framework may evolve and permit certain further processing operations that do not rely solely on compatibility with the initial purpose.

This latitude is fundamental to the analysis of the architectures examined in this repository.

An existing technical infrastructure may currently be legally limited to certain purposes, without that limitation necessarily constituting a definitive legal impossibility.

A change in the law could modify the processing operations that are authorized.

This does not, however, make it possible to presume that such a change will occur.

The tax domain explicitly benefits from this latitude

This possibility is not purely abstract in the domain examined.

Article 23 of the GDPR expressly provides that Union or national law may, under certain conditions, restrict the scope of several obligations and rights provided for by the Regulation in order to safeguard certain important objectives of general public interest S47.

The areas explicitly mentioned notably include:

- important economic or financial interests;
- monetary matters;
- budgetary matters;
- taxation matters;

- social security;
- certain monitoring, inspection or regulatory functions connected to the exercise of official authority S47.

This possibility remains subject to conditions.

The measure must notably:

> respect the essence of fundamental rights and freedoms;

and:

> be necessary and proportionate in a democratic society S47.

LEGAL SAFEGUARD:

> The GDPR does not authorize a general and uncontrolled restriction of rights in the name of tax interests.

LEGAL LATITUDE:

> The GDPR explicitly provides for the possibility for the legislature to adjust certain safeguards or rights where tax objectives or monitoring functions justify it, subject notably to the requirements of necessity and proportionality.

This latitude is already being used within the CFVR framework

The connection with the investigation becomes particularly concrete in the Order of 10 July 2026 amending CFVR S45-S47.

This Order:

- integrates data originating from electronic invoicing among the data processed;
- extends or specifies several data sources used by the system;
- organizes certain access and data transfers;
- and explicitly refers to points (e) and (h) of Article 23(1) of the GDPR S45-S47.

This is therefore not merely a theoretical possibility contained in the European regulation.

The current regulatory framework governing CFVR already makes use of the legal mechanisms allowing certain restrictions in the context of taxation and monitoring functions.

ESTABLISHED:

> The CFVR legal framework explicitly refers to the possibilities for restriction provided for by Article 23 of the GDPR for certain objectives of general public interest and certain monitoring functions S45-S47.

The law can therefore shift the boundary without removing all safeguards

This observation leads to an important distinction.

It would be incorrect to write:

> **"The purposes stated today definitively prohibit any new future use."**

The law can evolve.

It would be equally incorrect to write:

> **"It is sufficient to adopt a new legal text to make any use of the data legally possible."**

New provisions remain subject to the applicable higher-ranking legal norms.

Depending on the circumstances, these may notably include:

- the GDPR;
- the Charter of Fundamental Rights of the European Union;
- the right to respect for private life;
- the necessity test;
- the proportionality test;
- the principle of minimization;
- the safeguards applicable to data subjects S39-S43-S44-S46-S47.

The actual boundary is therefore not:

```
possible
   /
impossible
```

but rather:

```
currently authorized use
   ↓
envisaged extension
   ↓
possible compatibility
   or
new legal basis
   ↓
necessity test
   ↓
proportionality test
   ↓
applicable safeguards
```

First legal vulnerability: progressive expansion may be lawful

This conclusion reveals a particular vulnerability.

It does not necessarily result from a violation of the law.

On the contrary, it results from the ability of the law to progressively expand the scope of authorized processing.

An infrastructure may therefore successively undergo:

```
purpose A
   ↓
compatible extension A → A+
   ↓
new legal basis
   ↓
extension towards B
   ↓
new authorized cross-referencing
```

Each step may be legally regulated and yet, over time, lead to an architecture whose scope is much broader than when it was created.

LEGAL VULNERABILITY:

> Purpose limitation constitutes a safeguard against incompatible reuse that lacks a sufficient legal basis, but it does not guarantee that the legal scope of processing will remain unchanged.

IMPORTANT:

> This possibility of evolution demonstrates neither that a particular extension is envisaged nor that it would be legally permissible.

It demonstrates only that:

> **the legal boundary can evolve without requiring modification of the technical architecture already available.**

Second vulnerability: the accumulation of extensions

The legal analysis of an extension is generally carried out in relation to a specific processing operation and purpose.

However, the investigation also examines the cumulative effect of several infrastructures and successive developments.

A succession of individually justified extensions may progressively increase:

- the amount of data available;
- the number of sources;
- the number of possible cross-references;
- the number of recipients;
- the period during which certain information remains usable;
- the capacity for profiling or analysis.

The question then becomes:

> **at what point does the cumulative effect of several legally grounded extensions sufficiently alter the nature or intensity of the processing to require a new assessment of necessity and proportionality?**

TO BE ESTABLISHED:

> To what extent does the applicable law require the proportionality of not only each extension considered individually, but also the architecture resulting from their accumulation, to be reassessed?

This question must be considered alongside the analyses of necessity, proportionality and impact examined in the following sections.

An essential boundary for the interconnections examined in Chapter 5

This analysis also makes it possible to preserve an essential methodological boundary regarding the chains examined previously.

Chapter 5 identified several technical or experimental capabilities connecting notably:

```
transaction
   ↓
product
   ↓
DPP
   ↓
environmental data
```

as well as:

```
external data
   ↓
condition
   ↓
conditional payment
```

The existence of the further processing mechanism provided for by the GDPR does not make it possible to transform these technical possibilities into legally authorized uses.

Nor does it make it possible to conclude that a future legal basis will be created to connect them.

NOT ESTABLISHED:

> No element examined in this section establishes that environmental data from the DPP can currently be used to determine the authorization, refusal or limitation of a payment.

LEGALLY DEDUCIBLE:

> If such an interconnection involving personal data were to be implemented, its compliance would have to be examined in light of its purpose, its legal basis and the applicable safeguards, as well as, depending on the mechanism used, the requirements of necessity, proportionality and minimization.

This distinction prevents confusion between:

```
legally possible evolution in theory
   ↓
   and
legally authorized use today
```

Conclusion of 6.2

ESTABLISHED:

> The GDPR prohibits further processing incompatible with the initial purposes where no other relevant legal basis permits the processing S36-S43-S46.

ESTABLISHED:

> The GDPR provides a mechanism for assessing the compatibility of a further purpose with the initial purpose S46.

ESTABLISHED:

> Union or national law may also provide for certain restrictions or processing operations under the conditions laid down by the GDPR, notably for important objectives in the field of taxation and for certain monitoring functions S46-S47.

ESTABLISHED:

> The CFVR framework as amended in July 2026 explicitly refers to points (e) and (h) of Article 23(1) of the GDPR S45-S47.

LEGAL SAFEGUARD:

> An extension of uses does not become lawful merely because it is technically possible or pursues an objective of general interest.

LEGAL LATITUDE:

> The law nevertheless permits certain compatible forms of reuse and may evolve the scope of authorized processing, subject to the applicable conditions and safeguards.

LEGAL VULNERABILITY:

> Purpose limitation protects against certain forms of reuse, but does not permanently freeze the legal scope of a data infrastructure.

TO BE ESTABLISHED:

> How far can successive extensions of purposes, data sources and recipients accumulate before their overall effect requires a new assessment of necessity and proportionality?

NOT ESTABLISHED:

> Nothing in the sources examined here demonstrates that a legal development is currently envisaged to connect environmental data from the DPP to the authorization, refusal or limitation of a payment.

6.3 Data cross-referencing, matching and interconnection

Status: ESTABLISHED INTERCONNECTIONS / DOCUMENTED SAFEGUARDS / IDENTIFIED VULNERABILITIES AND BLIND SPOTS

The previous chapters showed that several of the infrastructures examined have cross-referencing or interconnection capabilities.

In the tax domain, this issue is now no longer merely technical.

The CFVR processing system already constitutes an architecture fed by numerous data sources and enabling their analysis or cross-referencing S37-S45.

The legal issue therefore becomes twofold:

> **which interconnections are actually authorized?**

and:

> **what safeguards prevent a large-scale data-matching infrastructure from itself becoming a disproportionate source of risk, notably in the event of compromise, misuse or expanded access?**

CFVR already constitutes a multi-source infrastructure

The Order amending CFVR in July 2026 is not limited to adding data originating from electronic invoicing S45.

The processing system is fed by numerous other sources.

The regulatory list notably includes data originating from:

- tax records;
- tax returns;
- withholding tax;
- property and housing occupancy data;
- inheritances;
- bank account details declared by tax households;
- cross-border payments recorded in CESOP;
- intra-EU VAT;
- exchanges of goods within the European Union;
- processing systems relating to vehicle tax clearance certificates;
- data processing systems originating from social security bodies;
- publicly accessible data collected from certain online platforms;

- and, now, electronic invoicing S45.

The Order also provides for data concerning natural persons that are necessary for certain work relating to the intensity of economic activity S45.

ESTABLISHED:

> CFVR is not a database limited solely to data originating from electronic invoicing.

It constitutes an analytical infrastructure fed by a much broader range of tax, economic and administrative sources and, in certain cases, data relating to natural persons.

Cross-referencing is a documented function of the system

The CNIL explicitly describes the intended processing of the new electronic invoicing data S37.

Part of the CFVR data, together with data originating from electronic invoicing, are intended to feed the DGFiP's secure data platform.

The results of queries performed on this platform can then be cross-referenced with data originating from CFVR in order to obtain, notably, lists of businesses considered to present certain risks.

Ultimately:

> **all CFVR data are intended to feed this platform** S37.

The documented chain therefore becomes:

```
multiple administrative / tax sources
   ↓
CFVR
   ↓
electronic invoicing data
   +
other CFVR data
   ↓
secure data platform
   ↓
queries / models / analyses
   ↓
cross-referencing of results
   ↓
anomaly detection
   ↓
selection of cases presenting certain risks
```

ESTABLISHED:

> The matching of multiple datasets constitutes an actual and legally organized function of CFVR S37-S45.

It is therefore no longer merely a technically conceivable interconnection.

Exchanges between administrations further broaden the scope

The documented interconnections also extend beyond the DGFiP alone.

Article L. 152 of the French Tax Procedures Code allows certain exchanges between the tax administration and social security bodies.

The CFVR system has been adapted accordingly S37-S45.

Data may be transmitted to social security bodies for certain tasks relating to the verification of the basis for social security contributions.

Conversely, certain data communicated by these bodies may also feed CFVR.

The CNIL notably mentions information relating to:

- undeclared work;
- remuneration;
- the results of tax audits S37.

ESTABLISHED:

> There is therefore a legally organized two-way flow of data between the tax administration and certain social security bodies.

This flow is based on a legal basis and specified purposes.

The scope of persons with access to the system is also evolving

The July 2026 Order provides for several categories of authorized agents who may access the data necessary for modelling and visualization work S45.

These notably include agents belonging to:

- the national data analysis network;
- interregional programming structures;
- certain specialized national services;
- departmental public finance directorates;
- the National Directorate of Tax Investigations.

Useful results are also accessible, on a need-to-know basis, to certain agents responsible for case management, programming and auditing, as well as to certain authorized agents of social security bodies S45.

The CNIL indicates that members of the national network must be individually authorized, trained and supervised, and that certain queries may be approved or rejected by the competent office S37.

LEGAL AND ORGANIZATIONAL SAFEGUARD:

> Access is not presented as being indiscriminately open to all public officials.

It is based on authorizations and must be limited to the need-to-know principle S37-S45.

Large-scale cross-referencing is itself a recognized risk factor

This architecture must, however, be considered in light of the criteria used by the CNIL for data protection impact assessments.

The criteria used to identify processing operations likely to result in a high risk notably include:

- large-scale processing;
- matching or combining datasets;
- evaluation or scoring;
- the use of innovative technologies or methods S49.

CFVR publicly exhibits several characteristics corresponding to these criteria:

```
massive volume
   +
data cross-referencing
   +
analysis / targeting
   +
algorithmic methods
```

The CNIL itself notes that the arrival of electronic invoicing **substantially** increases the volume of data processed and refers to several billion invoices per year S37.

MAJOR POINT OF VIGILANCE:

> The simultaneous increase in data volume, the number of sources and matching capabilities increases not only the analytical power of the system, but also the potential consequences of an error, misuse or compromise.

First vulnerability: concentration increases the potential impact of a compromise

A database or platform capable of matching numerous categories of data presents a different risk from several strictly segregated databases.

A compromise would not necessarily affect only a single isolated piece of information.

Depending on the access actually obtained, it could make it possible to match several categories of information.

The GDPR specifically requires the level of security to be appropriate to:

- the nature of the data;
- their scope;
- the context of the processing;

- the likelihood of the risk;
- its severity S48.

Here, the CNIL goes much further than a general statement.

In its opinion concerning CFVR, it explicitly notes:

> the massive volume of data;

> their sensitivity;

> the evolution of the threat;

> and the evolution of cyberattack methods S37.

LEGAL AND TECHNICAL VULNERABILITY:

> The more the architecture concentrates data, sources and matching capabilities, the higher the level of security that can reasonably be required.

This does not mean that CFVR is currently compromised or insufficiently secured.

It means that:

> **the change in scale also changes the level of risk over which the administration must be able to demonstrate effective control.**

The CNIL itself calls for enhanced protection against compromised access

The CNIL opinion provides a particularly concrete element here S37.

It welcomes the ministry's commitment to systematically implement:

- two-factor authentication;
- access only from secure devices.

However, the CNIL goes further regarding connection and activity logs.

It considers that logging should be accompanied by mechanisms enabling notably:

- proactive analysis of events;
- detection of unexpected behavior;
- generation of alerts;
- immediate blocking of the accounts concerned until doubts have been resolved by management S37.

DOCUMENTED SAFEGUARD:

> Two-factor authentication and the use of secure devices are the subject of a commitment by the ministry that was positively noted by the CNIL.

DOCUMENTARY BLIND SPOT:

> In its opinion published in 2026, the CNIL specifically calls on the ministry to implement proactive mechanisms for log analysis, alerts and account blocking in the event of unexpected behavior.

The public sources examined here do not yet make it possible to establish whether all of these recommended mechanisms have actually been deployed across all the environments concerned.

TO BE ESTABLISHED:

> Have the proactive detection and blocking mechanisms requested by the CNIL since been effectively deployed, with what coverage and according to what procedures?

This is a very concrete question that can be addressed to the administration.

Second vulnerability: the risk does not arise solely from an external attack

The security of an infrastructure of this nature does not concern only a hacker gaining access from the Internet.

Article 32 of the GDPR also covers risks of unauthorized access or disclosure S48.

Access control therefore becomes fundamental.

An infrastructure bringing together:

```
more data
   +
more sources
   +
more analyses
   +
several categories of persons with access
```

mechanically increases the number of situations in which an incorrect authorization, a compromised account, a misconfiguration or misuse could have significant consequences.

This is precisely why the CNIL emphasizes:

- limiting the number of agents;
- individual authorization;
- the strict need-to-know principle;
- supervision;
- logging;
- behavioral analysis S37-S50.

VULNERABILITY:

> The security of the system depends not only on protecting its IT perimeter but also on the ongoing quality of identity management, access authorizations and the detection of abnormal use.

Third vulnerability: interconnection expands the trust surface

Exchanges with other administrations add another dimension.

The CNIL notes the use of a secure file-transfer tool with state-of-the-art encryption for exchanges with social security bodies S37.

This is an important safeguard.

But an interconnection necessarily creates several environments involved:

```
organization A
   ↓
transfer mechanism
   ↓
organization B
```

Overall security therefore no longer depends solely on the original infrastructure.

It also depends on:

- the authorizations within each organization;
- the security of each organization's equipment;
- any copies that may be created;
- retention periods;
- effective deletion;
- logging;
- the ability to detect abnormal use or transfer.

DOCUMENTED SAFEGUARD:

> Exchanges between the DGFiP and social security bodies must use a secure and encrypted transfer mechanism S37.

STRUCTURAL VULNERABILITY:

> Any increase in the number of recipients or environments in which the data are accessible expands the surface across which confidentiality, integrity and access-control safeguards must be maintained.

This is not evidence of a current weakness in any particular organization.

It is a consequence of the distributed architecture itself.

A very concrete blind spot emerges regarding the retention of exchanged data

The CNIL opinion contains a particularly noteworthy observation concerning exchanges with social security bodies S37.

The Commission notes that the draft Order submitted to it:

> **did not specify the retention period for data transmitted as part of these exchanges.**

It then reiterates that exchanges between administrations are permitted only if their arrangements remain proportionate to the objectives pursued and emphasizes the need to limit retention to the period necessary S37.

IDENTIFIED DOCUMENTARY BLIND SPOT:

> The text submitted to the CNIL did not itself determine the retention period for data transferred between the DGFiP and social security bodies.

This does not demonstrate that the data are retained without limit.

Retention periods may be provided for in other legal texts, agreements, internal policies or recipient processing systems.

But this raises a legally verifiable question:

TO BE ESTABLISHED:

> For each category of data transferred between CFVR and social security bodies, what is the maximum retention period applicable at the recipient organization, by which legal text or document is it determined, and how is its effective deletion monitored?

This point may be far more relevant than a general criticism of data retention.

Fourth vulnerability: a change in risk may require a new assessment

The GDPR contains a mechanism that is particularly relevant for monitoring the evolution of this type of architecture.

Article 35 provides that, where a data protection impact assessment exists, the controller must review whether the processing remains compliant with that assessment when there is a change in the risk S48.

Several transformations are now documented:

- the arrival of a new massive category of data;
- several billion additional invoices;
- the use of an infrastructure with enhanced computing capabilities;
- cross-referencing with other information;
- the development of new learning methods;
- organizational expansion of the analysis network;
- new relationships with social security bodies S37-S45.

MAJOR LEGAL QUESTION:

> Have these developments been incorporated into an existing DPIA, or have they resulted in a new analysis or a formal reassessment of the risk in accordance with Article 35 of the GDPR?

The public sources examined do not, at this stage, make it possible to answer this question fully.

DOCUMENTARY BLIND SPOT:

> The possible existence of an internal DPIA should not be confused with its absence. However, we do not yet have a public document making it possible to establish precisely which impact assessment covers the entire CFVR + secure data platform + electronic invoicing + new cross-referencing + inter-administration exchanges chain.

This distinction is essential.

A DPIA would be particularly relevant in light of the CNIL's criteria

Without prejudging the legal analysis already carried out by the DGFiP, several high-risk criteria described by the CNIL objectively appear in the public documentation S37-S49:

```
large-scale processing            ✓
matching of datasets              ✓
evaluation / targeting            ✓
algorithmic methods               ✓
```

The presence of these characteristics makes it particularly important to be able to verify:

- the exact description of the processing examined in the DPIA;
- the categories of data covered;
- the interconnections taken into account;
- the risks of compromise;
- the risks related to access authorizations;
- the risks of excessive correlation;
- the measures taken to mitigate these risks;
- successive changes to the assessment.

TO BE ESTABLISHED:

> Which DPIA currently covers the processing of electronic invoicing data within CFVR and the secure data platform?

> When was it last revised?

> Does it take into account the arrival of several billion invoices per year?

> Does it take into account the cross-referencing carried out on the secure data platform?

> Does it take into account exchanges with social security bodies?

> Does it take into account the evolution of algorithmic methods and the expansion of the network of analysts?

Fifth vulnerability: segregation becomes a critical safeguard

The CNIL imposes a particularly strong condition regarding the secure data platform S37.

It considers that its use requires:

- strict segregation;
- that the data transferred to it be processed solely for the purposes currently provided for;
- that no new unauthorized person be able to access them;
- that technical protections be equivalent to those existing outside the secure data platform.

This wording shows that segregation is not a secondary issue.

It constitutes one of the safeguards preventing technical concentration from leading to functional opening of the data.

LEGAL AND TECHNICAL SAFEGUARD:

> The secure data platform must not become, solely because it hosts several datasets, an infrastructure enabling their general use by unauthorized users or for unauthorized purposes.

POTENTIAL VULNERABILITY:

> The legal robustness of the architecture therefore depends directly on technical segregation safeguards that cannot be fully verified from the public documentation examined.

TO BE ESTABLISHED:

> How are the separations between datasets, purposes, processing operations and access profiles technically implemented and audited within the secure data platform?

The security issue therefore cannot be reduced to "anything can be hacked"

It would be legally insufficient to claim:

> **"Any IT system can be hacked, therefore this architecture is dangerous."**

Zero risk does not exist, and the GDPR does not require the absolute impossibility of a compromise.

The legal requirement is different.

It concerns the relationship between:

```
level of risk
   ↓
measures implemented
   ↓
state of the art
   ↓
monitoring
   ↓
regular reassessment
   ↓
ability to demonstrate compliance
```

S48-S50

The analysis must therefore focus on this ground.

What 6.3 already makes it possible to raise

Several specific questions can now be addressed to the DGFiP, the CNIL or the legislature:

> **1. Which DPIA currently covers CFVR following the integration of electronic invoicing and its processing within the secure data platform?**

> **2. When was this DPIA last reassessed in light of the massive change in data volume and the new interconnections?**

> **3. Have the proactive mechanisms for detecting abnormal behavior and immediately blocking accounts recommended by the CNIL been fully deployed?**

> **4. What maximum retention period applies to data transferred between the DGFiP and each social security body?**

> **5. How is the effective deletion of copies received by recipient organizations monitored?**

> **6. How is segregation between datasets, purposes and categories of users technically guaranteed and audited within the secure data platform?**

> **7. What independent audits or regular tests make it possible to demonstrate that the level of security remains appropriate as threats evolve?**

These questions do not presume any violation.

They request evidence of the safeguards that the law specifically makes relevant.

Conclusion of 6.3

ESTABLISHED:

> CFVR already cross-references numerous tax, economic, administrative and social data sources and now integrates data originating from electronic invoicing S37-S45.

ESTABLISHED:

> Electronic invoicing data are intended to be processed within the secure data platform, and the resulting outputs may be cross-referenced with other information used by CFVR S37.

ESTABLISHED:

> Bidirectional exchanges of certain data are legally organized between the DGFiP and social security bodies S37-S45.

ESTABLISHED:

> The CNIL explicitly considers that the massive volume, the sensitivity of the data and the evolution of cyberattack methods require particular vigilance S37.

LEGAL SAFEGUARD:

> The GDPR requires a level of security appropriate to the risk, as well as reassessment when changes in processing operations result in a change in risk S48.

DOCUMENTED SAFEGUARD:

> The CNIL notably records commitments concerning two-factor authentication, secure devices, segregation and the limitation of access authorizations S37.

DOCUMENTARY BLIND SPOT:

> The public sources examined do not yet make it possible to establish whether all the proactive detection and blocking measures recommended by the CNIL have actually been deployed.

DOCUMENTARY BLIND SPOT:

> The draft examined by the CNIL did not specify the retention period for data transmitted to social security bodies; the precise regime applicable to each copy held by recipients remains to be established S37.

DOCUMENTARY BLIND SPOT:

> We have not yet identified a public DPIA making it possible to verify precisely how the entire CFVR + secure data platform + electronic invoicing + new cross-referencing + inter-administration exchanges architecture was assessed.

LEGAL VULNERABILITY:

> The simultaneous increase in data volume, the number of sources, matching capabilities and categories of persons with access increases the potential consequences of a compromise or misuse and therefore reinforces the requirements for security, segregation and risk reassessment.

TO BE ESTABLISHED:

> Can the administration demonstrate that the technical and organizational measures and impact assessments have been reassessed to match the change in scale introduced in 2026?

NOT ESTABLISHED:

> No element identified makes it possible to claim that CFVR or the secure data platform have suffered a compromise or that the security measures currently deployed are legally insufficient.

6.4 Profiling and automated decision-making

Status: ESTABLISHED ALGORITHMIC PROCESSING / DOCUMENTED HUMAN SAFEGUARD / IDENTIFIED LEGAL BOUNDARY / VULNERABILITIES TO BE ESTABLISHED

The previous sections established that data originating from electronic invoicing are intended to be processed on a large scale, cross-referenced with other information and used in a processing system enabling, notably, the identification of anomalies and businesses presenting certain tax risks S37-S45.

This architecture directly raises an additional legal question:

> **at what point does processing that analyzes, classifies or selects persons or businesses cease to be merely a decision-support tool and become sufficiently determinative to fall within the safeguards applicable to automated decisions?**

This boundary is particularly important because European law does not consider only the formal existence of an algorithm.

It also considers its concrete role in the resulting decision.

Profiling and automated decision-making are not synonymous

A first distinction must be maintained.

Profiling consists of using personal data to evaluate certain personal aspects relating to a natural person.

An automated decision may be based on profiling, but the two concepts are not the same S36-S43.

Processing may therefore:

```
analyze data
   ↓
produce a score / signal / classification
   ↓
without itself making
a decision producing a legal effect
```

Conversely, a decision may be fully automated without necessarily being based on prior profiling.

METHODOLOGICAL SAFEGUARD:

> The existence of algorithms, models or classifications is not, in itself, sufficient to demonstrate the existence of an automated individual decision prohibited or specifically regulated by Article 22 of the GDPR.

Article 22 nevertheless establishes an important boundary

Article 22 of the GDPR recognizes the data subject's right not to be subject to a decision based solely on automated processing, including profiling, where that decision:

- produces legal effects concerning them;
- or similarly significantly affects them S36-S43.

Exceptions exist.

Such a decision may notably be authorized where it is provided for by Union or Member State law and appropriate measures safeguard the rights, freedoms and legitimate interests of the individuals concerned S43.

The principle is therefore not:

```
algorithm
   =
prohibition
```

The legal question is more precise:

```
automated processing
   ↓
decision
   ↓
solely automated nature
   ↓
legal or significant effect
   ↓
Article 22
```

CFVR is currently upstream of this boundary according to the documented system

The public documentation relating to CFVR contains a particularly important safeguard here.

The CNIL indicates that the purpose of the processing is:

> to guide and inform the analysis carried out by agents,

and specifies that:

> **only agents can decide to initiate a tax audit procedure** S37.

It emphasizes this separation again when examining algorithmic methods.

The alerts generated by CFVR must remain a tool enabling agents to assess whether or not it is appropriate to open an audit.

They must not replace their analysis S37.

ESTABLISHED:

> The legally and organizationally documented operation of CFVR does not provide for an algorithm to decide on its own to initiate a tax audit.

LEGAL AND ORGANIZATIONAL SAFEGUARD:

> Human analysis must take place before an audit is initiated.

This safeguard therefore prevents claiming, on the basis of the sources currently available:

> **"CFVR automatically initiates tax audits."**

This claim is not established.

But the CNIL itself considers this human intervention indispensable

The wording used by the CNIL is particularly important.

It considers it:

> **indispensable to the balance of the system**

that the alerts generated must under no circumstances replace the analysis carried out by agents S37.

It also asks the ministry to guarantee:

> **effective human oversight and decision-making** S37.

It notably recommends:

- appropriate documentation for analysts;
- regular training;
- a tax analysis of the documents in each case;
- taking into account the latest available tax returns S37.

The CNIL describes these measures as essential to prevent:

> **the automation of the initiation of tax audits** S37.

This wording reveals a very clear legal and organizational boundary.

```
CFVR
   ↓
algorithmic alert
   ↓
EFFECTIVE HUMAN ANALYSIS
   ↓
possible decision
```

The robustness of the safeguard therefore depends on what actually happens at the central stage.

SCHUFA prevents the issue from being reduced to the formal presence of a human

The case law of the Court of Justice provides a major element here.

In the SCHUFA case, the Court had to examine a system in which a company automatically generated a probability value concerning an individual, then transmitted that value to a third party that formally made the final decision S51.

There were therefore two distinct stages:

```
automated system
   ↓
score
   ↓
third party
   ↓
decision
```

The Court nevertheless held that the automated establishment of the score could itself constitute an automated individual decision within the meaning of Article 22 where the third party's decision depended **in a determining manner** on that value S51.

PRINCIPLE ESTABLISHED BY CASE LAW:

> The existence of a human decision-maker or a third party at the end of the chain is therefore not necessarily sufficient to exclude Article 22 where the automated result plays, in practice, a determining role in the final decision.

This case law did not concern CFVR and does not make it possible to automatically transpose its conclusion to tax audits.

But it provides a particularly relevant criterion for examining this type of architecture.

First legal vulnerability: human intervention must be genuine, not merely formal

The question concerning CFVR therefore becomes more precise.

It is not merely:

> **"does a human click the final button?"**

It is:

> **"does this human genuinely have the information, time, expertise and autonomy necessary to challenge the signal produced by the system?"**

The CNIL itself appears to identify this difficulty, since it calls for **effective** human oversight and decision-making S37.

LEGAL VULNERABILITY:

> If human analysis were to become purely formal and algorithmic alerts were, in practice, to determine the initiation of audits, the legal classification of the process would have to be reassessed in light notably of Article 22 and the SCHUFA case law S43-S51.

NOT ESTABLISHED:

> The sources examined do not demonstrate that such de facto automation currently exists within CFVR.

TO BE ESTABLISHED:

> What proportion of CFVR alerts submitted to agents are ultimately accepted or rejected following human analysis?

> What elements make it possible to concretely assess the agents' ability to disregard an algorithmic recommendation?

> Are there indicators making it possible to identify near-systematic validation of alerts generated by certain models, services or categories of agents?

These data would make it possible to assess the actual effectiveness of the human safeguard.

A second vulnerability emerges: the algorithmic feedback loop

The CNIL explicitly identifies another issue S37.

The results of past tax audits are used to develop the models employed within CFVR.

This potentially creates a loop:

```
model
   ↓
selection of a population
   ↓
audits
   ↓
audit results
   ↓
new training data
   ↓
new model
   ↓
new selection
```

The issue arises when an initial bias influences the audits carried out.

Populations subject to more audits mechanically generate more data resulting from audits.

These data can then feed future models.

The CNIL specifically describes the risk of an amplification leading to a concentration of audits on certain populations or categories of entities that would no longer be justified by the current prevalence of fraud S37.

ESTABLISHED:

> The CNIL explicitly identifies a risk of bias amplification within CFVR due to the reuse of past audit results to develop the models.

This is therefore not a hypothetical vulnerability invented by the investigation.

The 50% safeguard is noteworthy but acknowledged as insufficient on its own

The ministry has introduced a specific safeguard.

It limits to 50% the proportion of tax audits initiated by agents following the analysis of signals originating from CFVR S37.

The CNIL considers this measure useful for limiting the development of significant biases.

But it immediately adds that:

> **this limitation is not sufficient, on its own, to prevent all risks of significant bias** S37.

It therefore also calls for:

- analyses concerning the explainability of algorithms;
- critical assessments of biases that may emerge;
- monitoring of the effectiveness of the safeguards S37.

The ministry has committed to carrying out these studies and reporting on them in CFVR activity reports.

DOCUMENTED SAFEGUARD:

> The ministry limits to 50% the proportion of audits initiated following CFVR signals.

EXPLICITLY ACKNOWLEDGED LIMITATION:

> The CNIL itself considers that this safeguard is not sufficient to eliminate all risks of bias.

TO BE ESTABLISHED:

> Have the announced studies on explainability and bias been carried out?

> What results have they produced?

> What indicators make it possible to verify that certain populations or categories of entities do not become progressively overrepresented in audits solely as a result of a learning feedback loop?

Unsupervised learning further increases the significance of the issue

The CNIL also notes the development of new learning methods within CFVR, notably so-called unsupervised methods S37.

In this type of method, the model seeks notably to distinguish behaviors considered normal or abnormal without prior labelling.

The CNIL considers that:

- the massive expansion of data;
- the development of these new methods;

have the effect of amplifying the risks associated with algorithms and bias S37.

This development is particularly important with the arrival of data originating from several billion invoices.

The chain becomes:

```
massive datasets
   ↓
automated detection of patterns / anomalies
   ↓
classification or alert
   ↓
list of businesses considered at risk
   ↓
human analysis
   ↓
possible audit
```

MAJOR POINT OF VIGILANCE:

> The more complex the operation of the model becomes and the more it depends on relationships automatically detected within very large volumes of data, the more legally and operationally important the ability to understand, control and explain the reasons for an alert becomes.

Third vulnerability: explainability becomes a central safeguard

European law now contains particularly precise case law concerning the explanation of automated decisions S52.

In Case C-203/22, the Court of Justice specifies that, where the relevant regime applies, the individual must be able to obtain information enabling them to understand:

- the procedure actually used;
- the principles applied;
- how their data contributed to the result S52.

The Court also specifies that:

> the complexity of the processing does not remove the obligation to provide an intelligible explanation.

A complex mathematical formula does not necessarily constitute a sufficient explanation.

Nor does an exhaustive description of all technical operations S52.

LEGAL SAFEGUARD:

> Where a decision falls within the GDPR regime governing automated decisions, the complexity of an algorithm cannot be used as a justification for making its result legally inexplicable.

A tension emerges with complex models

This case law raises an important question regarding the evolution of CFVR.

The CNIL specifically asks the ministry to work on:

> **the explainability of algorithms** S37.

At the same time, CFVR is developing:

- learning methods;
- unsupervised methods;
- analyses involving massive volumes of data;
- cross-referencing between multiple sources S37-S45.

A structural tension therefore emerges:

```
increasing complexity
   ↓
increasing detection capabilities
   ↓
but
   ↓
need to preserve
understanding
control
explainability
contestability
```

POTENTIAL LEGAL VULNERABILITY:

> An architecture whose results became sufficiently determinative to produce or condition significant decisions would have to remain capable of providing the transparency and explanation safeguards required by applicable law.

NOT ESTABLISHED:

> The sources examined do not make it possible to conclude that CFVR models are currently legally inexplicable.

Fourth vulnerability: data quality can directly influence targeting

The human intervention documented by the CNIL includes a revealing precaution.

Agents must notably verify:

> that the latest tax returns filed have been taken into account S37.

This requirement shows that an algorithmic alert may be influenced by the state of the data available at the time it is calculated.

Electronic invoicing data will considerably increase the quantity and granularity of exploitable information.

An error may arise from:

```
incorrect data
   ↓
cross-referencing
   ↓
anomaly detected
   ↓
alert
   ↓
business selected
```

The human safeguard must therefore make it possible to break this chain before an erroneous algorithmic signal produces unjustified consequences.

VULNERABILITY:

> The greater the number of sources and data used, the more decisive control over their accuracy, currency and context becomes for the quality of the algorithmic result.

The legal boundary becomes particularly important if the consequences evolve

Today, the documentation primarily establishes:

```
alert
   ↓
guidance for an agent
   ↓
human analysis
   ↓
possible tax audit
```

This architecture benefits precisely from the existence of this human stage.

But the SCHUFA case law shows that another configuration must be analyzed differently:

```
automated result
   ↓
determining result
   ↓
decision producing a significant effect
```

S51

The question therefore does not concern only CFVR as it exists today.

It also concerns any future development in which a score or classification produced by a public infrastructure became determinative in:

- automatically initiating a procedure;
- denying a right or service;
- modifying the conditions of access to a service;
- producing a financial consequence;
- imposing a restriction;
- or conditioning another decision producing a significant effect on an individual.

LEGAL BOUNDARY:

> The more determinative the algorithmic result becomes in producing a significant individual consequence, the more central the question of the application of Article 22 and the associated safeguards becomes S43-S51.

This boundary is essential for the bridge with the other infrastructures examined in the investigation

This conclusion provides an important legal element for the architectures examined in Chapter 5.

The previous chapters separately identified capabilities concerning:

- transactions;
- electronic invoicing;
- identity;
- products;
- the Digital Product Passport;
- environmental data;
- certain payment conditions.

No element examined currently demonstrates the existence of a system using all of these data to automatically produce an individual decision.

But the legal framework now makes it possible to identify what would need to be examined if such infrastructures were interconnected.

The legally sensitive chain would be:

```
economic data
   +
transaction data
   +
identity data
   +
product data
   +
environmental data
   ↓
profile / score / classification
   ↓
automated result
   ↓
determining influence
   ↓
decision producing
a legal or significant effect
```

At that stage, several safeguards would then have to be examined simultaneously:

- purpose of the processing;
- legal basis;
- minimization;
- proportionality;
- data accuracy;
- transparency;
- explainability;
- human intervention;
- ability to challenge;
- Article 22 of the GDPR where its conditions are met S43-S44-S46-S48-S51-S52.

LEGALLY DEDUCIBLE:

> The technical interconnection of several infrastructures is not sufficient to make a decision resulting from their combination legally permissible.

LEGALLY DEDUCIBLE:

> If their combination were to produce a score or classification playing a determining role in a significant individual decision, the formal existence of a human intermediary would not necessarily be sufficient to exclude the safeguards applicable to automated decisions S51.

NOT ESTABLISHED:

> No element examined currently demonstrates that an environmental score, a DPP or data originating from electronic invoicing determines the authorization or refusal of a payment or another individual right.

This boundary must be strictly maintained.

A deeper vulnerability nevertheless emerges

The infrastructures examined progressively reveal three distinct phenomena:

```
1. increase in available data
2. increase in matching possibilities
3. increase in algorithmic capabilities
```

Taken separately, each may have its own legal basis and safeguards.

But their combination increases the technical possibility of producing increasingly granular classifications.

The law does not prohibit this development as a matter of principle.

It does, however, require safeguards to evolve with the nature and influence of the processing.

STRUCTURAL VULNERABILITY:

> An architecture may remain legally presented as a decision-support system as long as human intervention remains genuine and determinative. The boundary becomes much more sensitive if the increasing precision, volume or authority given to algorithmic results progressively transforms this human intervention into essentially formal validation.

It is precisely this development that would need to be measurable over time.

Questions for testing this safeguard

The analysis now makes it possible to formulate several verifiable questions:

> **1. What is the rate at which agents reject cases proposed by CFVR following human analysis?**

> **2. Is this rate monitored model by model and alert category by alert category?**

> **3. What mechanisms make it possible to detect excessive reliance by agents on algorithmic recommendations?**

> **4. Have the studies on bias and explainability announced to the CNIL been carried out, and can their results be disclosed?**

> **5. How is any potential overrepresentation of certain categories of taxpayers or businesses in alerts measured?**

> **6. How does the administration verify that a correlation detected by a model remains linked to a real and current prevalence of fraud?**

> **7. What information can be provided to an individual seeking to understand the role played by algorithmic processing in the selection of their case?**

> **8. What safeguards prevent a future development from transforming an algorithmic recommendation into the automatic or near-automatic initiation of a procedure?**

These questions do not presume any violation.

They make it possible to test the effectiveness of the safeguards invoked.

Conclusion of 6.4

ESTABLISHED:

> CFVR uses algorithmic methods to identify anomalies and guide tax audit programming S37-S45.

ESTABLISHED:

> The development of unsupervised learning methods and the massive expansion of data lead the CNIL itself to consider that algorithmic risks and risks of bias are amplified S37.

ESTABLISHED:

> The results of previous audits are used to develop the models, which, according to the CNIL, exposes the system to a risk of bias amplification over time S37.

DOCUMENTED SAFEGUARD:

> CFVR alerts must not replace the analysis carried out by agents, and the initiation of a tax audit must currently result from a human decision S37.

DOCUMENTED SAFEGUARD:

> The ministry limits to 50% the proportion of audits initiated following signals originating from CFVR S37.

EXPLICITLY ACKNOWLEDGED LIMITATION:

> The CNIL considers that this 50% limit is not sufficient, on its own, to prevent all risks of significant bias and calls for additional work on explainability and bias S37.

PRINCIPLE ESTABLISHED BY CASE LAW:

> According to the CJEU, an automated result may itself fall within the concept of an automated decision where the subsequent decision depends in a determining manner on that result S51.

LEGAL SAFEGUARD:

> Where the regime governing automated decisions applies, the technical complexity of the system does not remove the requirements of transparency and explanation S52.

LEGAL VULNERABILITY:

> The protection provided by human intervention depends on its actual effectiveness. Essentially formal human validation of a determinative algorithmic result could require a reassessment of the legal classification of the process.

DOCUMENTARY BLIND SPOT:

> The public sources examined do not make it possible to precisely measure the rate at which CFVR alerts are rejected by agents or, consequently, the degree of practical influence that algorithmic recommendations have on decisions to initiate audits.

TO BE ESTABLISHED:

> Do the announced studies on explainability and bias make it possible to demonstrate that the massive expansion of data and the development of new methods do not lead to an unjustified concentration of audits on certain populations or categories of entities?

TO BE ESTABLISHED:

> What mechanisms make it possible to demonstrate that human intervention remains substantive as the predictive capabilities and complexity of the models increase?

LEGALLY DEDUCIBLE:

> If a future infrastructure combined economic, transaction, identity, product or environmental data in order to produce a result determinative of a significant individual decision, that chain would have to be examined in light of the safeguards applicable to automated processing, irrespective of the mere formal presence of a human at the end of the chain S51.

NOT ESTABLISHED:

> No element examined currently makes it possible to claim that CFVR automatically decides to initiate a tax audit or that environmental data, a DPP or invoicing data automatically determines access to a payment, service or right.

6.5 Necessity, proportionality and minimization

Status: ESTABLISHED LEGAL OBLIGATIONS / ESTABLISHED CHANGE IN SCALE / JUSTIFICATIONS TO BE ESTABLISHED

The previous sections established several important elements.

Data originating from electronic invoicing are intended to feed an infrastructure enabling their large-scale algorithmic processing.

They are incorporated into a processing system already fed by numerous other sources.

Cross-referencing is carried out notably to detect anomalies and identify businesses presenting certain tax risks.

The announced volume reaches several billion electronic invoices per year S37-S45.

The legal question then becomes different.

It is no longer merely:

> **"does the fight against fraud constitute a legitimate purpose?"**

That purpose is established.

The question becomes:

> **"are all the data collected, their granularity, their cross-referencing, their retention periods and the ways in which they are processed necessary and proportionate to that purpose?"**

This distinction is essential.

A legitimate purpose is not sufficient to demonstrate the necessity of each item of data

The principle of data minimization laid down in Article 5 of the GDPR requires personal data to be:

> **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed** S36-S43.

This requirement therefore concerns not only the existence of a legitimate purpose, but also the relationship between that purpose and the data actually used.

The legal chain is not:

```
objective of general interest
   ↓
all data that may potentially be useful
```

It is:

```
precisely defined objective
   ↓
necessary data
   ↓
necessary quantity
   ↓
necessary duration
   ↓
necessary access
   ↓
necessary processing
```

LEGAL SAFEGUARD:

> The potential usefulness of data is not necessarily sufficient to demonstrate its legal necessity.

The CJEU applies this requirement directly to tax administrations

Case C-175/20 is particularly important for this investigation because it specifically concerns a tax administration S53.

The Court of Justice reiterates that limitations on data protection must remain limited to what is strictly necessary.

It concludes that a controller, even when acting in the context of a task carried out in the public interest:

> **cannot collect personal data in a general and indiscriminate manner** S53.

It must also:

> **refrain from collecting data that are not strictly necessary for the purposes of the processing** S53.

The Court adds that the controller must seek to minimize the amount of data collected as much as possible.

PRINCIPLE ESTABLISHED BY CASE LAW:

> A tax administration therefore does not have, solely by virtue of its mission to combat fraud, a general right to indiscriminately collect all personal data that may be of analytical interest.

The burden of demonstrating compliance is a particularly important element

The Court adds an essential requirement.

The controller must be able to demonstrate compliance with the principles laid down in Article 5 of the GDPR S53.

Regarding minimization, it states that it is for the administration concerned to establish that it has sought to minimize the amount of data collected as much as possible.

Regarding duration, it also specifies that the period concerned cannot exceed what is strictly necessary for the objective of general interest pursued S53.

The question is therefore not merely:

> **"can it be demonstrated that these data are useful?"**

It becomes:

> **"can it be demonstrated why this precise amount of data is necessary?"**

and:

> **"can it be demonstrated why a smaller amount, lower granularity or shorter period would not be sufficient to achieve the objective pursued?"**

LEGAL SAFEGUARD:

> The principle of accountability requires the controller to be able to demonstrate compliance with data minimization.

This case law directly intersects with CFVR's change in scale

The CNIL notes that the arrival of data originating from electronic invoicing substantially increases the volume of data processed within CFVR S37.

It indicates that the volume of electronic invoices is estimated at:

> **2 to 3 billion per year** S37.

The volume is such that the ministry indicates that these data could not be processed within the existing CFVR infrastructure.

An infrastructure with enhanced computing power, the secure data platform, becomes necessary precisely to enable their processing S37.

The documented chain is therefore:

```
new category of data
   ↓
substantial increase in volume
   ↓
2 to 3 billion invoices / year
   ↓
existing infrastructure insufficient
   ↓
secure data platform with enhanced computing power
   ↓
processing
   ↓
cross-referencing of results
   ↓
tax targeting
```

ESTABLISHED:

> The integration of electronic invoicing does not constitute a marginal increase in processing.

It results in a change in scale significant enough to require an infrastructure with enhanced computing power S37.

First vulnerability: the change in scale must be justifiable data by data

The change in scale does not, in itself, constitute a violation of the principle of data minimization.

Mass collection may be necessary where a legitimate task cannot reasonably be carried out otherwise.

But C-175/20 prevents reasoning solely on the basis of the general interest pursued S53.

The data actually necessary must also be examined.

The question therefore becomes:

> **Are all categories of personal data originating from electronic invoicing that are integrated into or processed within this chain necessary for the models and analyses pursued?**

And more specifically:

> **Does each personal data field processed make a necessary contribution to a specified purpose?**

> **Could certain analyses operate with fewer fields?**

> **Could certain data be aggregated, pseudonymized or deleted before processing?**

> **Could the same effectiveness be achieved without retaining certain elements at transaction level?**

LEGAL VULNERABILITY:

> The more systematically an infrastructure absorbs data, the less reasonably the demonstration of necessity can be limited to the general assertion that these data may improve the fight against fraud.

TO BE ESTABLISHED:

> What documented demonstration justifies, category by category, the personal data originating from electronic invoicing that are actually necessary for the processing carried out within the secure data platform and CFVR?

The case law also requires examining whether more limited targeting is possible

Case C-175/20 contains particularly noteworthy reasoning here S53.

In that case, the Court specifically asks whether it would be possible to achieve the tax objective without potentially obtaining data relating to all the advertisements concerned.

It explicitly considers the possibility of:

> **targeting certain advertisements using specific criteria** S53.

The principle is important.

Where the objective can be achieved through more targeted collection, generalized collection becomes more difficult to justify.

Applied to the architecture examined, this raises a question that is no longer theoretical:

```
processing of invoicing data
on a very large scale
   VS
prior selection
of categories / transactions / situations
presenting risk criteria
```

MAJOR LEGAL QUESTION:

> Is the processing of the mass of electronic invoicing data necessary for the purposes pursued, or could certain analyses be carried out on the basis of a less intrusive prior selection?

The answer requires technical and statistical information that is not present in the public sources examined.

DOCUMENTARY BLIND SPOT:

> We have not yet identified any public demonstration comparing the planned large-scale processing with less intrusive architectures that might produce comparable results.

Second vulnerability: minimization also concerns granularity

Two processing operations may involve the same number of documents while presenting very different levels of interference.

A distinction must be made between:

```
existence of an invoice
```

and:

```
detailed content of the invoice
```

and further:

```
detailed content
   +
history
   +
counterparties
   +
cross-referencing with other databases
```

The principle of data minimization applies to the amount of data, but also to the extent of processing and their accessibility S43.

The relevant question is therefore not merely:

> **how many invoices are processed?**

It is also:

> **what level of detail originating from each of these invoices is actually necessary for each model or query?**

LEGAL VULNERABILITY:

> A justification concerning the necessity of using invoices does not automatically demonstrate the necessity of using every item of personal data they contain.

Third vulnerability: cross-referencing changes the intensity of processing

An isolated item of data and the same item cross-referenced with numerous other pieces of information do not necessarily involve the same level of interference.

CFVR specifically enables multiple sources to be cross-referenced S37-S45.

The secure data platform is intended to progressively host all the data processed within CFVR S37.

Thus:

```
data A
   +
data B
   +
data C
   +
electronic invoicing
   +
tax history
   +
other sources
   ↓
increased inference capability
```

The principle of data minimization must therefore be examined not only at the level of each database considered separately, but also in light of the processing actually carried out through their combination.

STRUCTURAL VULNERABILITY:

> Data that are individually necessary for several processing operations may, when cross-referenced, produce a much more intrusive analytical capability than that resulting from each source considered separately.

TO BE ESTABLISHED:

> How are necessity and proportionality assessed for combinations of data and not only for each source considered separately?

The French Constitutional Council also requires a proportionality assessment

This requirement does not arise solely from the GDPR and European case law.

The French Constitutional Council links the protection of personal data to the right to respect for private life guaranteed by Article 2 of the Declaration of the Rights of Man and of the Citizen S44.

It holds that:

> **the collection, recording, retention, consultation and communication of personal data must be justified by a reason of general interest and implemented in a manner that is appropriate and proportionate to that objective** S44.

The assessment therefore concerns several successive operations:

```
collection
   ↓
recording
   ↓
retention
   ↓
consultation
   ↓
communication
```

CONSTITUTIONAL SAFEGUARD:

> The existence of a reason of general interest does not exempt the system from an assessment of the appropriateness and proportionality of its practical arrangements.

Fourth vulnerability: retention must be justified separately

Data that are necessary today do not automatically remain necessary for the entire period during which their retention is technically possible.

The principle of storage limitation requires that data enabling individuals to be identified not be retained for longer than necessary in relation to the purposes pursued S43.

C-175/20 also applies the logic of strict necessity to the period covered by tax-related data collection S53.

This question becomes particularly important in an algorithmic infrastructure.

The longer the available history:

```
more historical data
   ↓
more possible comparisons
   ↓
more possible models
   ↓
greater inference capabilities
```

But:

```
analytical usefulness
   ≠
automatic legal necessity
```

LEGAL VULNERABILITY:

> A long retention period must be justifiable in relation to the purposes pursued and cannot be based solely on the potential value of having access to a richer historical dataset.

A first concrete point already exists regarding exchanges with social security bodies

The CNIL specifically applied this reasoning to exchanges between the DGFiP and social security bodies S37.

It notes that the draft submitted to it did not specify the retention period for the data transmitted.

It then reiterates that exchanges between administrations are permitted only where their arrangements remain proportionate to the objectives pursued.

It calls for retention to be limited to the period necessary S37.

The ministry committed to providing for a maximum retention period of ten years.

But the CNIL also asks for something more precise:

> that the applicable retention periods be determined **category of data by category of data** in the agreements concluded with social security bodies S37.

This clarification is particularly noteworthy.

It shows that:

```
a general maximum retention period
   ≠
individualized justification
of the necessary duration
for each category
```

ESTABLISHED:

> The CNIL itself calls for a more granular assessment of retention periods for data exchanged with social security bodies S37.

Fifth vulnerability: "up to ten years" does not mean "ten years are necessary"

This distinction must be maintained.

The fact that a legal framework permits retention for up to a certain period does not necessarily mean that all categories of data must actually be retained for that entire period.

The principles of data minimization and storage limitation require identifying the period necessary for the processing concerned S43-S53.

Thus:

```
maximum legally permissible period
   ≠
necessary period for each item of data
```

QUESTION TO BE ESTABLISHED:

> Among the data that may be retained for up to ten years, which actually require that retention period and which could be deleted or anonymized earlier?

Sixth vulnerability: progressive accumulation may shift the proportionality assessment

Section 6.2 identified a question that was deliberately left open:

> how far can successive extensions of purposes, sources and recipients accumulate before their overall effect requires a new assessment of necessity and proportionality?

This question now becomes much more concrete.

CFVR is no longer the processing system it was when it was created.

Its scope has evolved.

Its sources have evolved.

Its methods have evolved.

Its computing capabilities have evolved.

The categories of agents involved have evolved.

Inter-administration exchanges have evolved.

And several billion electronic invoices are now being added to this architecture S37-S45.

The evolution can therefore be represented as follows:

```
initial processing
   ↓
new sources
   ↓
new cross-referencing
   ↓
new algorithms
   ↓
new persons with access
   ↓
new exchanges
   ↓
new computing infrastructure
   ↓
several billion invoices / year
```

Each extension may separately have a legal basis.

But this does not fully answer another question:

> **does the resulting architecture, as a whole, remain necessary and proportionate?**

STRUCTURAL LEGAL VULNERABILITY:

> Assessing each extension in isolation may not be sufficient to account for the overall intensity of the processing resulting from their accumulation.

The principle of accountability shifts part of the reasoning here

One of the most important contributions of C-175/20 is that the responsibility for demonstrating data minimization lies with the controller S53.

This changes how the questions in this investigation can be formulated.

We do not necessarily have to demonstrate:

> **"these data are unnecessary."**

The legally relevant question may be:

> **"what evidence establishes that these data are necessary?"**

Likewise, it is not necessary to claim:

> **"this retention period is excessive."**

We can ask:

> **"what evidence establishes that this retention period is necessary for this purpose?"**

Or:

> **"what evidence establishes that the same objective could not be achieved with a smaller amount of data?"**

This is a fundamental methodological difference.

Seventh vulnerability: technical capabilities do not constitute the measure of necessity

The CNIL explains that the secure data platform is technically necessary because the volume of electronic invoicing data exceeds the capabilities of the existing CFVR environment S37.

This establishes:

> **the technical necessity of a more powerful infrastructure to process the envisaged volume of data.**

However, this does not answer a different question:

> **the legal necessity of processing the entire envisaged volume.**

The two lines of reasoning must not be confused.

```
"we need the secure data platform
to process this much data"
   ≠
"we have demonstrated that it is necessary
to process this much data"
```

DOCUMENTARY VULNERABILITY:

> The sources examined explain why enhanced computing power is necessary to process the planned volume of data, but they do not, on their own, demonstrate why this precise volume constitutes the minimum level necessary for each purpose pursued.

This distinction is particularly important.

This reasoning becomes crucial for the other infrastructures examined in the investigation

The principle of necessity does not concern CFVR alone.

It also provides a legal test for any future interconnection involving personal data.

The previous chapters identified various infrastructures relating notably to:

- transactions;
- invoicing;
- identity;
- products;
- the DPP;
- environmental information;

- certain payment infrastructures.

The separate existence of legal bases permitting certain processing operations within each of these infrastructures would not necessarily be sufficient to justify their combination.

The question would have to be asked again for the resulting processing:

```
data necessary in system A
   +
data necessary in system B
   +
data necessary in system C
   ≠ automatically
necessary combination of A + B + C
```

LEGALLY DEDUCIBLE:

> The necessity of collecting data within its original system does not automatically demonstrate the necessity of cross-referencing it with data from another infrastructure.

This is an important legal boundary for the bridge constructed in this investigation.

Application to the environmental / identity / payment bridge

No element examined currently demonstrates the existence of processing combining all of these infrastructures in order to produce an individual decision.

But if a future development were to lead, for example, to:

```
identity
   +
transaction
   +
product
   +
DPP
   +
environmental information
   +
payment
   ↓
analysis / classification
   ↓
individual consequence
```

the mere existence of a legal basis specific to each component would not necessarily be sufficient to establish the necessity and proportionality of the resulting processing.

It would notably be necessary to examine:

- the precise purpose of the cross-referencing;
- the data strictly necessary;
- the necessary granularity;
- the necessary duration;
- the persons who may access it;
- less intrusive alternatives;
- the consequences for individuals;
- safeguards against secondary uses S43-S44-S53.

LEGALLY DEDUCIBLE:

> The more several infrastructures are interconnected, the more the justification must concern the processing resulting from their combination and not solely the individual legality of each of their components.

NOT ESTABLISHED:

> Nothing in the sources examined currently demonstrates that such a comprehensive interconnection is implemented or legally provided for.

A genuine line of legal assessment emerges

After Sections 6.1 to 6.5, the legal reasoning can now be summarized as follows:

```
legal basis
   ↓
legitimate purpose
   ↓
   BUT
   ↓
necessary data?
   ↓
necessary quantity?
   ↓
necessary granularity?
   ↓
necessary cross-referencing?
   ↓
necessary duration?
   ↓
necessary persons with access?
   ↓
less intrusive alternative?
   ↓
overall proportionality?
```

A positive answer to the first two stages therefore does not automatically answer the subsequent ones.

Questions for concretely testing proportionality

The analysis now makes it possible to ask much more precise questions:

> **1. Which exact categories of personal data originating from invoices are processed within the secure data platform for each model or query?**

> **2. What analysis demonstrates the necessity of each of these categories?**

> **3. What tests have been carried out using a smaller or less granular dataset?**

> **4. Has the administration compared the effectiveness of large-scale processing with that of collection or prior selection based on risk criteria?**

> **5. Which data are deleted before processing because they are not necessary?**

> **6. Which data are aggregated, pseudonymized or anonymized before being cross-referenced?**

> **7. For each category of data, what retention period is actually applied and why is that period necessary?**

> **8. What analysis addresses the cumulative effect of the different sources used within CFVR?**

> **9. Does the DPIA examine less intrusive alternative architectures?**

> **10. What evidence makes it possible to establish that the change in scale introduced by several billion invoices remains proportionate to the benefits obtained for the purposes pursued?**

These questions do not ask the administration to demonstrate that the processing presents zero risk.

They ask for evidence of its necessity and proportionality.

Conclusion of 6.5

ESTABLISHED:

> The principle of data minimization requires personal data to be adequate, relevant and limited to what is necessary for the purposes pursued S36-S43.

PRINCIPLE ESTABLISHED BY CASE LAW:

> A tax administration cannot collect personal data in a general and indiscriminate manner and must refrain from collecting data that are not strictly necessary S53.

PRINCIPLE ESTABLISHED BY CASE LAW:

> The controller must be able to demonstrate that it has sought to minimize as much as possible the amount of data collected and the period concerned S53.

CONSTITUTIONAL SAFEGUARD:

> The collection, recording, retention, consultation and communication of personal data must be justified by a reason of general interest and implemented in a manner that is appropriate and proportionate to that objective S44.

ESTABLISHED:

> The integration of electronic invoicing results in a substantial increase in the volume of data processed within CFVR, estimated at several billion invoices per year, requiring the use of an infrastructure with enhanced computing power S37.

ESTABLISHED:

> Regarding certain inter-administration exchanges, the CNIL already requires retention periods to be specified category of data by category of data S37.

LEGAL VULNERABILITY:

> The legitimacy of the fight against fraud does not remove the requirement to demonstrate the necessity of the amount, granularity, duration and cross-referencing of the data actually used.

STRUCTURAL VULNERABILITY:

> The individual necessity of data originating from several systems does not automatically demonstrate the necessity of combining them.

DOCUMENTARY VULNERABILITY:

> The public sources examined explain why an infrastructure with enhanced computing power is necessary to process the envisaged volume, but they are not sufficient to demonstrate why processing this precise volume itself constitutes the minimum means necessary for each purpose pursued.

DOCUMENTARY BLIND SPOT:

> We have not identified in the public sources examined a comparison making it possible to determine whether certain CFVR purposes could be achieved with a smaller amount of data, lower granularity or more restrictive prior targeting.

TO BE ESTABLISHED:

> Can the administration demonstrate, in accordance with the principle of accountability, the necessity of each category of personal data processed and the absence of a reasonably less intrusive solution capable of achieving the same purposes?

TO BE ESTABLISHED:

> Is the cumulative effect of successive extensions of CFVR subject to an overall and regularly reassessed evaluation of necessity and proportionality?

LEGALLY DEDUCIBLE:

> Any future interconnection of personal data originating from invoicing, identity, products, the DPP, environmental data or payment infrastructures would have to justify the necessity of the cross-referencing itself and not merely the separate legality of each source.

NOT ESTABLISHED:

> The sources examined do not make it possible to conclude that the current integration of electronic invoicing data into CFVR is disproportionate or contrary to the GDPR.

6.6 Data subject rights and CNIL oversight

Status: ESTABLISHED RIGHTS / EXPRESSLY PROVIDED RESTRICTIONS / INDEPENDENT OVERSIGHT / EFFECTIVENESS TO BE EXAMINED

The previous sections established that a significant amount of personal data may be collected, cross-referenced and analyzed within CFVR.

They also established that:

- electronic invoicing data are intended to be incorporated into this architecture;
- certain results are produced by algorithmic processing;
- these results may contribute to the selection of cases;
- exchanges exist with other administrations;
- data and results may circulate between several environments and categories of recipients S37-S45.

A question then becomes central:

> **What means does an individual have to know which data concerning them are being used, verify their accuracy, obtain their correction and challenge processing that would infringe their rights?**

This question concerns the effectiveness of the safeguards.

A right laid down in a legal text and a right that can actually be exercised are not necessarily the same thing.

The GDPR grants important rights to individuals

The GDPR notably provides for:

- a right to information;
- a right of access;
- a right to rectification;
- under certain conditions, a right to erasure;
- a right to restriction of processing;
- under certain conditions, a right to object;
- safeguards relating to certain automated decisions;
- a right to lodge a complaint with a supervisory authority;
- a right to an effective judicial remedy S43.

The right of access provided for in Article 15 notably makes it possible to know:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients;
- the retention period or the criteria used to determine it;

- the existence of certain other rights;
- the source of the data where they were not collected from the individual;
- in the situations provided for by the GDPR, certain information relating to the logic of automated decision-making S43.

LEGAL SAFEGUARD:

> An individual is therefore not legally deprived of means of control over the use of their data by an administration.

CFVR explicitly provides for the exercise of some of these rights

Article 6 of the Order establishing CFVR expressly provides that the rights of access and rectification under Articles 15 and 16 of the GDPR may be exercised S45.

Depending on the source of the data, these rights are exercised:

- with the SJCF-1D office;
- or with the public finance center responsible for the individual concerned S45.

The right to restriction provided for in Article 18 of the GDPR may also be exercised with the SJCF-1D office S45.

ESTABLISHED:

> CFVR is not a processing system placed outside the rights of access, rectification and restriction.

But the Order immediately provides for several restrictions.

First major restriction: the right to object does not apply to CFVR

Article 6 of the CFVR Order explicitly provides that:

> **the right to object provided for in Article 21 of the GDPR does not apply to the processing** S45.

Since the July 2026 amendment, this exclusion has been expressly linked to the objectives referred to in points (e) and (h) of Article 23(1) of the GDPR S45.

These provisions notably concern:

- important objectives of general public interest of the Union or a Member State, notably in tax matters;
- monitoring, inspection or regulatory functions connected notably to those objectives S43.

The practical consequence is significant.

An individual cannot simply decide:

```
"I object to my data
being used within CFVR"
   ↓
processing stops
```

The right to object is expressly excluded for this processing.

LEGAL LATITUDE:

> European law permits, subject to conditions, certain rights to be restricted in order to protect notably important tax interests and the associated monitoring functions.

ESTABLISHED RESTRICTION:

> Within CFVR, the right to object provided for in Article 21 of the GDPR does not apply S45.

This restriction therefore does not, in itself, constitute a violation of the GDPR.

It nevertheless constitutes a concrete limitation on the individual's control over the use of their data.

Second restriction: access and rectification may themselves be limited

The CFVR Order also provides that the rights of access and rectification may be subject to restrictions under the conditions laid down in Article 52 of the French Data Protection Act S45-S54.

This provision specifically concerns certain processing operations used by administrations to audit or collect taxes S54.

The rationale is understandable:

```
right of access
   ↓
but
   ↓
do not disclose information
that could compromise
the tax audit
```

An individual subject to a risk analysis may therefore not necessarily be able to immediately obtain all the information that could reveal audit methods or compromise their purpose.

LEGAL LATITUDE:

> The law expressly provides for the possibility of restricting certain rights in order to preserve the effectiveness of certain tax functions.

But this possibility creates an obvious tension:

```
to challenge effectively
   ↓
one must understand
what is being done
   but
to preserve the audit
   ↓
certain information
may be restricted
```

The CNIL then becomes an essential intermediary

When the restrictions provided for CFVR apply, the individual exercises their rights through the CNIL under the conditions laid down in Article 118 of the French Data Protection Act S45-S54.

The CNIL then carries out the necessary checks.

It may arrange for the necessary changes to be made.

It then informs the individual that the checks have been carried out and indicates the existence of a judicial remedy S54.

Where certain information can be disclosed without compromising the protected purposes, it may be communicated under the conditions provided for by law S54.

LEGAL SAFEGUARD:

> Restricting direct access does not therefore necessarily result in the absence of oversight.

An independent institutional third party can verify the processing.

But a fundamental difference emerges between verification and personal understanding

This architecture simultaneously protects two interests:

```
effectiveness of tax audits
   ↕
individual rights
```

But it may produce a particular situation:

```
the individual suspects
incorrect data or analysis
   ↓
they request access / rectification
   ↓
certain information is restricted
   ↓
the CNIL carries out checks
   ↓
the individual may be informed
that the checks have been carried out
   ↓
without necessarily knowing
all of the protected information
```

STRUCTURAL LEGAL VULNERABILITY:

> The more the information necessary to understand the origin of an alert is protected against disclosure, the more the effectiveness of an individual challenge depends on the oversight exercised by the CNIL and, where applicable, by the courts.

This does not mean that the remedy becomes ineffective.

It means that individual oversight may become partly **mediated by an independent authority** rather than exercised directly by the individual.

Rectification becomes particularly important in an interconnected architecture

The right to rectification makes it possible to obtain the correction of inaccurate personal data S43.

But the architecture examined is no longer necessarily limited to data stored in a single database.

Data may follow a chain:

```
source data
   ↓
transmission
   ↓
cross-referencing
   ↓
analysis
   ↓
indicator
   ↓
algorithmic result
   ↓
case proposed
```

The GDPR also provides that where rectification, erasure or restriction takes place, the controller must in principle communicate it to the recipients to whom the data have been disclosed, unless this proves impossible or involves disproportionate effort S43.

This safeguard becomes particularly important in a multi-source architecture.

First difficult question: does correcting the data correct its consequences?

Consider a hypothetical situation:

```
incorrect data A
   ↓
cross-referencing with B and C
   ↓
indicator D
   ↓
score / classification E
   ↓
alert F
```

The correction of A is legally regulated.

But several additional questions arise:

> **Is D automatically recalculated?**

> **Is E deleted or reassessed?**

> **Is F withdrawn if it was based on the incorrect information?**

> **Are the recipients of F informed?**

> **Do derived data remain in other environments?**

The GDPR contains mechanisms for rectification, restriction and notification to recipients S43.

But their application to complex chains of derived data must be examined in practice.

DOCUMENTARY BLIND SPOT:

> The public sources examined do not make it possible to determine precisely the technical mechanism by which a rectification made to source data is propagated to results, indicators, classifications or alerts already produced from those data within CFVR and the secure data platform.

This question is not theoretical for CFVR

The CNIL requires agents to verify notably that the latest tax returns filed have been taken into account before deciding whether to initiate an audit S37.

This requirement constitutes an important safeguard.

But it also confirms that an algorithmic result may be affected by the state of the data used at the time it is produced.

The following chain is therefore legally relevant:

```
outdated / inaccurate / incomplete data
   ↓
algorithmic analysis
   ↓
apparent anomaly
   ↓
alert
   ↓
human verification
```

Human verification constitutes an essential barrier here.

DOCUMENTED SAFEGUARD:

> The agent must not treat the algorithmic signal as an autonomous truth and must analyze the case on the basis of relevant and up-to-date information S37.

The right to restriction provides an additional safeguard

Article 18 of the GDPR provides notably that an individual may request restriction of processing where they contest the accuracy of data, for the period necessary for the controller to verify their accuracy S43.

CFVR expressly provides for the exercise of this right with the SJCF-1D office S45.

Restriction may therefore constitute a particularly important safeguard where information capable of influencing processing is contested.

LEGAL SAFEGUARD:

> Contesting the accuracy of data may, under the conditions provided for by the GDPR, lead to the temporary restriction of its processing while its accuracy is being verified S43-S45.

TO BE ESTABLISHED:

> How is this restriction technically propagated when the contested data have already contributed to producing results across several environments?

The issue becomes more complex with derived data

An algorithmic infrastructure does not necessarily merely replicate source data.

It may produce:

- indicators;

- categories;
- relationships;
- anomalies;
- scores;
- query results;
- audit proposals.

CFVR notably feeds GALAXIE with certain links between individuals and entities and PILOT CF with cases proposed for audit S45.

The question of rectification must therefore potentially be considered at several levels:

```
level 1
source data

level 2
cross-referenced data

level 3
inference / indicator

level 4
algorithmic result

level 5
operational consequence
```

STRUCTURAL VULNERABILITY:

> The more an architecture produces derived data from multiple sources, the more the effective correction of inaccurate information requires control not only over the initial data, but also over the results derived from it.

Second difficult question: can an individual know why their case was selected?

The right of access makes it possible to obtain a wide range of information relating to the processing S43.

But CFVR is specifically a system for detecting and programming tax audits.

Overly detailed disclosure of detection rules could compromise some of its purposes.

Hence the possibility of restricting certain rights S45-S54.

The individual may therefore face a structural difficulty:

```
to challenge an alert
   ↓
understand why
the system produced it
   but
explaining precisely
the detection method
   ↓
may compromise
the effectiveness of the audit
```

LEGAL VULNERABILITY:

> The effectiveness of the right to challenge depends on the balance between the level of information accessible to the individual and the level of secrecy necessary to protect audit methods.

This tension directly relates to the explainability examined in 6.4

The case law examined in 6.4 shows that, where the regime governing automated decisions applies, the complexity of a system does not exempt the controller from providing the explanations legally required S52.

According to the current sources, CFVR does not constitute a system that automatically decides to initiate an audit.

But the question of explainability remains important because the CNIL itself asks the ministry to carry out work on explainability and bias S37.

This produces a boundary:

```
necessary secrecy
of audit methods
   ↕
necessary understanding
to exercise rights
```

TO BE ESTABLISHED:

> What level of explanation can be provided to an individual regarding the role of a CFVR result in the selection of their case without compromising audit methods?

Informing individuals nevertheless remains mandatory

Regarding the new exchanges between the DGFiP and social security bodies, the CNIL expressly reiterates that each of the administrations concerned must inform individuals in accordance with Articles 12 to 14 of the GDPR S37.

The ministry indicated that the agreements governing these exchanges will reiterate this obligation S37.

This is an important point.

The existence of legally authorized exchanges therefore does not automatically remove the obligation to provide information.

DOCUMENTED SAFEGUARD:

> The CNIL requires the individuals concerned to be informed of data exchanges between the DGFiP and social security bodies under the conditions provided for by the GDPR S37.

But general information does not mean individual knowledge of each use

A distinction must be made between:

```
being informed
of the existence of processing
   ≠
knowing that specific data
were used in a specific analysis
   ≠
knowing the result
of that analysis
   ≠
knowing that this result
contributed to a decision
```

These four levels of information do not have the same purpose or necessarily the same legal regime.

DOCUMENTARY VULNERABILITY:

> General information about the existence and purposes of CFVR does not, on its own, make it possible to determine the extent to which an individual can concretely trace the use of their data in a particular analysis.

The CNIL has significant supervisory powers

The CNIL is not limited to issuing opinions when processing systems are created or modified.

The GDPR notably grants it powers to:

- require the necessary information;
- conduct investigations and audits;
- access the personal data necessary for its tasks;
- access processing premises and equipment;
- order certain measures to bring processing into compliance;
- restrict or prohibit certain processing operations under the conditions provided for by law S43.

An individual may also lodge a complaint with a supervisory authority where they consider that processing concerning them infringes the GDPR S43.

INSTITUTIONAL SAFEGUARD:

> Oversight of the lawfulness of processing therefore does not depend solely on the administration that processes the data.

The CNIL's prior opinion does not, however, constitute definitive validation of the system

CFVR has existed since 2014.

Since then, its scope has undergone numerous changes S37-S45.

It has notably been extended:

- to professionals;
- to individuals connected to businesses;
- to private individuals;
- to new sources;
- to new algorithmic methods;
- to data originating from platforms;
- to new administrative exchanges;
- to a new computing infrastructure;
- and now to data originating from electronic invoicing S37-S45.

The CNIL has issued several successive opinions on these developments S37.

But an opinion issued at a given point in time concerns the system presented to it at that time.

SAFEGUARD:

> Significant modifications to the system are subject to a legal framework, and some have resulted in new opinions from the CNIL.

STRUCTURAL VULNERABILITY:

> The compliance of an evolving architecture cannot be considered definitively established solely because an earlier version or a particular modification was the subject of a CNIL opinion.

Compliance with the GDPR is a continuing obligation.

Ex post oversight therefore becomes essential

The CNIL may investigate an organization:

- following a complaint;
- following an alert;
- or on its own initiative S43.

It may carry out on-site inspections, documentary inspections, hearings or online investigations.

In the event of non-compliance, various corrective measures may be implemented.

This distinction is fundamental:

```
opinion on a proposed system
   ≠
oversight of actual operation
   ≠
finding of permanent compliance
```

INSTITUTIONAL SAFEGUARD:

> The existence of a favorable opinion or an opinion containing observations does not deprive the CNIL of its subsequent supervisory powers.

A particular vulnerability emerges from the continuous evolution of systems

Sections 6.3 to 6.5 showed that several characteristics may evolve simultaneously:

```
more data
   +
more sources
   +
more cross-referencing
   +
new algorithms
   +
new recipients
   +
new infrastructure
```

Each of these developments may alter the level of risk to rights and freedoms.

A safeguard designed for a given architecture may therefore become insufficient if the architecture changes substantially.

LEGAL VULNERABILITY:

> In an evolving processing system, the effectiveness of safeguards depends on their reassessment when the nature, scale or risks of the processing change.

This question directly relates to the obligation to review the data protection impact assessment when changes in risk justify it S48.

Judicial remedy constitutes the final safeguard

The GDPR recognizes:

- the right to lodge a complaint with a supervisory authority;

- the right to an effective judicial remedy against certain decisions of that authority;
- the right to an effective judicial remedy against a controller or processor where the individual considers that their rights have been infringed S43.

The specific procedure provided for by Article 118 of the French Data Protection Act also reiterates the existence of a judicial remedy S54.

LEGAL SAFEGUARD:

> Even where an individual cannot directly obtain certain protected information, the processing does not escape all external oversight.

But an effective remedy requires being able to identify the problem sufficiently

A difficulty nevertheless remains.

To effectively challenge processing, an individual must generally be able to identify at least the existence of a problem.

In a complex architecture:

```
collection
   ↓
cross-referencing
   ↓
inference
   ↓
alert
   ↓
transmission
   ↓
consequence
```

an error may arise far from the initial data.

The individual may know the consequence without necessarily immediately knowing:

- the data that caused it;
- the source of those data;
- the cross-referencing performed;
- the inference produced;
- the system that generated the signal;
- the recipients who received it.

STRUCTURAL VULNERABILITY:

> The more stages, controllers and derived data a processing chain involves, the more the effective exercise of rights depends on the internal traceability of the processing and the ability of supervisory authorities to reconstruct that chain.

This question extends beyond CFVR and relates to the other infrastructures examined in the investigation

The previous chapters separately identified several infrastructures capable of processing information concerning:

- identity;
- transactions;
- invoicing;
- products;
- the DPP;
- environmental characteristics;
- payments.

No source examined currently demonstrates the existence of a single system using all of this information in order to make an individual decision.

But if several of these infrastructures were one day interconnected, the question of rights would become more complex.

```
system A
identity
       ↓
system B
transaction
       ↓
system C
product / DPP
       ↓
system D
environmental information
       ↓
system E
payment
```

The question would no longer be solely:

> **"do I have a right of access within each of these systems?"**

It would become:

> **"can I reconstruct the chain that led to the consequence affecting me?"**

The right of access to each component does not automatically guarantee understanding of the resulting system

This distinction is essential.

Suppose that each infrastructure separately provides:

```
A → access possible
B → access possible
C → access possible
D → access possible
E → access possible
```

It does not automatically follow that:

```
A + B + C + D + E
   ↓
possible understanding
of the resulting decision
```

STRUCTURAL LEGAL VULNERABILITY:

> In an interconnected architecture, the effectiveness of rights must be assessed not only processing operation by processing operation, but also in light of the individual's ability to understand and challenge the processing chain that produces a consequence affecting them.

This conclusion constitutes a new legal bridge with the previous chapters.

The connection with fundamental rights must nevertheless remain rigorous

The right to the protection of personal data is not merely a technical requirement.

It contributes to the protection of individuals' rights and freedoms.

But not every collection of data or administrative processing operation automatically constitutes an infringement of a fundamental right.

The legally relevant question is:

```
interference / processing
   ↓
legal basis
   ↓
legitimate purpose
   ↓
necessity
   ↓
proportionality
   ↓
safeguards
   ↓
effective rights
   ↓
independent oversight
   ↓
effective remedy
```

A legally problematic interference may arise when this balance is no longer respected.

The real point of vulnerability is therefore effectiveness

After the previous sections, a common thread emerges.

Protection does not rely on the technical impossibility of using the data.

It relies on a succession of legal and organizational safeguards:

```
purpose limitation
   ↓
minimization
   ↓
proportionality
   ↓
security
   ↓
human intervention
   ↓
information
   ↓
access
   ↓
rectification
   ↓
restriction
   ↓
CNIL oversight
   ↓
judicial remedy
```

The more infrastructures become capable of collecting, cross-referencing and analyzing data, the more important the effectiveness of each of these safeguards becomes.

STRUCTURAL VULNERABILITY:

> The protection of rights and freedoms therefore does not rely solely on the formal existence of rights, but on the practical ability to exercise them and on the existence of authorities capable of overseeing processing where individual access must be restricted.

Questions for testing this effectiveness

The investigation can now ask much more precise questions:

> **1. Can an individual obtain a list of the data concerning them that are actually used within CFVR and their source?**

> **2. Can they know the recipients to whom results concerning them have been transmitted?**

> **3. When data are rectified, what mechanisms ensure the correction or recalculation of results derived from those data?**

> **4. Is a restriction requested under Article 18 propagated to the environments and results in which the data have already been used?**

> **5. Is it possible to know the role played by CFVR in the selection of a case without revealing methods whose confidentiality is necessary for tax audits?**

> **6. What information is actually communicated to an individual when their right of access is exercised through the CNIL?**

> **7. What mechanisms enable the CNIL to reconstruct the complete chain when data have circulated between several processing systems or administrations?**

> **8. Are individuals informed with sufficient precision about the new exchanges between the DGFiP and social security bodies?**

> **9. How are rights exercised when several controllers intervene successively within the same chain?**

> **10. Do developments in CFVR result in regular reassessment of the effectiveness of rights and the restrictions imposed on them?**

These questions do not presume any violation.

They make it possible to test whether the safeguards are genuinely operational.

Conclusion of 6.6

ESTABLISHED:

> CFVR provides for the exercise of the rights of access, rectification and restriction S45.

ESTABLISHED RESTRICTION:

> The right to object provided for in Article 21 of the GDPR does not apply to CFVR S45.

ESTABLISHED RESTRICTION:

> The rights of access and rectification may be subject to restrictions under the conditions provided for by the French Data Protection Act S45-S54.

LEGAL SAFEGUARD:

> Where a restriction applies, a procedure for exercising rights through the CNIL is provided for, and a judicial remedy remains available S54.

LEGAL SAFEGUARD:

> The GDPR provides mechanisms notably enabling the rectification of inaccurate data, the restriction of certain processing operations and the notification of certain rectifications or restrictions to recipients S43.

DOCUMENTED SAFEGUARD:

> The CNIL reiterates that the DGFiP and social security bodies must inform the individuals concerned of the data exchanges planned between them S37.

INSTITUTIONAL SAFEGUARD:

> The CNIL has investigative and supervisory powers independent of its prior opinions, and an individual may lodge a complaint where they consider that the processing of their data infringes the GDPR S43.

LEGAL VULNERABILITY:

> Individual protection becomes more dependent on oversight by the CNIL and the courts where the information necessary for a direct understanding of the processing may lawfully be restricted.

STRUCTURAL VULNERABILITY:

> In a multi-source architecture, the effective rectification of data requires control over the results, inferences and transmissions already produced from those data.

DOCUMENTARY BLIND SPOT:

> The public sources examined do not make it possible to determine precisely how a rectification or restriction is propagated to algorithmic results and derived data already produced within CFVR, the secure data platform or the applications fed by their results.

DOCUMENTARY BLIND SPOT:

> The public sources examined do not make it possible to precisely measure the level of information actually obtained by an individual where certain information relating to CFVR is subject to the restrictions provided for by tax law.

TO BE ESTABLISHED:

> Can an individual sufficiently reconstruct the chain leading from source data to an alert or an audit proposal in order to effectively exercise their rights where several processing systems contributed to the result?

TO BE ESTABLISHED:

> Do traceability mechanisms enable the CNIL to reconstruct this complete chain where the individual themselves cannot directly access certain information?

LEGALLY DEDUCIBLE:

> If several infrastructures relating to identity, transactions, invoicing, products, environmental data or payments were one day interconnected to produce an individual consequence, the existence of separate rights within each infrastructure would not necessarily be sufficient to guarantee an effective remedy against the result produced by their combination.

NOT ESTABLISHED:

> The sources examined do not make it possible to conclude that the restrictions currently provided for within CFVR deprive individuals of an effective remedy or are contrary to the GDPR.

6.7 Safeguards specific to the infrastructures examined

Status: ESTABLISHED SPECIFIC SAFEGUARDS / DOCUMENTED INTERFACES / IDENTIFIED LEGAL BOUNDARIES

The previous sections examined the general safeguards applicable to data processing:

- purpose;
- legal basis;
- minimization;
- proportionality;
- security;
- profiling;
- automated decisions;
- data subject rights;
- oversight by independent authorities.

But the infrastructures examined in the previous chapters also have safeguards specific to them.

This section therefore examines separately:

```
electronic invoicing
   +
digital identity
   +
Digital Product Passport
   +
environmental data
   +
payment / digital euro
```

The objective is then to determine what happens to these safeguards when several infrastructures may interact.

First finding: the infrastructures are not legally designed as a single database

The previous chapters identified several technical possibilities for interconnection.

But the legal texts examined instead organize several forms of separation.

These notably include:

```
tax data
→ specified tax purposes

digital identity
→ user control
→ selective disclosure
→ segregation

DPP
→ product information
→ specified access rights
→ protection of customer data

payment
→ specific purposes
→ data protection
→ specific safeguards
```

STRUCTURAL SAFEGUARD:

> None of the texts examined establishes a general right allowing all data originating from these infrastructures to be freely merged.

Technical interoperability therefore does not constitute a general authorization for legal interconnection.

European digital identity includes particularly strong safeguards

The eIDAS 2 Regulation provides that the European Digital Identity Wallet operates under the control of the user S55.

The user must notably be able to:

- select the data they wish to present;
- combine different attributes;
- use selective disclosure;
- view the relying parties with which they have interacted;
- know, where applicable, the data exchanged;
- request the deletion of certain data;
- report a suspicious request to the data protection authority S55.

The wallet may also generate and locally store pseudonyms.

The Regulation even provides for technologies enabling a user to demonstrate that a condition is satisfied without revealing the underlying data.

Example:

```
full attribute
"date of birth: ..."
   ↓
minimal proof
"over 18: YES"
```

rather than:

```
transmission of
full identity
   +
date of birth
   +
other unnecessary attributes
```

LEGAL AND TECHNICAL SAFEGUARD:

> The European digital identity architecture explicitly incorporates mechanisms designed to reduce the amount of information disclosed when accessing a service S55.

The wallet provider must not become a general observer of its user

A particularly important safeguard appears in the Regulation.

The wallet provider must not collect information about its use that is not necessary for the provision of the service S55.

It must ensure a form of "unobservability" preventing it from obtaining a general overview of the transactions carried out by the user.

It is also prohibited from combining identification data or other personal data linked to the wallet with data originating from other services where such combination is not necessary for the wallet service, unless expressly requested by the user S55.

Attribute attestation services are also subject to separation requirements.

MAJOR SAFEGUARD:

> The European Digital Identity Wallet is not legally designed to allow its provider to freely reconstruct all of its user's digital activities.

This safeguard directly addresses one of the risks identified in the previous chapters.

Refusing to use the wallet must not become a general ground for exclusion

The Regulation also provides that access to public and private services, the labor market and the freedom to conduct a business must not be restricted or made disadvantageous solely because an individual does not use

the European Digital Identity Wallet S55.

Alternative means must remain available.

The consequence is important.

```
use of the wallet
   ↓
possible
   but
refusal to use the wallet
   ↓
must not, by itself,
result in exclusion
```

SAFEGUARD OF FREEDOM OF CHOICE:

> The current framework explicitly seeks to prevent the European Digital Identity Wallet from becoming a general and mandatory condition for access to services.

This safeguard will be particularly important to monitor during the practical deployment of the system.

But the wallet is also designed to combine attributes

The same infrastructure has another characteristic.

The wallet must enable its user to:

> request, obtain, select, combine, store, delete, share and present person identification data and electronic attestations of attributes S55.

It is therefore designed to be able to present several attributes originating from distinct sources to a relying party.

```
identity
   +
attribute A
   +
attribute B
   +
attestation C
   ↓
presentation to a service
```

This capability is not, in itself, a vulnerability.

It is precisely one of the functions of the wallet.

But it creates an important boundary.

LEGAL BOUNDARY:

> Protection does not rely on the technical impossibility of combining attributes. It relies on user control, limitation of the data requested, the purpose of the service and the rules applicable to the relying party.

Relying parties must declare the data they request

A party wishing to use the European Digital Identity Wallet must register and notably declare the intended use as well as the data it intends to request S55.

It must then not request from the user any data other than those declared.

It must also identify itself to the user.

LEGAL SAFEGUARD:

> A relying party therefore does not have indiscriminate access to the attributes contained in the wallet.

The architecture operates according to a logic of specified access:

```
service
   ↓
declared purpose
   ↓
declared attributes
   ↓
request
   ↓
selective presentation
```

and not:

```
service
   ↓
access to the entire wallet
```

The DPP also contains a fundamental separation

The Digital Product Passport is designed as an infrastructure for product-related data S56.

It may notably contain information relating to:

- product characteristics;
- its compliance;
- its life cycle;
- its durability;

- certain environmental characteristics;
- its traceability.

The DPP must be associated with a unique product identifier and operate within an open and interoperable data environment S56.

Depending on the applicable requirements, it may be established at the level of:

```
model
   or
batch
   or
item
```

The latter possibility significantly increases the potential granularity of product traceability.

But the Regulation immediately introduces an important safeguard.

The DPP is not legally an environmental record of the consumer

The ESPR explicitly provides that:

> personal data relating to customers must not be stored in the Digital Product Passport without their explicit consent S56.

This rule breaks an association that might otherwise appear obvious:

```
identifiable product
   ↓
identifiable buyer
```

The first element does not legally produce the second.

A DPP may precisely identify a product or item without identifying its owner or user.

MAJOR LEGAL SAFEGUARD:

> The current DPP framework explicitly separates product identification from the personal identification of the customer.

NOT ESTABLISHED:

> In the texts examined, the European DPP does not constitute an "individual environmental passport" recording a citizen's purchases or personal environmental footprint.

This distinction must be strictly maintained.

But the unique identifier and interoperability make another operation technically possible

The previous safeguard does not mean that a product can never be linked to an individual in another system.

A commercial transaction may already contain:

```
buyer
   +
seller
   +
product
   +
date
   +
amount
```

The DPP may, for its part, contain:

```
product identifier
   +
product characteristics
   +
environmental data
```

An external association could therefore theoretically produce:

```
transaction
   ↓
identified product
   ↓
DPP
   ↓
environmental characteristics
```

This technical possibility has already been identified in the previous chapters.

But legally:

LEGAL BOUNDARY:

> The protection of the DPP against the storage of customers' personal data does not constitute a general prohibition on any external cross-referencing between a product and a transaction.

Such cross-referencing would, however, constitute separate processing that would need its own purpose, its own legal basis and would have to comply with the requirements of necessity, proportionality and minimization where it involves personal data S43-S44-S53-S56.

A first asymmetry therefore emerges

The DPP protects its own content:

```
DPP
   ↓
no customer personal data
without explicit consent
```

But this safeguard concerns:

> **what is stored in the DPP.**

It does not necessarily mean:

> **that no other system can use the product identifier to perform cross-referencing authorized under another legal basis.**

STRUCTURAL VULNERABILITY:

> A safeguard preventing the centralization of personal data within one infrastructure does not necessarily constitute a prohibition on reconstructing the relationship between several data points through external processing.

This is an important distinction for the entire investigation.

The digital euro also includes a particularly strong safeguard

The proposed framework for the digital euro contains an explicit prohibition:

> **the digital euro must not be programmable money** S57.

A unit of digital euro must therefore not contain intrinsic logic imposing:

```
usable only
for product X
   or
prohibited for product Y
   or
usable only
before a certain date
   or
usable only
with a certain beneficiary
```

The ECB also reiterates that such limitations would be incompatible with the chosen design of the digital euro S57.

MAJOR MONETARY SAFEGUARD:

> The proposed framework prohibits the digital euro from intrinsically becoming money whose use would be restricted according to goods, services, dates or beneficiaries.

This safeguard directly addresses one of the strongest concerns that may arise around a central bank digital currency.

But "non-programmable money" does not mean "payments cannot be conditional"

This is where a much subtler boundary emerges.

The proposal explicitly distinguishes:

```
**PROGRAMMABLE MONEY**

logic embedded in the money
that limits its fungibility
   ↓
PROHIBITED
```

from:

```
**CONDITIONAL PAYMENT**

software
   +
predetermined condition
   +
payer / payee agreement
   +
automatic triggering
   ↓
PROVIDED FOR
```

S57

A conditional transaction is defined as a transaction automatically triggered when predetermined conditions agreed by the payer and the payee are met.

The proposal even allows the ECB to provide the standards and functionalities necessary for such payments, including the reservation of funds S57.

EXPLICIT LEGAL LATITUDE:

> The proposed framework prohibits the intrinsic programming of the money but allows the programming of certain conditions governing the execution of a payment.

This distinction is fundamental.

The protection therefore concerns the money, not the existence of any conditional logic surrounding the payment

The boundary can be represented as follows:

```
"this euro can only purchase
certain categories of products"
   ↓
programmable money
   ↓
PROHIBITED
```

but:

```
"execute this payment
if agreed condition X
is satisfied"
   ↓
conditional payment
   ↓
PROVIDED FOR
```

LEGAL FRICTION POINT:

> The prohibition of programmable money therefore does not constitute a general prohibition on any infrastructure capable of automatically conditioning the execution of a payment.

This is probably one of the most important distinctions identified in this investigation.

This still does not mean that an environmental condition is provided for

The documentary boundary must immediately be maintained.

Official examples of conditional payments notably concern:

- payment upon delivery;
- pay-per-use;
- payments linked to certain milestones;
- certain automated machine-to-machine payments S57.

No source examined demonstrates that a digital euro payment is intended to be conditional on:

- an individual environmental score;
- a personal carbon footprint;
- a DPP;
- a purchase history;
- or an environmental classification of an individual.

NOT ESTABLISHED:

> No official mechanism examined currently links environmental data or a DPP to the authorization or refusal of a digital euro payment.

But the condition may originate from information external to the payment

A conditional payment necessarily requires a system to be able to determine whether:

```
condition X
   =
satisfied
   or
not satisfied
```

The work examined in the previous chapters has already experimentally established the possibility for an external system to verify a condition used to trigger a payment.

The general technical structure is therefore:

```
external source
   ↓
condition verification
   ↓
condition satisfied?
   ↓
YES / NO
   ↓
payment execution
```

The nature of the external source depends on the service concerned.

LEGAL BOUNDARY:

> The proposed framework allows for the existence of a condition external to the payment, but the lawfulness of the condition itself would depend on its purpose, the mechanism used, the data processed, the agreement of the parties and the other applicable rules.

In other words:

> **the capability to impose conditions exists; the legal freedom to choose any condition is not established.**

Digital identity and the digital euro have an explicitly provided interface

Another element is particularly important.

The proposed Regulation on the digital euro provides that front-end services must be:

> **interoperable with or integrated into European Digital Identity Wallets** S57.

The European Digital Identity Wallet, for its part, enables the presentation of identity data and attestations of attributes to public or private services S55.

We therefore have an interconnection here that is no longer merely technically deduced:

```
European Digital
Identity Wallet
   ↕
digital euro services
```

DOCUMENTED INTERFACE:

> The proposed framework for the digital euro explicitly provides for interoperability or integration with the European Digital Identity Wallet.

This interface does not mean that all attributes in the wallet become accessible to the payment system.

The safeguards of the eIDAS 2 Regulation continue to apply.

But the existence of the interface itself is documented.

The identity → payment bridge is therefore established, but strictly limited in scope

The conclusion must be precise.

We can now establish:

```
digital identity
   ↕
provided interface
   ↕
digital euro
```

But not:

```
all identity attributes
   ↓
all payments
```

and even less:

```
identity
   +
environment
   ↓
payment authorization
```

ESTABLISHED AT THE LEVEL OF THE PROPOSED FRAMEWORK:

> An interface between the European Digital Identity Wallet and digital euro payment services is explicitly provided for S57.

NOT ESTABLISHED:

> This interface does not demonstrate any use of environmental attributes or DPPs to authorize, refuse or restrict a payment.

The digital euro framework also provides strong privacy safeguards

The proposal notably distinguishes between online and offline payments S57.

For offline payments, the intended level of privacy should be close to that of cash.

The details of offline transactions must not be accessible to the ECB or national central banks under the same conditions as online payments.

For online payments, the proposal provides for technical and organizational measures designed to prevent data transmitted to the Eurosystem from enabling the direct identification of individual users S57.

PRIVACY SAFEGUARD:

> The proposed architecture is not based on the idea that the ECB should have access to a general nominative history of individual payments.

European data protection authorities have nevertheless called for additional safeguards

The EDPB and EDPS examined the digital euro proposal.

They acknowledge the efforts made regarding privacy protection, notably:

- the offline mode;
- data protection by design;
- minimization;
- maintaining the choice between cash and the digital euro.

But they also called for the design to avoid excessive centralization of personal data by the ECB or national central banks.

INSTITUTIONAL POINT OF VIGILANCE:

> Even an architecture explicitly designed to provide a high level of privacy must be examined in light of the amount of data centralized and the allocation of responsibilities among the different actors.

The ability to pay in cash itself constitutes an important safeguard

The proposed framework for the digital euro is not intended to eliminate cash.

The digital euro must constitute an additional means of payment.

European data protection authorities have expressly welcomed maintaining the choice between the digital euro and cash.

The ECB also states that the digital euro should complement banknotes and coins.

SAFEGUARD OF FREEDOM OF CHOICE:

> Under the framework currently proposed, the digital euro must not constitute the only available means of payment.

This safeguard significantly reduces the risk that a restriction specific to the digital euro would automatically result in a general inability to pay.

An interesting architecture emerges when only the documented interfaces are assembled

At this stage, it is necessary to distinguish what is actually established from what remains hypothetical.

The documented elements already make it possible to write:

```
DIGITAL IDENTITY
   ↓
provided interface
   ↓
DIGITAL EURO

DIGITAL EURO
   ↓
conditional payments possible
   ↓
external condition verified

PRODUCT
   ↓
unique identifier
   ↓
DPP
   ↓
product / environmental data

TRANSACTION
   ↓
may identify a product
```

By contrast, the following link remains absent:

```
DPP / environment
   ↓
payment condition
```

DOCUMENTARY BOUNDARY:

> Several segments of the chain exist separately or have documented interfaces, but the connection enabling environmental data originating from the DPP to determine a payment condition is not established.

The real potential weakness is therefore not the absence of safeguards

There are numerous safeguards.

These notably include:

```
IDENTITY

→ user control

→ selective disclosure

→ unobservability

→ data separation

→ alternatives to the wallet

DPP

→ access rights

→ decentralized architecture

→ no customer personal data

  without explicit consent

DIGITAL EURO

→ privacy

→ cash maintained

→ programmable money prohibited
```

But each of these safeguards primarily protects **its own scope**.

The cross-cutting question becomes:

> **What happens when information leaves its original infrastructure and becomes a legally authorized input into another processing operation?**

This is where the most interesting point of friction in 6.7 lies.

A local safeguard does not necessarily constitute a global prohibition on cross-referencing

Three examples illustrate this distinction.

DPP

```
no customer personal data
in the DPP without consent
```

does not automatically mean:

```
impossibility of cross-referencing elsewhere
a transaction and the product identifier
```

Digital identity

```
wallet provider
must not observe
all transactions
```

does not mean:

```
no authorized service
may receive an attribute
presented by the user
```

Digital euro

```
programmable money prohibited
```

does not mean:

```
conditional payment prohibited
```

STRUCTURAL VULNERABILITY:

> Several strong safeguards identified in the texts are scope-specific safeguards: they limit what an infrastructure or actor may do directly, without necessarily constituting a general prohibition on any subsequent processing or any authorized interface with another infrastructure.

This is where Sections 6.2 to 6.6 regain their full importance

Information leaving its silo does not enter a legal vacuum.

Its subsequent processing should still satisfy the requirements examined previously:

```
legal basis
   ↓
purpose
   ↓
compatibility / new legal basis
   ↓
necessity
   ↓
minimization
   ↓
proportionality
   ↓
security
   ↓
rights
   ↓
oversight
```

Thus, the existence of technical interfaces does not remove the general safeguards.

But conversely:

> **the safeguards specific to each infrastructure are not necessarily sufficient, on their own, to prevent any future interconnection.**

A particularly important boundary emerges around consent

Several protections identified rely on an action or request by the user.

For example:

- voluntary presentation of attributes in the wallet;
- explicit consent for certain personal data in the DPP;
- payment conditions agreed between payer and payee.

This constitutes an important safeguard.

But consent is legally valid only where it meets the applicable requirements, notably where it must be freely given.

A question would therefore arise if access to a good, service or means of payment became, in practice, conditional on accepting the cross-referencing of data.

LEGAL BOUNDARY:

> The formal existence of consent or agreement would not necessarily be sufficient if the legal conditions required for it to be considered freely given and valid were no longer met.

NOT ESTABLISHED:

> The sources examined do not demonstrate the current existence of a system requiring an individual to share environmental data in order to access a payment or an essential service.

Freedom of choice therefore constitutes a cross-cutting safeguard to monitor

Two infrastructures include particularly interesting protections in this respect.

For digital identity:

```
wallet
   ↓
must not become
the only means of access
```

For the digital euro:

```
digital euro
   ↓
complement to cash
   ↓
no mandatory replacement
```

This redundancy constitutes a strong safeguard.

It means that the current framework preserves alternative means.

CROSS-CUTTING SAFEGUARD:

> As long as genuine alternatives remain accessible without unjustified disadvantage, the ability of a digital infrastructure to impose, on its own, a condition on economic or administrative life as a whole remains legally and practically limited.

The important word, however, is:

> **genuine.**

An alternative existing only in law but becoming impracticable in practice would raise a different question.

At this stage, the most important boundary can be identified

The investigation does not make it possible to establish:

```
identity
   +
invoicing
   +
DPP
   +
environment
   +
payment
   ↓
individual control
```

But it now makes it possible to establish something more precise:

```
each infrastructure
has its own safeguards
   ↓
certain interfaces
between infrastructures
are explicitly provided for
   ↓
certain external capabilities
can provide conditions
   ↓
local safeguards
do not necessarily amount to
a global prohibition
on future cross-referencing
   ↓
any new cross-referencing
would then have to pass
the general safeguards
examined in 6.1 to 6.6
```

This is the boundary that must be preserved going forward.

Questions now open

> **1. What categories of attributes will actually be usable in the integration between the European Digital Identity Wallet and digital euro services?**

> **2. Can the data presented during this interaction be technically and legally reused for purposes other than authentication or execution of the requested service?**

> **3. How will the wallet's unobservability be audited in interactions with payment services?**

> **4. What safeguards prevent a product or transaction identifier from being used to indirectly reconstruct a relationship between an individual and a DPP without storing that relationship in the DPP itself?**

> **5. What categories of external sources will be able to provide the conditions used by future conditional payment services?**

> **6. To what extent can a payment condition relate to an attribute concerning the payer without becoming incompatible with data protection, proportionality or non-discrimination rules?**

> **7. How will the existence of genuine alternatives be guaranteed when the European Digital Identity Wallet or the digital euro are integrated into public or private services?**

> **8. Can an architecture that is legally compliant silo by silo become disproportionate when its interfaces make it possible to reconstruct information that each silo was specifically designed not to centralize?**

The last question probably constitutes the main cross-cutting research issue arising from this section.

Conclusion of 6.7

ESTABLISHED SAFEGUARD:

> The European Digital Identity Wallet provides for user control, selective disclosure, unobservability of its use by the provider and limitations on the combination of data S55.

ESTABLISHED SAFEGUARD:

> Refusing to use the European Digital Identity Wallet must not, by itself, restrict or disadvantage access to public or private services; alternatives must remain available S55.

ESTABLISHED SAFEGUARD:

> The DPP must not store personal data relating to customers without their explicit consent S56.

ESTABLISHED SAFEGUARD:

> The identification of a product or item in a DPP does not legally constitute, by itself, the identification of its buyer S56.

PROPOSED SAFEGUARD:

> The proposed framework for the digital euro prohibits programmable money and maintains the principle of fully fungible money S57.

EXPLICIT LEGAL LATITUDE IN THE PROPOSAL:

> This prohibition does not extend to conditional payments: the proposed framework expressly provides for payments automatically triggered when predetermined and agreed conditions are met S57.

DOCUMENTED INTERFACE IN THE PROPOSAL:

> Digital euro front-end services must be interoperable with or integrated into European Digital Identity Wallets S57.

LEGAL BOUNDARY:

> The prohibition of programmable money protects the fungibility of the money, but does not constitute a general prohibition on any conditional logic applied to the execution of a payment.

STRUCTURAL VULNERABILITY:

> The safeguards specific to the infrastructures examined primarily protect their respective scopes. They do not necessarily constitute a general prohibition on any external association of data where another processing operation has a valid legal basis.

STRUCTURAL VULNERABILITY:

> An architecture may avoid centralizing a relationship within each of its components while technically allowing that relationship to be reconstructed in a separate processing operation by cross-referencing their identifiers or data.

TO BE ESTABLISHED:

> Are the segregation safeguards provided separately for identity, products and payments sufficient to prevent a future interconnection from reconstructing, within another processing operation, relationships that each infrastructure considered in isolation does not retain?

TO BE ESTABLISHED:

> What legal limits would apply to the choice of an external condition used to trigger a conditional payment where that condition concerns data or attributes relating to an individual?

NOT ESTABLISHED:

> No element examined demonstrates that environmental data, a DPP, a consumption history or an individual environmental score is currently intended to authorize, refuse or restrict a digital euro payment.

NOT ESTABLISHED:

> The digital euro has not yet been adopted or issued as of September 3, 2026. The provisions examined concerning its legal architecture remain those of the legislative framework currently under negotiation.

6.8 Evolution of purposes and the legal framework

Status: ESTABLISHED LEGAL EVOLUTION / NON-IMMUTABLE SAFEGUARDS / FUTURE BOUNDARIES TO BE ESTABLISHED

The previous sections established a significant set of safeguards.

They notably show that current law:

- limits the purposes of processing;

- requires a legal basis;
- regulates reuse;
- imposes necessity, proportionality and minimization;
- protects certain individual decisions against excessive automation;
- provides for rights and avenues of redress;
- imposes specific safeguards on certain infrastructures;
- currently prohibits certain uses, such as programmable money under the proposed framework for the digital euro.

One question nevertheless remains essential:

> **do these safeguards permanently fix the legally authorized purposes and uses?**

The answer is no.

A legal protection applicable today does not necessarily constitute a permanent legal impossibility.

Three different situations must be distinguished

The evolution of an infrastructure may result from very different legal mechanisms.

```
1. same purpose
   +
   technical evolution

2. new use
   compatible with the initial purpose

3. new purpose
   +
   new legal basis
```

These three situations must not be confused.

The GDPR regulates further processing and notably provides for an assessment of the compatibility of a new purpose with the purpose that initially justified the collection S43-S46.

But where new processing is based on a provision of Union or national law satisfying the applicable requirements, the law may also create or modify the legal basis allowing that processing S43-S46-S47.

LEGAL SAFEGUARD:

> An administration cannot simply decide that data collected for a specified purpose may now be used for any other purpose.

LEGAL LATITUDE:

> The legislature or competent regulatory authority may nevertheless modify the legally authorized scope of processing where the conditions laid down by higher-ranking law are respected.

The difference is fundamental.

Purpose limitation is therefore not a guarantee of immutability

An overly simplistic reading of the principle of purpose limitation would suggest:

```
data collected for X
   ↓
usable only for X
forever
```

The law operates in a more complex manner.

Depending on the circumstances, an evolution may result from:

```
initial purpose
   ↓
compatible further processing
```

or:

```
initial purpose
   ↓
new legal text
   ↓
new authorized processing
under new conditions
```

S43-S46

LEGAL VULNERABILITY:

> A safeguard based on the current purpose of processing limits present uses, but does not guarantee that the legal scope of that processing can never evolve.

This does not mean that every evolution would be authorized.

It means that the boundary is legal and not technically immutable.

CFVR provides a concrete example of the gradual evolution of the same infrastructure

This possibility is not merely theoretical.

CFVR has existed since 2014 S58.

Since its creation, its framework has been amended several times.

```
2014

creation of CFVR
   ↓
2017

modification of the processing
   +
experimental extension
to fraud involving individuals
   ↓
2021

further modification
   +
connection with the collection
of certain public data
from online platforms
   ↓
2024

further modification
   ↓
2026

further modification
   +
electronic invoicing
   +
new sources
   +
exchanges with social security bodies
   +
use within the secure data platform
```

S37-S45-S58

ESTABLISHED:

> The legal scope of CFVR has evolved through successive stages since its creation.

The processing nevertheless retains the same general identity:

> **"targeting fraud and enhancing the value of queries."**

An infrastructure can therefore retain its name while changing significantly in scale

This observation is important.

The evolution of a public system does not necessarily require:

```
old system
   ↓
removal
   ↓
new system
```

It may take the form of:

```
same infrastructure
   ↓
new source
   ↓
new category of data
   ↓
new recipient
   ↓
new capability
   ↓
new legal amendment
```

CFVR provides a documented example of precisely this type of evolution S58.

ESTABLISHED:

> The institutional continuity of a processing operation does not mean that its scope of data, sources, recipients or methods of use remains stable.

The 2017 development is particularly revealing

In 2017, the CFVR framework explicitly distinguished between:

```
fraud involving
businesses
   ↓
permanent processing
```

and:

```
fraud involving
individuals
   ↓
two-year
experiment
```

S58

The processing could therefore experimentally use data concerning individuals with no connection to a business.

The current framework now covers fraud involving **both businesses and individuals** S45-S58.

This evolution provides a particularly clear example:

```
limited / experimental capability
   ↓
evaluation and legal evolution
   ↓
integration into
a broader scope
```

LEGAL VULNERABILITY:

> The experimental or limited nature of processing at a given date does not guarantee that its scope will remain experimental or limited.

This does not mean that every experiment necessarily becomes permanent.

It merely demonstrates that making it permanent constitutes a legally possible evolution where a new framework authorizes it.

The integration of electronic invoicing provides a second example

CFVR already existed before the reform examined in this investigation.

Electronic invoicing constitutes a distinct infrastructure, developed notably to meet its own tax and economic requirements.

In 2026, data originating from this infrastructure were expressly integrated among the categories of data used by CFVR S37-S45.

The sequence is therefore documented:

```
infrastructure A
electronic invoicing
   +
infrastructure B
CFVR
   ↓
legal amendment
   ↓
data from A
used in B
```

ESTABLISHED:

> An existing data infrastructure may subsequently become a new legally authorized source for a pre-existing processing operation.

This observation is central to the entire investigation.

The question is therefore no longer solely whether two infrastructures are connected today

It is necessary to distinguish:

```
CURRENT INTERCONNECTION
   ↓
factual question
```

from:

```
FUTURE INTERCONNECTION
   ↓
legal question
   +
possible evolution of the law
```

The current absence of an interconnection is important information.

But it does not make it possible to state:

> **"this interconnection can never legally exist."**

Conversely, the possibility of changing the law provides absolutely no basis for stating:

> **"this interconnection will be created."**

LEGAL SAFEGUARD:

> Any new interconnection involving personal data would have to comply with the legal framework applicable at the time of its implementation.

NOT ESTABLISHED:

> The abstract legal possibility of modifying a processing operation does not demonstrate any institutional intention to create a specific interconnection.

This distinction is essential for the DPP

The current DPP framework provides strong safeguards S56.

But the ESPR itself provides that the delegated acts applicable to the different product groups will notably specify:

```
DPP data
   +
model / batch / item level
   +
actors with access
   +
data accessible to each
   +
period of availability
```

S56

The Regulation also provides that where other provisions of Union law require or allow specific data to be included in the DPP, those data may be incorporated in accordance with the applicable delegated act.

ESTABLISHED:

> The specific content of the DPP and its access rights are not entirely fixed in the framework Regulation: they must be specified for the different product groups through delegated acts S56.

But some DPP limitations remain embedded in the Regulation itself

This capacity for evolution does not remove higher-level safeguards.

The Regulation notably provides that personal data relating to customers must not be stored in the DPP without their explicit consent S56.

Evolution through a delegated act therefore does not mean:

```
Commission
   ↓
unlimited freedom
   ↓
any data
in the DPP
```

Delegated acts must remain within the scope of the delegation and comply with applicable higher-ranking law.

LEGAL SAFEGUARD:

> The ability to specify or modify the content of an infrastructure through subsequent acts does not remove the limitations laid down by the Regulation governing it.

The European Digital Identity Wallet also has an evolving architecture

The eIDAS 2 Regulation establishes the fundamental safeguards of the wallet S55.

But its practical operation also relies on implementing acts determining technical standards, specifications and procedures.

This notably concerns:

- wallet interfaces;
- the issuance and presentation of attributes;
- the identification of relying parties;
- registration procedures;
- certain certification arrangements;
- interoperability S55.

The Regulation also allows several attestations of attributes to be combined under the control of the user.

ESTABLISHED:

> The fundamental legal framework of the wallet is established by the Regulation, while a significant part of its practical operation is specified through implementing acts and technical specifications S55.

Technical evolution can therefore significantly change practical capabilities without removing legal safeguards

This is an additional distinction.

```
stable legal rule
   ↓
new specification
   ↓
new technical capability
```

is not necessarily:

```
new legal purpose
```

But the evolution of standards may increase:

- interoperability;
- the number of available attributes;
- the number of compatible services;
- the ease with which certain proofs can be presented;
- the number of possible interactions between infrastructures.

LEGAL VULNERABILITY:

> The evolution of an infrastructure's practical capabilities may precede or accompany the evolution of its uses, making it necessary to regularly reassess whether the initial legal safeguards remain appropriate to the capabilities actually deployed.

The boundary is even more evident for the digital euro

Unlike eIDAS 2 and the ESPR, the Regulation establishing the digital euro has not yet been definitively adopted at the time of this investigation S57.

The safeguards examined in 6.7 concerning notably:

- the prohibition of programmable money;
- conditional payments;
- privacy;
- integration with the European Digital Identity Wallet;

must therefore be qualified according to their status in the legislative process.

LEGAL SAFEGUARD:

> Until the text is adopted, the provisions of the proposal must not be presented as a definitive and immutable framework.

TO BE ESTABLISHED:

> What safeguards, definitions and technical possibilities relating to conditional payments and interoperability with the European Digital Identity Wallet will appear in the text ultimately adopted?

The central point now emerges: legal protection is dynamic

The previous chapters could give the impression of a static architecture:

```
system
   +
purpose
   +
safeguards
   =
definitive balance
```

The history of CFVR shows a different reality.

The balance looks more like:

```
infrastructure
   ↓
initial legal framework
   ↓
new capability
   ↓
new source
   ↓
amendment of the framework
   ↓
new safeguards
   ↓
new capability
   ↓
new amendment
   ↓
etc.
```

S58

LEGAL VULNERABILITY:

> The compliance of an infrastructure at a given date does not guarantee that its future scope will remain identical; on the contrary, it requires compliance to be reassessed when purposes, data, sources, recipients or capabilities evolve.

This changes the way the safeguards identified in 6.7 should be interpreted

In 6.7, we established in particular:

```
DPP
→ no personal customer data
  without explicit consent

WALLET
→ user control
→ selective disclosure
→ limitation of requests
→ alternatives

DIGITAL EURO
→ programmable currency prohibited
→ conditional payments provided for
  within the proposed framework
```

These safeguards are real.

But they must be read as:

> **safeguards of the applicable legal framework.**

Not as:

> **eternal technical impossibilities.**

The distinction is fundamental.

An evolution can also occur without physically merging the databases

This is probably the most important point for the architecture studied.

A legal evolution does not necessarily need to create:

```
CENTRAL MEGA DATABASE
identity
   +
invoices
   +
products
   +
environment
   +
payments
```

It could theoretically authorize:

```
system A
   ↓
result / attribute

system B
   ↓
result / attribute

   ↓
processing C
```

In other words, the question of freedoms does not depend solely on the existence of a centralized database.

It also depends on:

- the accessible data;
- the identifiers enabling cross-referencing;
- the attributes that can be presented;
- the results that can be transmitted;
- the conditions that can be verified;
- the consequences attached to these results.

LEGAL VULNERABILITY:

> An evolution of the framework can increase the possibilities of cross-referencing without requiring the physical merger of the infrastructures concerned.

This is precisely why the interfaces identified in Chapter 5 and in 6.7 are important

We have separately documented:

```
transaction
⇔ product

product
⇔ DPP

DPP
⇔ environmental data

wallet
⇔ verified attributes

wallet
⇔ digital euro services
   within the proposed framework

external condition
⇔ conditional payment
```

The complete chain:

```
identity
   +
economic history
   +
product
   +
environment
   ↓
condition
   ↓
authorization / refusal / limitation
of a payment
```

is **not established**.

But the relevant legal question is no longer only:

> **"does this chain exist today?"**

It also becomes:

> **"what legal changes would be needed to enable each of its junctions, and what safeguards would oppose them?"**

This is a much more precise and verifiable question.

An important legal boundary appears around rights and freedoms

EU law and constitutional law do not allow the legislature to freely eliminate all protection simply by adopting a new text.

An evolution remains notably confronted with:

```
fundamental rights
   ↓
privacy
   +
data protection
   +
necessity
   +
proportionality
   +
effective safeguards
```

S39-S44-S53

Where a restriction on the rights protected by the GDPR falls within the scope of Article 23, it must notably respect the essence of fundamental freedoms and rights and constitute a necessary and proportionate measure in a democratic society S47.

LEGAL SAFEGUARD:

> The fact that the legislature can make the law evolve does not mean it can legally authorize any surveillance, any profiling, or any restriction whatsoever.

The real vulnerability therefore lies between two false claims

First excessive claim:

```
"it's forbidden today,
so it will be impossible tomorrow"
```

False.

Second excessive claim:

```
"the law can change,
so they will be able to do anything"
```

Also false.

The legally defensible position is:

```
technically capable architecture
   +
use not authorized today
   ↓
possible legal evolution
   ↓
but subject to higher-order norms
   ↓
necessity review
   +
proportionality
   +
fundamental rights
   +
safeguards
   +
judicial review
```

The history of CFVR nevertheless shows why this distinction is not theoretical

Between 2014 and 2026, the same processing underwent several successive modifications S58.

Over the course of these developments, we notably see:

```
more categories of persons
   +
more sources
   +
more data
   +
more analytical capabilities
   +
more exchanges
   +
new computing infrastructure
   +
electronic invoicing
```

S37-S45-S58

Each development taken in isolation may have its own justification and its own safeguards.

The cross-cutting question, however, becomes:

> **at what point should one re-examine not only each extension separately, but also the cumulative effect of all previous extensions?**

This question links directly back to 6.5.

TO BE ESTABLISHED:

> Is there a comprehensive, periodic assessment allowing the cumulative effect of successive modifications to a processing operation on privacy and freedoms to be measured, beyond the legal examination of each modification taken separately?

The documentary risk is one of gradual normalization

Particular caution is required here.

The sources show no evidence of any strategy aimed at progressively introducing a system of generalized control.

Such an intention cannot be inferred merely from the succession of legal texts.

But an objective property can be examined:

```
extension A
→ legally authorized

extension B
→ legally authorized

extension C
→ legally authorized

extension D
→ legally authorized
```

does not automatically imply that:

```
A + B + C + D
```

was the subject of a separate, comprehensive public assessment.

DOCUMENTARY BLIND SPOT:

> The public sources examined do not make it possible to systematically establish how the cumulative effect of all successive extensions of an infrastructure is assessed when a new modification is adopted.

This formulation is much more solid than asserting the existence of drift.

A safeguard can also change in nature when the ecosystem changes

A safeguard that is effective within an isolated infrastructure can become less protective if the technical environment evolves.

Abstract example:

```
product identifier
alone
   ↓
weak capacity
for personal identification
```

then:

```
product identifier
   +
identifiable transaction
   +
identity attribute
   ↓
much greater
cross-referencing capacity
```

The rule specific to the DPP may remain exactly the same.

But the ecosystem surrounding the DPP has changed.

Same reasoning applies to:

```
wallet attribute
   +
payment service
   +
external condition
```

LEGAL VULNERABILITY:

> The real effectiveness of a compartmentalization safeguard must be assessed within the technical and legal ecosystem in which the infrastructure operates, not solely on the basis of the content of its own founding text.

The ultimate question becomes that of a change in consequence

A system may initially serve only to:

```
inform
```

then possibly:

```
recommend
```

then:

```
classify
```

then:

```
orient
```

then, if the law permitted it:

```
condition a decision
```

This last step profoundly changes the legal analysis.

Sections 6.4 and 6.5 showed that the more an automated result becomes determinative in a decision producing a legal or similarly significant effect, the more central the safeguards relating to automated decisions, necessity, and proportionality become S43-S51-S53.

LEGAL SAFEGUARD:

> The fact that a piece of data may legally be used to inform or orient does not automatically mean it can be used to produce an individual restriction.

Applied to the environment, this point becomes decisive

The DPP and environmental infrastructures can produce information concerning the characteristics of a product.

An informative use could take the form of:

```
product
   ↓
environmental information
   ↓
consumer information
```

A far more intrusive architecture would be:

```
product
   +
consumption history
   +
identity
   ↓
individual environmental profile
   ↓
consequence on
payment / right / service
```

These two architectures are not legally equivalent.

NOT ESTABLISHED:

> No element examined currently demonstrates the existence or preparation of a European mechanism assigning individuals an individual environmental score used to limit their payments, purchases, or rights.

LEGAL SAFEGUARD:

> Moving from product-related environmental information to an individual restriction based on a personal profile would constitute a substantial change in processing and would need to be examined against the applicable legal bases and safeguards.

The current absence of the complete chain therefore remains an important conclusion

At this stage:

```
DPP
   ↓
product / environmental information

wallet
   ↓
identity / attributes

conditional payment
   ↓
possible external condition
```

are documented separately.

But:

```
environmental DPP
   ↓
individual profile
   ↓
imposed condition
   ↓
payment refused
```

remains:

> **NOT ESTABLISHED.**

This boundary must not be weakened.

On the contrary, it makes the investigation more solid.

What now needs to be monitored is therefore not an intention, but verifiable modifications

The relevant indicators would notably be:

```
new category of data
   ↓
new identifier
   ↓
new category of accessors
   ↓
new interface
   ↓
new purpose
   ↓
new cross-referencing possibility
   ↓
new individual consequence
```

A change in any one of these elements can be objectively documented.

There is no need to speculate about intentions.

Open questions after 6.8

> **1. What successive modifications have precisely increased the scope of each infrastructure studied since its creation?**

> **2. When a new source is added to an existing processing operation, is the cumulative effect with all sources already present subject to a separate analysis?**

> **3. How will future developments in the DPP's delegated acts modify the available data, its granularity, and the categories of actors able to access it?**

> **4. What new categories of attestations will progressively become usable within the European Digital Identity Wallet?**

> **5. What data will actually be exchanged between the European Digital Identity Wallet and future digital euro services?**

> **6. What external sources could be used by services offering conditional payments?**

> **7. Would a new legal basis be needed if environmental data relating to a product were to be transformed into an attribute relating to a person?**

> **8. What legal basis and what safeguards would be needed if such an attribute were subsequently to influence access to a payment, a service, or a right?**

> **9. Is there a mechanism for identifying the moment when several extensions, individually legally admissible, together produce an architecture requiring a new overall assessment of proportionality?**

Conclusion of 6.8

ESTABLISHED:

> The legal scope of a public data infrastructure can evolve over time. CFVR provides a documented example of this since 2014 S58.

ESTABLISHED:

> CFVR has undergone several successive modifications concerning in particular the persons concerned, the data sources, the associated processing operations, and, in 2026, the integration of data from electronic invoicing S37-S45-S58.

ESTABLISHED:

> The ESPR regulation provides that the concrete content, granularity, and access rights to the DPP are to be specified for different product groups by delegated acts S56.

ESTABLISHED:

> The concrete operation of the European Digital Identity Wallet also relies on implementing acts and technical specifications, within the limits set by the eIDAS 2 regulation S55.

LEGAL SAFEGUARD:

> A change in the law does not permit the higher-order requirements relating to fundamental rights, data protection, necessity, and proportionality to be freely set aside.

LEGAL LATITUDE:

> A purpose, data source, recipient, or interconnection that is not legally authorized today may, depending on the circumstances, subsequently become subject to a new legal basis, provided the applicable higher-order norms are respected.

LEGAL VULNERABILITY:

> A safeguard based on the current scope of a processing operation constitutes present protection, but not a guarantee that this scope will remain unchanged.

LEGAL VULNERABILITY:

> An evolution can increase the possibilities of cross-referencing between infrastructures without requiring their physical merger into a single database.

DOCUMENTARY BLIND SPOT:

> The public sources examined do not make it possible to systematically establish how the cumulative effect of all successive extensions of an infrastructure is reassessed when a new extension is adopted.

TO BE ESTABLISHED:

> To what extent can several successive extensions, each individually legally regulated, alter the overall balance of an infrastructure before a new overall assessment of necessity and proportionality becomes indispensable?

NOT ESTABLISHED:

> No element examined demonstrates that a legal evolution is currently underway to create an individual environmental profile linked to digital identity and used to authorize, refuse, or limit a payment, a purchase, a service, or a right.

NOT ESTABLISHED:

> The legal possibility of subsequently modifying the purposes or interfaces of an infrastructure does not constitute proof that such a modification is being contemplated.

6.9 Legal vulnerabilities and limits of the analysis

Status: VULNERABILITIES IDENTIFIED / HIGHER-ORDER SAFEGUARDS / FACTUAL LIMITS OF THE INVESTIGATION

The investigation is now able to answer a more important question than whether each infrastructure studied is, taken in isolation, legally regulated.

The final question is:

> **what happens when several legally distinct infrastructures simultaneously increase their capacities for collection, identification, cross-referencing, analysis, and action?**

The preceding sections have established that the law contains numerous protections.

They have also shown that these protections do not all constitute technical impossibilities, and that the legal scope of infrastructures can evolve.

The main vulnerability identified by this investigation lies precisely in this gap.

```
TECHNICAL CAPABILITY
   ↓
broader than
   ↓
LEGALLY AUTHORIZED USE
TODAY
```

This difference currently protects against certain uses.

But it also means that the evolution of the law becomes an essential variable of the architecture.

First vulnerability: functional centralization can exist without a single central database

The investigation did not identify a single European database bringing together:

```
identity
   +
invoices
   +
transactions
   +
products
   +
environmental data
   +
payments
```

Such a claim would be incorrect.

The preceding chapters have, however, documented several specialized infrastructures with their own identifiers, interfaces, registries, verification mechanisms, or cross-referencing capabilities.

French electronic invoicing provides a particularly concrete example.

Data from electronic invoices now constitutes a source for CFVR and must feed the DGFiP's secure data platform in order to be exploited at scale S37-S45.

CFVR already cross-references numerous other tax, economic, administrative, and social sources.

ESTABLISHED:

> Physical centralization in a single database is not necessary to enable cross-referencing between information originating from distinct systems.

LEGAL VULNERABILITY:

> The separate regulation of several infrastructures is not necessarily sufficient to assess the consequences resulting from their combination when they become interoperable, or when the results produced by one can be used by another.

The determining question is therefore not only:

> **"where is the data stored?"**

but also:

> **"what information can be linked, verified, transmitted, or used to produce a consequence?"**

Second vulnerability: a purpose that is legally limited today may evolve tomorrow

Section 6.8 established that CFVR already provides a historical example of successive modifications to the same processing operation S58.

An infrastructure can retain its institutional existence while seeing the following evolve:

- its sources;

- its categories of data;
- the persons concerned;
- its recipients;
- its technical capabilities;
- its modes of operation.

LEGAL SAFEGUARD:

> An administration cannot freely modify a purpose or freely reuse data outside the applicable legal framework.

LEGAL VULNERABILITY:

> The current absence of a given use does not necessarily constitute a definitive legal prohibition: a new text may modify the authorized scope, subject to compliance with higher-order law.

This distinction rules out two opposing conclusions.

```
"it's not authorized today
so it will always be impossible"
```

is not demonstrated.

But:

```
"the law can evolve
so this use will be authorized tomorrow"
```

is not demonstrated either.

Third vulnerability: accumulation can become more significant than each extension taken in isolation

The analysis of CFVR reveals a cross-cutting difficulty.

A succession can take the form of:

```
extension A
   +
extension B
   +
new source C
   +
new exchange D
   +
new capability E
```

Each can be legally examined at the time of its introduction.

But the ultimate issue becomes:

```
A + B + C + D + E
   ↓
OVERALL CAPABILITY
```

DOCUMENTARY BLIND SPOT:

> The public sources examined do not make it possible to systematically establish how the cumulative effect of all successive extensions of an infrastructure is reassessed independently of the examination of each new modification.

This question becomes particularly important when the following progress simultaneously:

```
volume
   +
number of sources
   +
precision
   +
interoperability
   +
algorithmic capability
   +
number of recipients
```

Fourth vulnerability: interoperability can produce a new capability without merging systems

The infrastructures studied are increasingly designed around:

- identifiers;
- interfaces;
- registries;
- verifiable attestations;
- attribute-presentation mechanisms;
- services capable of verifying conditions;
- common standards.

This allows for an architecture in which one infrastructure does not necessarily need to receive all the raw data from another.

```
SYSTEM A
   ↓
attribute / proof / result

SYSTEM B
   ↓
verification

SYSTEM C
   ↓
consequence
```

LEGAL VULNERABILITY:

> A distributed infrastructure can produce consequences comparable to those of a centralized system without requiring the creation of a database physically containing all the data concerned.

This property makes it insufficient to examine databases alone.

The interfaces must also be examined.

Fifth vulnerability: the shift from information to consequence

This boundary is probably the most important in the entire chapter.

Data can be used to:

```
INFORM
```

then:

```
VERIFY
```

then:

```
CLASSIFY
```

then:

```
ORIENT
```

and possibly:

```
CONDITION
```

These functions do not produce the same legal consequences.

CFVR already provides an example of this distinction.

Algorithmic results can guide officers, but the CNIL requires that they not replace human analysis and that the human decision remain effective S37-S51.

LEGAL SAFEGUARD:

> Authorization to use data to inform, detect, or verify does not automatically constitute authorization to use it to produce an individual restriction.

LEGAL VULNERABILITY:

> The more determinative a piece of data or an algorithmic result becomes for access to a payment, a service, a right, or another significant possibility, the more determinative the requirements relating to legal basis, proportionality, accuracy, transparency, the ability to challenge, and automated decisions become.

Sixth vulnerability: an error can change in nature as it passes through several infrastructures

The preceding sections identified the rights of access and rectification.

But an interconnected architecture poses an additional difficulty.

```
erroneous data A
   ↓
processing B
   ↓
classification C
   ↓
attribute D
   ↓
decision E
```

Correcting A does not, on its own, technically guarantee that:

```
B
C
D
E
```

have all been recalculated, corrected, or neutralized.

The law provides for various obligations of rectification, restriction, and notification to recipients when the corresponding conditions are met S43.

LEGAL VULNERABILITY:

> In a distributed architecture, the effectiveness of the right to rectification depends not only on correcting the source data, but also on the ability to identify and correct the derived consequences still associated with that data.

DOCUMENTARY BLIND SPOT:

> The public sources examined do not establish the existence of a cross-cutting mechanism allowing a person to learn of, and then have automatically corrected, all derived data or propagated consequences across several legally distinct infrastructures.

Seventh vulnerability: protection sometimes depends on maintaining a functional separation

Several of the safeguards identified rest on boundaries.

For CFVR:

```
algorithm
   ↓
flagging
   ↓
human analysis
   ↓
decision
```

For the DPP:

```
product information
   ≠
personal consumer profile
```

For the digital euro within the proposed framework:

```
conditional payment
   ≠
programmable currency
```

For the European wallet:

```
presentation of a necessary attribute
   ≠
systematic disclosure
of the entire identity
```

These separations constitute genuine safeguards.

But their effectiveness depends on their being maintained.

LEGAL VULNERABILITY:

> When a protection rests on a separation between two functions that are technically capable of being brought closer together, any evolution reducing that separation must be subject to a new legal analysis.

Eighth vulnerability: the digital euro could be created without the individual consent of each citizen

A distinction must be drawn here between the creation of a currency and an individual obligation to use it.

The proposed European framework provides for a legislative procedure enabling the digital euro to be established.

Once this framework is adopted, the decision whether or not to issue the digital euro would belong to the ECB S57.

This is not, therefore, a mechanism based on the individual consent of each citizen to the creation of this new form of currency.

ESTABLISHED:

> The possible creation of the digital euro falls within the European institutional and legislative process and, subsequently, within the framework envisaged, an issuance decision by the ECB; it is not conditional on the individual agreement of each user.

But this observation does not mean:

```
digital euro created
   =
obligation for each citizen
to give up cash
```

The framework currently being negotiated instead provides for the coexistence of the digital euro with cash, together with measures intended to preserve the access to and acceptance of cash S57.

NOT ESTABLISHED:

> No element examined makes it possible to assert that the current framework provides for the abolition of cash or a general obligation for each citizen to use the digital euro exclusively.

Ninth vulnerability: control of a digital currency and control of the use of each unit are not legally equivalent

A central bank digital currency infrastructure necessarily entails rules concerning, among other things:

- its issuance;
- its distribution;
- its operation;
- its intermediaries;
- its possible holding limits;
- its payment mechanisms.

The framework currently proposed does indeed envisage holding limits S57.

But another boundary exists.

The ECB considers that intrinsically limiting:

```
where
 +
when
 +
to whom
```

a unit of digital euro can be spent would amount to creating a programmable currency incompatible with its character as a fully fungible currency and with its status as legal tender S57.

LEGAL SAFEGUARD:

> The proposed framework excludes the transformation of the digital euro into a programmable currency whose units would intrinsically impose restrictions concerning the goods, services, places, times, or beneficiaries for which they could be used.

This safeguard is important.

It must not be confused with conditional payments.

Tenth vulnerability: conditional payments nevertheless create an interface with external conditions

The preceding chapters documented the technical and experimental possibility of using an externally verified condition to trigger a payment.

The proposed framework for the digital euro precisely distinguishes:

```
PROGRAMMABLE CURRENCY
   ↓
intrinsic restriction
on the currency
   ≠
CONDITIONAL PAYMENT
   ↓
payment triggered
according to an agreed condition
```

S22-S27-S28-S57

ESTABLISHED:

> The proposed framework prohibits programmable currency while allowing the development of conditional payment services.

This distinction constitutes simultaneously:

```
a SAFEGUARD
   +
an INTERFACE TO MONITOR
```

The safeguard is that the currency itself cannot be restricted to certain uses.

The interface to monitor concerns the nature of the conditions used by payment services.

This is where the environmental question must be formulated with maximum precision

The preceding chapters established:

```
product
   ↓
DPP
   ↓
environmental data
```

and separately:

```
external condition
   ↓
verification
   ↓
conditional payment
```

But they did not establish:

```
identity
   ↓
purchase history
   ↓
personal environmental score
   ↓
quota
   ↓
payment authorization / refusal
```

NOT ESTABLISHED:

> No element examined currently demonstrates the existence, deployment, or legal adoption of an individual "environmental pass" using DPP data to determine whether or not a person may make a payment.

This conclusion must remain explicit.

But it does not exhaust the legal question.

The real question becomes: what protections would be activated if this boundary were crossed?

A hypothetical architecture:

```
IDENTITY
   +
TRANSACTIONS
   +
PRODUCTS
   +
ENVIRONMENTAL DATA
   ↓
INDIVIDUAL PROFILE
   ↓
CONDITION
   ↓
PAYMENT / SERVICE / RIGHT
```

could not be analyzed as a mere technical extension.

It would notably have to be examined in light of:

- its legal basis;
- its purpose;
- necessity;

- proportionality;
- minimization;
- rights of access and rectification;
- rules relating to profiling;
- automated decisions, where their conditions are met;
- the fundamental rights affected;
- the available remedies.

S43-S44-S47-S51-S53

LEGAL SAFEGUARD:

> An infrastructure technically capable of producing a restriction is not legally authorized to produce it merely because that capability exists.

And even a new law does not constitute an unlimited power

This is probably the most important legal boundary in this chapter.

A new law or a new regulation may change the authorized uses.

But:

```
NEW LAW
   ≠
UNLIMITED LEGAL POWER
```

Where a measure restricts fundamental rights protected by EU law, that restriction must notably:

```
be provided for by law
   +
respect the essential content of the right
   +
be necessary
   +
be proportionate
   +
genuinely meet
an objective of general interest
or protect the rights of others
```

S39-S44

LEGAL SAFEGUARD:

> The evolution of the law can shift certain boundaries, but it remains itself subject to higher-order legal norms and to judicial review.

This safeguard constitutes the limit to the idea that:

> **"it would be enough to change the law to be able to do anything."**

The electronic invoicing reform nevertheless constitutes a major change of scale

It is worth returning here to the starting point of the investigation.

A structured electronic invoice is not merely a PDF sent by another route.

It transforms previously scattered economic information into data that is:

```
structured
   +
standardized
   +
automatically exploitable
   +
transmissible
   +
cross-referenceable
   +
analyzable at scale
```

Chapters 1 and 2 established the nature and lifecycle of this data.

Chapter 5 examined the possibilities for interconnection.

The present chapter has shown that certain electronic invoicing data are now integrated into CFVR and exploited within an algorithmic infrastructure capable of processing a volume of several billion invoices per year S37-S45.

ESTABLISHED:

> The reform substantially increases the quantity of structured economic data likely to be processed automatically by the tax administration.

But "centralizing everything" would be an excessive conclusion

The record does not demonstrate:

```
ELECTRONIC INVOICING
   ↓
SINGLE DATABASE
   ↓
all identity
   +
all products
   +
all the environment
   +
all payments
```

NOT ESTABLISHED:

> The French electronic invoicing reform does not, on the basis of the sources examined, constitute a central database bringing together all the infrastructures analyzed in this investigation.

The precise conclusion is different:

> **it creates a new, massive layer of structured economic data that can become a source for other processing operations when the law authorizes it.**

CFVR now provides a concrete example of this.

This is precisely what makes electronic invoicing a structuring infrastructure

The critical point is therefore not:

> **"electronic invoicing already controls everything."**

The documented point is:

```
ECONOMIC ACTIVITY
   ↓
STRUCTURED DATA
   ↓
TRANSMISSION
   ↓
LARGE-SCALE PROCESSING
   ↓
CROSS-REFERENCING
   ↓
ALGORITHMIC ANALYSIS
```

This chain now exists within the tax domain studied S37-S45.

LEGAL VULNERABILITY:

> The more an infrastructure transforms diffuse economic activity into structured, standardized, and interoperable data, the more decisive the evolution of its purposes, its recipients, and its cross-referencing possibilities becomes for freedoms.

The fundamental vulnerability is therefore not a hidden function

At the conclusion of the investigation, no source revealed:

```
secret button
"total control"
```

The vulnerability identified is more structural.

```
DIGITIZATION
   ↓
STRUCTURING
   ↓
IDENTIFICATION
   ↓
INTEROPERABILITY
   ↓
CROSS-REFERENCING
   ↓
ANALYSIS
   ↓
POSSIBLE CONDITION / DECISION
```

At each stage, safeguards exist.

But each stage also increases the potential capability of the next.

The protection of freedoms therefore depends less on the existence of capabilities than on the boundaries imposed on their use

This investigation ultimately shows that two realities can be true simultaneously.

First reality:

> **the infrastructures studied do not today constitute a legally authorized system of general control over purchases, identity, the environment, and currency.**

Second reality:

> **they objectively increase the technical capabilities for identification, structuring, cross-referencing, verification, and automation available within the European digital ecosystem.**

There is no contradiction between these two findings.

It is precisely the space between them that the law must protect.

The red lines then become identifiable

The investigation now makes it possible to define changes that would require a particularly rigorous reassessment:

> **1. use of a common identifier systematically linking identity, purchases, products, and payments;**

> **2. transformation of environmental information relating to products into an individual environmental profile;**

> **3. use of this profile to produce a consequence on a payment, a service, or a right;**

> **4. transformation of algorithmic assistance into a mechanism practically determining the human decision;**

> **5. disappearance or substantial reduction of the possibility of using a means of payment not associated with the same level of traceability;**

> **6. extension of purposes allowing the cross-use of data initially collected within distinct infrastructures;**

> **7. practical impossibility for a person to know, correct, or challenge the data and derived results used with respect to them;**

> **8. multiplication of separately justified extensions without sufficient public assessment of their cumulative effect.**

None of these points should be presented as having occurred when it has not.

They constitute verifiable monitoring criteria.

What the investigation does not allow us to assert

NOT ESTABLISHED:

> It is not established that the European Union or France are currently setting up a system intended to assign an individual environmental score to citizens.

NOT ESTABLISHED:

> It is not established that DPP data will be used to determine the authorization or refusal of a person's purchases.

NOT ESTABLISHED:

> It is not established that the digital euro will allow the ECB to authorize or prohibit a person's purchases depending on the products they wish to buy.

NOT ESTABLISHED:

> It is not established that electronic invoicing, the DPP, the European Digital Identity Wallet, and the digital euro will be brought together within a single control infrastructure.

NOT ESTABLISHED:

> It is not established that cash will be abolished upon the possible introduction of the digital euro.

These limits do not diminish the investigation.

They define its solidity.

What it does allow us to establish

ESTABLISHED:

> Electronic invoicing transforms a significant portion of economic activity into structured data that can be exploited automatically.

ESTABLISHED:

> Some of this data is now intended to feed CFVR and the DGFiP's secure data platform S37-S45.

ESTABLISHED:

> CFVR already combines numerous sources and uses algorithmic methods to detect anomalies and guide tax audits S37.

ESTABLISHED:

> The DPP makes it possible to associate structured information with products, which may notably include environmental information S56.

ESTABLISHED:

> The European Digital Identity Wallet enables the presentation and verification of electronic attributes according to the framework studied S55.

ESTABLISHED:

> The proposed framework for the digital euro distinguishes and prohibits programmable currency while allowing conditional payment services S57.

ESTABLISHED:

> The purposes, sources, and scope of certain public infrastructures can evolve legally over time, as the history of CFVR demonstrates S58.

LEGAL SAFEGUARD:

> These technical capabilities cannot be freely combined to produce any individual consequence whatsoever: their use remains subject to legal bases, authorized purposes, fundamental rights, and the requirements of necessity and proportionality.

Conclusion of 6.9

The result of the investigation is therefore neither:

```
"everything is already connected"
```

nor:

```
"current safeguards make
any evolution impossible"
```

The result is more precise.

```
DISTINCT INFRASTRUCTURES
   ↓
GROWING CAPABILITIES
   ↓
GROWING INTEROPERABILITY
   ↓
CROSS-REFERENCING POSSIBILITIES
   ↓
USES LIMITED BY
CURRENT LAW
   ↓
BUT A LEGAL FRAMEWORK
LIKELY TO EVOLVE
   ↓
UNDER THE CONTROL OF
FUNDAMENTAL RIGHTS
```

LEGAL VULNERABILITY:

> The main risk identified is not the demonstrated existence of a single control system, but the possibility that successive extensions of purposes, access, interfaces, or consequences progressively bring initially separate infrastructures closer together.

DOCUMENTARY BLIND SPOT:

> Public sources generally make it possible to study each infrastructure and each legal modification separately, but make it much less easy to assess the cumulative effect of the entire ecosystem on the capabilities for identification, cross-referencing, and decision-making.

LEGAL SAFEGUARD:

> Even where an evolution is decided by the legislature, restrictions placed on fundamental rights remain subject to the requirements of legality, respect for the essential content of rights, necessity, and proportionality.

NOT ESTABLISHED:

> The investigation currently demonstrates neither the existence of an individual "environmental pass," nor the use of an environmental profile to control payments, nor a single architecture automatically linking electronic invoicing, digital identity, the DPP, and the digital euro in order to restrict citizens' rights or purchases.

CONCLUSION:

> **The determining question is therefore not whether the infrastructure already allows for generalized control. It is whether the legal boundaries that today separate collection, information, identification, cross-referencing, profiling, and decision-making will continue to evolve at the same pace as the technical capabilities that make it possible to cross them.**

And it is precisely for this reason that the analysis must remain evolving:

> **every new data source, every new identifier, every new interface, every new purpose, and every new consequence attached to these infrastructures must be examined not only in isolation, but also for what it enables when combined with what already exists.**

Chapter 7 — General Summary

> **Navigation:** ← Back to table of contents

This chapter brings together the main elements established over the course of the investigation and puts the results of the various chapters into perspective.

The aim is to clearly distinguish:

- what is **ESTABLISHED** by the sources examined;
- what has been **TESTED/PILOTED** in documented projects or pilots;
- what is **TECHNICALLY DEDUCIBLE** from the identified architectures and connections;
- what remains **NOT ESTABLISHED** or **TO BE ESTABLISHED**.

The summary does not seek to turn a technical possibility into an established fact. On the contrary, it aims to determine how far the sources allow the chain under study to be traced back, and to precisely identify the points at which the demonstration stops.

Table of contents

Chapter 1 — Invoicing data transmitted to the administration

Status: ESTABLISHED

The French electronic invoicing reform puts in place an infrastructure enabling the automated transmission of structured economic data to the tax administration.

This data notably includes the identification of the businesses party to a transaction, invoice dates and numbers, amounts excluding tax, VAT rates and amounts, as well as certain information relating to deliveries and payments.

From 1 September 2027, for the B2B transactions concerned, the data transmitted will also include information at the invoice-line level:

- the precise description of the good or service;
- the quantity;
- the unit price excluding tax.

In these situations, the system therefore makes it possible to transmit to the administration structured data precisely describing the economic content of a B2B transaction.

For B2C transactions falling under e-reporting, by contrast, the data currently planned is aggregated on a daily basis. The documented elements therefore do not make it possible to assert that the details of each individual purchase made by a private individual are transmitted to the administration.

Chapter 2 — Data retention, access, and purposes

Status: ESTABLISHED / TO BE ESTABLISHED

The texts examined establish that the reform is not limited to the technical transmission of invoices. Structured data from invoices, transactions, and, in the situations provided for, payments, is transmitted to the administration within an organized framework involving accredited platforms.

Businesses remain subject to their own obligations to retain tax documents. These obligations do not, however, make it possible to infer that the administration retains the data it receives for an identical period.

Combating VAT fraud, pre-filling VAT returns, real-time knowledge of business activity, and steering public policy are among the officially stated objectives of the reform.

DGFiP documentation also indicates that the availability and use of data obtained automatically and continuously is intended to facilitate understanding of economic conditions, notably by sector of activity, as well as the steering of the economy by public authorities.

The reform's preparatory work also mentions the possibility of enriching analytical models with the data collected, in particular to facilitate the detection of, and support for, businesses in difficulty.

It is therefore established that the data collected does not serve solely a function of invoice transmission or VAT determination: its exploitation must also contribute to monitoring economic activity and steering public policy.

Several elements nevertheless remain to be established, notably the precise retention period for the various categories of data by the administration, access and authorization rules, the automated processing actually applied, any cross-referencing with other databases, and the legal conditions allowing their reuse for other public policies.

The sources examined do not make it possible to establish the existence of an interconnection with environmental data, a digital monetary infrastructure, or mechanisms allowing certain transactions to be made conditional. These possibilities must be examined separately in the following chapters.

Chapter 3 — Environmental data

Status: ESTABLISHED / TECHNICALLY DEDUCIBLE / TO BE ESTABLISHED

The European Union has established a legal and technical framework for the Digital Product Passport (DPP), allowing structured, machine-readable, interoperable digital data to be associated with identifiable products.

Depending on the requirements applicable to different product categories, the passport can be defined at the model, batch, or individual item level.

The information that may be associated with certain products notably includes data relating to their composition, durability, repairability, recyclability, and their carbon or environmental footprint.

The European Union also has methods enabling it to quantify certain environmental impacts of products over their life cycle. The battery regulation already provides a concrete example in which a quantitative carbon footprint is officially associated with certain categories of products.

The DPP is based on structured identifiers and may notably include a GTIN or an equivalent identifier. The standards used in electronic commercial exchanges also make it possible to carry standardized identifiers at item level.

It is therefore technically possible, where a common identifier or a matching mechanism exists and the necessary access rights are in place, to cross-reference a commercial transaction with the environmental information associated with the corresponding product.

Environmental data does not need to be directly recorded on the invoice for such cross-referencing to be technically achievable: the product identifier can be used to retrieve this information from a separate system.

Likewise, the buyer's identity does not need to be stored in the DPP for cross-referencing to be technically possible, if another system separately holds the information needed to identify the party to the transaction and the product concerned.

Where several transactions involve identifiable products to which quantitative environmental values are attached, these values can also, from a technical standpoint, be cross-referenced and aggregated by a system with the necessary data and access rights.

The DPP's regulatory architecture also provides for interoperability mechanisms, automated exchanges, an API, a European registry, and an interconnection with customs systems. Several European projects also combine digital traceability, proof of commercial transactions, and administrative actors responsible in particular for VAT and customs.

These elements do not, however, make it possible to establish that an individual environmental footprint of purchases is currently calculated by the administration, that products' environmental data is automatically cross-referenced with French invoicing or e-reporting data, or that it is used to authorize, refuse, or make a payment conditional.

Chapter 4 — Digital euro and payment infrastructures

Status: ESTABLISHED / TECHNICALLY DEDUCIBLE / TO BE ESTABLISHED

The digital euro project rests on a centralized settlement infrastructure operated by the Eurosystem and distributed to users via payment service providers.

This infrastructure does not rest on a blockchain as the foundation of the system. Users would mainly retain a relationship with their bank or payment service provider, while the Eurosystem would perform the central functions needed for settlement and for the infrastructure's operation.

For online payments, the published technical model provides for the processing of structured data relating to users, accounts, devices, providers, payers, payees, and transactions.

Transactions notably have identifiers, an amount, a date and time, a type, an environment, and a status. The model also includes various pieces of information enabling the identification or categorization of the actors involved in a transaction.

Certain information relating to the merchant may also come into play in the process. The Merchant Category Code, or MCC, notably makes it possible to categorize the type of commercial activity of the payee and is among the information transmitted at certain stages of the documented payment process.

The architecture, however, distinguishes between the data present in the model, the data actually transmitted during a transaction, and the data each actor can actually access. The existence of a data field in the technical model therefore does not mean that all participants in the system can view it.

The project also provides for offline functionality allowing certain payments to be made directly between devices without an internet connection. In this mode, the personal details of the transaction are not transmitted to payment service providers or to the Eurosystem, either during or after the payment. This architecture constitutes an important limitation on the possibilities for systematically centralizing transaction-related information.

The digital euro proposal explicitly excludes the creation of a programmable currency, understood as monetary units to which restrictions determining the goods, services, places, persons, or periods for which they could be used would be intrinsically attached.

This prohibition does not, however, mean the absence of automated mechanisms around payments.

European Central Bank documentation explicitly provides for conditional payments, in which the execution of a transaction may depend on the prior verification of a condition.

The Eurosystem can provide the fundamental monetary functions necessary for these mechanisms, notably the reservation of funds, while the logic used to determine whether a condition is satisfied can be managed by payment service providers or other market actors.

The ECB's technical work also indicates that external monitoring can play a part in triggering these conditions.

This general mechanism is no longer merely a theoretical possibility. Market actors have connected their own platforms, via APIs, to an environment simulating the digital euro's back end in order to experiment with various conditional payment scenarios.

The scenarios studied notably include payment on delivery, pay-per-use, staged payments, certain automated refunds, and machine-to-machine payments.

It is therefore established, in principle, that information or an event originating from a system external to the monetary layer can be verified by a service in order to play a part in the decision to execute, release, hold, or return funds associated with a given transaction.

The external information used to verify a condition does not necessarily need to be stored in full within the monetary infrastructure: an external system can perform the verification and transmit only the result needed for the conditional process.

European digital identity, moreover, has an explicitly documented link with payment infrastructures.

The European Digital Identity Wallet, or EUDI Wallet, can be used in payment authentication processes. The ECB also plans to use it as a strong authentication method by providers participating in the digital euro pilot for certain online transactions.

The EUDI Wallet notably relies on mechanisms for verifiable attestations, data minimization, and selective disclosure. The existence of this link therefore does not mean that all the information held in the wallet is communicated to the merchant, the payment provider, or the Eurosystem.

The elements examined thus make it possible to separately establish the existence of structured and identifiable transactions, conditional payments, a conditionality layer capable of using information from external systems, interfaces allowing market-actor platforms to interact with the payment environment, and an explicit link between digital identity and payment.

These elements make it technically possible to build services in which information from an external infrastructure plays a part in an automated decision concerning a given transaction, without the currency itself becoming programmable.

They do not, however, make it possible to establish that a digital product passport, a GTIN, a carbon footprint, data from electronic invoicing, or an individual environmental profile is currently used to trigger, prevent, or modify a payment in digital euros.

The generic link between an external system and a conditional payment is therefore documented. The specific link between environmental or tax data and the execution of a payment remains to be established.

Chapter 5 — Interconnections

Status: ESTABLISHED / TESTED/PILOTED / TECHNICALLY DEDUCIBLE / NOT ESTABLISHED

Chapter 5 examined the links — existing, planned, tested, or technically possible — between the infrastructures studied separately in the preceding chapters.

The research shows that these infrastructures do not constitute a single, centralized system, but that they are not entirely independent of one another either.

The European Commission explicitly places several of these mechanisms within a shared objective of interoperability and the creation of synergies. The Digital Product Passport, eInvoicing, the European Business Wallets, and other European infrastructures are notably presented as forming part of a coherent ecosystem of digital solutions.

The reuse of electronic invoicing data, moreover, goes beyond the mere processing of the invoice itself. European work notably provides for its reuse for sustainability reporting and its cross-referencing with certain customs data.

The European Business Wallets constitute another documented point of convergence. The project provides for their use in identifying economic operators, verifiable attestations, certain tax and transactional information, and interactions with the Digital Product Passport and product-related data.

Standardization work also provides a direct link between transaction and product. The European model for eReceipts provides that a receipt may contain an identifier linking the purchased product to its Digital Product Passport and the corresponding verified information, notably including certain information on its durability and environmental impacts.

The following chain therefore now has documented links:

```
transaction
   ↓
eReceipt
   ↓
DPP identifier
   ↓
Digital Product Passport
   ↓
product / durability / environmental information
```

At the same time, the European pilots examined have documented a chain linking business identity, payment, a detailed electronic receipt, the Business Wallet, and experimental accounting or tax processing.

```
identity / authorization
   ↓
wallet
   ↓
payment
   ↓
detailed eReceipt
   ↓
Business Wallet
   ↓
accounting / experimental tax processing
```

The link between digital identity and payment is also documented: the EUDI Wallet can be involved in payment authentication, and its use is planned in the work relating to the digital euro pilot.

Finally, the ECB's work establishes that an external system can play a part in verifying a condition used by a conditional payment service.

```
external system
   ↓
verification of a condition
  ↓
conditionality layer
   ↓
payment
```

These various elements make it technically possible to reconstruct an architecture in which data relating to a product could be retrieved from an external infrastructure, evaluated by a service, and turned into a result usable by automated logic surrounding a transaction.

It nevertheless remains **NOT ESTABLISHED** that environmental data originating from the Digital Product Passport or an equivalent infrastructure is currently used as a condition to authorize, refuse, or limit a payment.

It also remains **NOT ESTABLISHED** that a centralized system brings together individual identity, a comprehensive purchase history, tax data, environmental data, and payment data, or that a generalized individual carbon profile is calculated from these infrastructures.

The work relating to the digital euro also maintains an essential distinction: programmable currency, whose units would intrinsically carry restrictions on the goods or services that could be purchased, is explicitly excluded, whereas conditional payment services distinct from the currency itself are planned and being tested.

The result of Chapter 5 is therefore precise: **a significant portion of the infrastructures and links technically enabling transaction, product, environment, identity, and payment to be associated with one another is now documented; some of these links are explicitly planned, standardized, or tested; but the link that would actually turn environmental data into an imposed rule authorizing or refusing a payment has not been established.**

Chapter 6 — Legal safeguards

Status: ESTABLISHED / LEGAL SAFEGUARDS / LEGAL VULNERABILITIES / DOCUMENTARY BLIND SPOTS

Chapter 6 examined whether the technical capabilities and interconnections identified in the preceding chapters could be freely exploited and combined.

The answer is no.

The existence of a piece of data, an identifier, an interface, or a technical possibility for cross-referencing does not in itself constitute legal authorization to use it for a new purpose.

The GDPR, EU law, national law, and the safeguards specific to the various infrastructures notably impose requirements relating to:

- the legal basis of processing operations;
- the determination and compatibility of purposes;
- necessity and proportionality;
- data minimization;
- security and access control;
- the rights of individuals;
- profiling and automated decisions;
- oversight by independent authorities and the courts.

The investigation nevertheless established that these protections do not all constitute technical impossibilities or guarantees of permanence.

The example of CFVR is particularly important.

This processing operation has had its scope legally modified on several occasions since its creation. In 2026, data from electronic invoicing was integrated among its new sources, within an architecture allowing its large-scale algorithmic exploitation and its cross-referencing with other information used for anomaly detection and the targeting of tax audits.

This development concretely demonstrates that a data infrastructure created for one specific function can subsequently become a legally authorized source for another processing operation.

It does not demonstrate that every future interconnection will be authorized.

It demonstrates that the current legal scope of processing operations must not be confused with a permanent impossibility of their uses evolving.

Chapter 6 also identified an essential distinction between physical centralization and functional centralization.

An architecture does not need to bring all information together in a single database in order to enable it to be cross-referenced.

Distinct systems can exchange:

```
identifier
   +
attribute
   +
proof
   +
result
   +
verified condition
```

without necessarily transferring the entirety of their raw data.

This property is particularly important for the analysis of the infrastructures studied in this report, which rely heavily on structured identifiers, registries, interfaces, verifiable attestations, and interoperability mechanisms.

Chapter 6 also established that certain important safeguards are explicitly written into the frameworks studied.

The DPP notably provides for restrictions concerning customers' personal data.

The European Digital Identity Wallet provides for mechanisms of minimization, user control, and selective disclosure.

The framework currently proposed for the digital euro excludes programmable currency, that is, a currency whose units would intrinsically carry restrictions determining the goods, services, persons, places, or periods for which they can be used.

This prohibition, however, coexists with the possibility of developing conditional payment services based on externally verified conditions.

The distinction is fundamental:

```
programmable currency
   ≠
conditional payment
```

The first mechanism is excluded within the framework studied.

The second is planned for and has been the subject of experiments.

Chapter 6 identified no basis for asserting that environmental data relating to a product is currently being turned into an individual payment restriction.

But it confirms the legal importance of the boundary located between:

```
information
   ↓
verification
   ↓
profiling
   ↓
condition
   ↓
individual consequence
```

The more determinative a piece of data or a result becomes for access to a payment, a service, a right, or another significant possibility, the more central the requirements relating to legal basis, necessity, proportionality, accuracy, transparency, the ability to challenge, and fundamental rights become.

ESTABLISHED:

> The technical capabilities documented in the preceding chapters are legally regulated and cannot be freely combined for any purpose whatsoever.

ESTABLISHED:

> Data from electronic invoicing joined a pre-existing tax processing operation, CFVR, in 2026; CFVR's scope had already undergone several successive changes.

LEGAL SAFEGUARD:

> A new technical capability or a new interconnection does not, on its own, constitute legal authorization to produce an individual consequence.

LEGAL VULNERABILITY:

> The legally authorized scope of an infrastructure can evolve, subject to compliance with the applicable higher-order norms.

LEGAL VULNERABILITY:

> An increase in the possibilities for cross-referencing does not necessarily require the creation of a centralized database physically bringing all the data together.

DOCUMENTARY BLIND SPOT:

> The public sources examined make it easier to assess each infrastructure and each extension separately than to assess the cumulative effect of the full set of their developments and interconnections.

NOT ESTABLISHED:

> No element examined currently demonstrates the existence of a mechanism using an individual environmental profile to authorize, refuse, or limit a person's payments, purchases, services, or rights.

NOT ESTABLISHED:

> No element examined demonstrates the existence of a single infrastructure automatically bringing together electronic invoicing, digital identity, environmental data, the Digital Product Passport, and the digital euro in order to control individual transactions.

General conclusion

The six chapters now make it possible to trace a chain that, at the start of the investigation, was only a hypothesis to be verified.

The French electronic invoicing reform is transforming a significant portion of economic activity into structured, standardized, transmissible data that can be exploited automatically.

This data does not serve merely to carry an invoice.

The sources examined establish its use, or intended use, for various tax and economic purposes, notably combating fraud, pre-filling VAT returns, monitoring economic activity, and steering public policy.

Since 2026, certain data from electronic invoicing has also become a source for the CFVR processing operation and its large-scale processing infrastructure.

At the same time, the European Union is developing several other digital infrastructures.

The Digital Product Passport makes it possible to associate structured data with identifiable products, which may include information relating to their durability and environmental impacts.

European standards for electronic receipts make it possible to link a transaction and a product to its Digital Product Passport.

Digital identity infrastructures enable the presentation and verification of attributes.

The link between digital identity and payment is documented.

Pilots have connected identity, payment, a transactional receipt, and the Business Wallet.

Finally, work relating to the digital euro has established that an external system can play a part in verifying a condition used by a conditional payment service.

The bridge sought at the start of the investigation has therefore indeed been partially built

The investigation does not end at the same point where it began.

At the outset, the question was whether infrastructures concerning:

```
invoicing
   +
transaction
   +
product
   +
environment
   +
identity
   +
payment
```

could actually have points of connection.

Several of these links are now **ESTABLISHED**, **STANDARDIZED**, or **TESTED/PILOTED**.

The resulting documentary chain can be represented as follows:

```
INVOICING / TRANSACTION
   ↓
STRUCTURED DATA
   ↓
PROCESSING AND CROSS-REFERENCING

TRANSACTION
   ↓
eRECEIPT
   ↓
IDENTIFIABLE PRODUCT
   ↓
DIGITAL PRODUCT PASSPORT
   ↓
PRODUCT INFORMATION
   ↓
DURABILITY / ENVIRONMENT
```

At the same time:

```
IDENTITY / ATTRIBUTES
   ↓
WALLET
   ↓
AUTHENTICATION
   ↓
PAYMENT
```

and:

```
EXTERNAL SYSTEM
   ↓
VERIFICATION
OF A CONDITION
  ↓
CONDITIONAL
PAYMENT SERVICE
   ↓
PAYMENT
```

Another chain has also been tested:

```
IDENTITY / AUTHORIZATION
   ↓
WALLET
   ↓
PAYMENT
   ↓
DETAILED eRECEIPT
   ↓
BUSINESS WALLET
   ↓
ACCOUNTING /
TAX PROCESSING
```

The result is therefore different from a simple juxtaposition of independent infrastructures.

> **Bridges exist.**

But not all segments carry the same status or the same level of evidence.

The final decisive connection has not been established

The investigation makes it technically possible to reconstruct:

```
transaction
   ↓
identifiable product
   ↓
DPP
   ↓
environmental information
```

It also makes it possible to reconstruct separately:

```
external system
   ↓
verified condition
   ↓
conditional payment
```

It further documents:

```
digital identity
   ↓
payment
```

But it has not established the final connection:

```
IDENTITY
   +
TRANSACTION HISTORY
   +
PRODUCTS
   +
ENVIRONMENTAL DATA
   ↓
INDIVIDUAL
ENVIRONMENTAL PROFILE
   ↓
IMPOSED CONDITION
   ↓
AUTHORIZATION / REFUSAL /
LIMITATION OF A PAYMENT
```

NOT ESTABLISHED:

> No element examined currently demonstrates that this complete chain is deployed or legally organized in order to control an individual's payment possibilities.

This limitation is fundamental.

It prevents presenting as a fact what remains a possibility constructed from separately documented capabilities.

But it would also be incorrect to conclude that the bridge does not exist

The absence of the final connection does not reset the findings of the investigation.

The sources made it possible to move from:

```
HYPOTHESIS
“these systems might perhaps
one day be connected”
```

to:

```
FINDING
several connections already exist,
are standardized,
provided for
or have been experimented with
```

The documentary boundary is now located much further along the chain.

What remains **NOT ESTABLISHED** is no longer the general possibility of linking transactions, products, environmental data, identity and payments.

What remains **NOT ESTABLISHED** is their combined use for a single purpose producing an individual restriction.

This distinction constitutes one of the main findings of the investigation.

Chapter 6 nevertheless introduces a second boundary: technical possibility is not legal authorization

Even when a connection is technically possible, it cannot be freely exploited.

Processing remains subject in particular to:

```
legal basis
   +
purpose
   +
necessity
   +
proportionality
   +
data minimization
   +
data subject rights
   +
oversight
   +
fundamental rights
```

An infrastructure capable of linking two pieces of information is therefore not automatically authorized to do so.

And an infrastructure capable of producing a condition is not automatically authorized to use that condition to restrict a payment, a service or a right.

This distinction constitutes a genuine safeguard.

But the legal framework is not immutable

The investigation has also established that the purposes, sources, categories of data and recipients of a processing operation can evolve legally.

CFVR provides a concrete example.

Since its creation, its scope has been amended several times.

In 2026, data from electronic invoicing became a new source for this pre-existing processing system.

The boundary between:

```
"technically possible
but not used"
```

and:

```
"legally authorised
and effectively used"
```

can therefore evolve.

This finding does not demonstrate any particular future development.

It demonstrates that the legal framework observed today should not be presented as a guarantee of immutability.

The electronic invoicing reform must therefore be placed within a broader shift in scale

The investigation does not establish that electronic invoicing constitutes a central database bringing together all the information examined.

Such a claim would be excessive.

It does establish, however, that this reform transforms a significant share of economic activity into structured data that can be transmitted and processed automatically.

In the tax domain, its integration into CFVR now provides a concrete example of reuse within a broader algorithmic infrastructure.

The reform therefore constitutes a ****structuring infrastructure for economic data****.

Its significance does not come from the fact that it already centralises "everything".

It comes from the fact that it makes a growing share of economic activity:

```
STRUCTURED
↓
STANDARDISED
↓
MACHINE-READABLE
↓
TRANSMISSIBLE
↓
CROSS-REFERENCABLE
↓
ANALYSABLE
```

The question of its future interconnections therefore becomes just as important as that of its present purposes.

The final result must therefore be formulated with two simultaneous truths

First truth:

> **the investigation has not demonstrated the current existence of a generalised system using identity, purchases, environmental data and digital currency to control individuals' economic possibilities.**

Second truth:

> **the investigation has demonstrated that a significant part of the technical building blocks and connections enabling transactions, products, environmental information, identity and payment to be linked already exists, is provided for by standards, integrated into European architectures or has been the subject of experiments.**

These two statements are not contradictory.

They precisely define the level of evidence reached.

What has been established

ESTABLISHED:

> Electronic invoicing creates a massive infrastructure of structured economic data that can be processed automatically.

ESTABLISHED:

> Certain data from this infrastructure now feeds into CFVR, where it can be cross-referenced with other information as part of algorithmic processing intended in particular for anomaly detection and tax targeting.

ESTABLISHED:

> Standards make it possible to link a transaction, an identifiable product, a Digital Product Passport and verified information relating to the product, including certain environmental information.

ESTABLISHED / EXPERIMENTED:

> Digital identity can be involved in payment processes, and experiments have linked identity, payment, detailed electronic receipts and the Business Wallet.

ESTABLISHED / EXPERIMENTED:

> An external system can verify a condition whose result is used within a conditional payment service.

TECHNICALLY DEDUCIBLE:

> The documented connections make it technically possible to build a chain linking an identifiable transaction to information relating to the product and its environmental impact, and then to use the result of an external verification within conditional logic surrounding a payment.

What has not been established

NOT ESTABLISHED:

> It has not been demonstrated that a generalised individual environmental profile is currently calculated from citizens' purchases.

NOT ESTABLISHED:

> It has not been demonstrated that environmental information from the DPP is currently used as a condition for authorising, refusing or limiting a person's payments.

NOT ESTABLISHED:

> It has not been demonstrated that electronic invoicing, the DPP, digital identity and the digital euro are brought together within a single infrastructure intended to control individual behaviour.

NOT ESTABLISHED:

> It has not been demonstrated that the digital euro will make it possible to intrinsically programme the currency in order to prohibit the purchase of certain categories of goods; on the contrary, the framework examined explicitly excludes programmable money.

The conclusion of the investigation is therefore neither a validation nor an accusation

It is a mapping.

It shows:

```
what exists
   +
what communicates
   +
what has been experimented with
   +
what is technically possible
   +
what the law allows
   +
what it prohibits or regulates
   +
what remains to be demonstrated
```

The essential finding is that **the bridge has indeed been built over a substantial part of its path**.

It no longer rests solely on a succession of hypotheses.

Several of its pillars are documented by regulations, standards, technical architectures, European projects and experiments.

But the final passage:

```
ENVIRONMENTAL DATA
   ↓
INDIVIDUAL PROFILE
   ↓
IMPOSED RULE
   ↓
ECONOMIC
OR MONETARY RESTRICTION
```

remains **NOT ESTABLISHED**.

This is exactly where the available evidence ends today.

Final conclusion

> **This investigation does not establish the current existence of a system for environmental control of payments or individual economic behaviour.**

> **It does establish, however, that a substantial part of the technical architecture that would make certain connections possible already exists: structured economic data, identification of transactions and products, Digital Product Passport, environmental data associated with products, digital identity, payment infrastructures, verification of external conditions and conditional payments.**

> **Several connections between these building blocks are established, standardised or have been experimented with. The technical bridge is therefore no longer an abstract hypothesis.**

> **What has not been established is its full activation for a single purpose enabling an individual environmental profile to be established and an imposed consequence to be derived from it regarding a payment, purchase, service or right.**

> **Current law also provides several safeguards against such a development. However, the study of CFVR demonstrates that the legal scope of processing operations can evolve over time.**

> **The boundary to monitor is therefore no longer limited to the emergence of new databases. It lies in new connections, new purposes, new attributes, new conditions and, above all, the new consequences that the law could progressively authorise on the basis of already existing infrastructures.**

> **The investigation therefore stops exactly at the limit of the available evidence: far enough to establish that the building blocks and several bridges exist; not far enough to assert that they currently constitute the integrated control system that their combination would make technically possible.**

Official Sources

> **Navigation:** ← Back to table of contents

This file constitutes the central registry of sources used throughout the report.

Each source is assigned a unique identifier `[S1](#s1)`, `[S2](#s2)`, `[S3](#s3)`, etc.

This identifier is retained throughout all chapters to allow claims to be verified and their precise origin to be identified.

Primary and official sources are given priority.

S1 DGFiP — Invoice data transmitted to the administration

Organization: Directorate General of Public Finances

Document: Summary table of invoice data to be transmitted to the administration — domestic B2B transactions

Updated: August 2026

Used in: Chapter 1

Established elements: nature and granularity of B2B invoicing data transmitted to the administration, including line-level data applicable from September 1, 2027: precise description of the good or service, quantity and unit price excluding tax.

Link:

- https://www.impots.gouv.fr/sites/default/files/media/1_metier/2_professionnel/EV/2_gestion/290_facturation_electronique/japprof_donnees-de-facture-a-transmettre-a-ladministration-correspondance-flux_vf.pdf

---

S2 DGFiP — Transaction data transmitted to the administration

Organization: Directorate General of Public Finances

Document: Transaction data — transaction e-reporting — to be transmitted to the administration pursuant to Article 290 of the French General Tax Code

Updated: August 2026

Used in: Chapter 1

Established elements: data transmitted for B2C and international B2B transactions; daily aggregated nature of B2C e-reporting; detailed data applicable to international B2B transactions.

Link:

- https://www.impots.gouv.fr/sites/default/files/media/1_metier/2_professionnel/EV/2_gestion/290_facturation_electronique/japprof_donnees-de-transactions-a-transmettre_vf.pdf

---

S3 DGFiP — Payment data transmitted to the administration

Organization: Directorate General of Public Finances

Document: Payment data to be transmitted to the administration

Updated: August 2026

Used in: Chapter 1

Established elements: transmission of collection dates and amounts collected by VAT rate; arrangements applicable to electronic invoices, international B2B transactions and B2C transactions.

Link:

- https://www.impots.gouv.fr/sites/default/files/media/1_metier/2_professionnel/EV/2_gestion/290_facturation_electronique/japprof_donnees-de-paiement-a-transmettre_vf.pdf

---

S4 DGFiP — External specifications for electronic invoicing

Organization: Directorate General of Public Finances

Document: B2B External Specifications

Version examined: 3.2 — April 30, 2026

Used in: Chapters 1 and 2

Established elements: functional architecture of the system, formats and methods for exchanging data with the administration, centralization of invoicing, transaction and payment data.

Link:

- https://www.impots.gouv.fr/specifications-externes-b2b

S5 DGFiP — Objectives of the reform

Organization: Directorate General of Public Finances

Document: Discovering electronic invoicing

Used in: Chapter 2

Established elements: official objectives of the reform, including combating VAT fraud, pre-filling tax returns, obtaining real-time knowledge of business activity and supporting public policy management.

Link:

- https://www.impots.gouv.fr/professionnel/je-decouvre-la-facturation-electronique

---

S6 DGFiP — Educational fact sheet on the objectives of the reform

Organization: Directorate General of Public Finances

Document: Educational fact sheet on electronic invoicing

Updated: September 2025

Used in: Chapter 2

Established elements: automatic and continuous processing of data, knowledge of economic conditions and economic policy management by public authorities.

Link:

- https://www.impots.gouv.fr/sites/default/files/media/1_metier/2_professionnel/EV/2_gestion/290_facturation_electronique/fiche-0_tpe_preambule_2025.pdf

---

S7 French General Tax Code — Data transmission

Organization: French Republic — Légifrance

Document: French General Tax Code — provisions relating to electronic invoicing and e-reporting

Version examined: provisions applicable as of September 1, 2026

Used in: Chapter 2

Established elements: legal basis for the transmission of invoicing, transaction and payment data to the administration.

Link:

- https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006162565/

S8 French Tax Procedures Code — Article L. 102 B

Organization: French Republic — Légifrance

Document: French Tax Procedures Code — Article L. 102 B

Versions examined: version applicable as of September 1, 2026 and version applicable from January 1, 2027

Used in: Chapter 2

Established elements: retention period for books, registers, documents and records that may be subject to the administration's rights of access, investigation and audit; six-year period in the version applicable in 2026 and extension of the general period to ten years from January 1, 2027.

Link — version applicable in 2026:

- https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000046869194/2026-07-27

Link — version applicable from January 1, 2027:

- https://www.legifrance.gouv.fr/codes/id/LEGIARTI000053189500/2027-01-01

S9 French Tax Procedures Code — Article L. 102 B bis

Organization: French Republic — Légifrance

Document: French Tax Procedures Code — Article L. 102 B bis

Version examined: provisions applicable from January 1, 2027

Used in: Chapter 2

Established elements: obligation to retain invoices under conditions guaranteeing the authenticity of their origin, the integrity of their content and their legibility throughout their retention period.

Link:

- https://www.legifrance.gouv.fr/codes/id/LEGIARTI000053189500/2027-01-01

S10 French General Tax Code, Annex II — Articles 242 nonies E and 242 nonies E bis

Organization: French Republic — Légifrance

Document: French General Tax Code, Annex II — obligations of approved platforms

Version examined: in force since July 29, 2026

Used in: Chapter 2

Established elements: mandatory services provided by approved platforms; guarantees of authenticity of origin, integrity of content and legibility of invoices; processing and transmission of information required for the system; retention for three years after the termination of the formal agreement allowing a platform to update certain information in the central directory.

Link:

- https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006069569/LEGISCTA000046385430/

S11 French General Tax Code, Annex II — Article 242 nonies L

Organization: French Republic — Légifrance

Document: French General Tax Code, Annex II — Article 242 nonies L

Version examined: in force since July 29, 2026

Used in: Chapter 2

Established elements: transmission of invoicing data to the administration by the issuer's approved platform within twenty-four hours of the electronic invoice being submitted to the platform.

Link:

- https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000054552554/2026-09-01

S12 French General Tax Code, Annex II — Articles 242 nonies G and 242 nonies H

Organization: French Republic — Légifrance

Document: French General Tax Code, Annex II — central directory and transmission of data to the administration

Version examined: in force since July 29, 2026

Used in: Chapter 2

Established elements: collection, through a dedicated solution, of invoicing, transaction and payment data as well as information relating to processing statuses; content and operation of the central directory; identification of taxable persons, legal persons governed by public law and approved platforms; consultation of the directory by approved platforms for invoice addressing purposes.

Link:

- https://www.legifrance.gouv.fr/codes/id/LEGISCTA000054552483/2026-07-29

S13 DGFiP — Electronic invoicing and approved platforms

Organization: Directorate General of Public Finances

Document: Electronic invoicing and approved platforms

Used in: Chapter 2

Established elements: role of the approved platform registration service; monitoring of transmission obligations imposed on platforms and their users; possible imposition of financial penalties; possible withdrawal of registration in the event of repeated breaches.

Link:

- https://www.impots.gouv.fr/facturation-electronique-et-plateformes-agreees

S14 Government — Preliminary assessment of the electronic invoicing reform

Organization: Government — document appended to the 2022 supplementary finance bill, published by the French National Assembly

Document: Preliminary assessment of the article relating to the generalization of electronic invoicing and the transmission of transaction data

Year: 2022

Used in: Chapter 2

Established elements: objective of improving real-time knowledge of business activity in order to enable economic policy management as closely aligned as possible with the economic reality of businesses; example of a potential use of the collected data to enrich analytical models and facilitate the detection and support of businesses in difficulty.

Link:

- https://www.assemblee-nationale.fr/dyn/docs/PRJLANR5L16B0017.raw

S15 European Union — Ecodesign for Sustainable Products Regulation and Digital Product Passport

Organization: European Parliament and Council of the European Union

Document: Regulation (EU) 2024/1781 of June 13, 2024 establishing a framework for the setting of ecodesign requirements for sustainable products

Used in: Chapter 3

Established elements: legal framework for the Digital Product Passport; possibility of establishing the passport at model, batch or item level; association of the passport with a persistent unique product identifier;

structured, machine-readable, searchable and transferable data based on open and interoperable standards; establishment of a digital registry managed by the European Commission containing at least the unique identifiers; access to the registry by the Commission, competent national authorities and customs authorities in the performance of their duties; planned interconnection between the registry and the EU CSW-CERTEX system enabling automated exchanges with national customs systems.

Link:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1781

[S16] European Commission — Data accessible through the Digital Product Passport

Organization: European Commission — Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

Document: The Digital Product Passport (DPP) for Consumers

Used in: Chapter 3

Established elements: depending on the product group and applicable legislation, the Digital Product Passport may provide information relating to durability, repairability and recyclability; environmental impacts, including carbon and environmental footprints; product materials and components; its use and maintenance; hazardous substances; as well as its disassembly, reuse or recycling.

Link:

- https://single-market-economy.ec.europa.eu/single-market/digital-product-passport/consumers_en

---

S17 OpenPeppol — Standard item identification in electronic invoicing

Organization: OpenPeppol

Document: Peppol BIS Billing 3.0 — structure and rules relating to standard item identification

Used in: Chapter 3

Established elements: invoice lines may contain a standard item identifier corresponding to business term BT-157; this identifier is based on a registered identification scheme; Peppol also provides for the use of standardized product identifiers in its business flows, including the GTIN for item identification in orders.

Link:

- https://docs.peppol.eu/poacc/billing/3.0/bis/

S18 European Commission — Product Environmental Footprint method

Organization: European Commission

Document: Commission Recommendation (EU) 2021/2279 of December 15, 2021 on the use of the Environmental Footprint methods to measure and communicate the life cycle environmental performance of products and organisations

Used in: Chapter 3

Established elements: existence of a harmonized European Product Environmental Footprint (PEF) method for measuring and communicating the potential environmental impacts of a product throughout its life cycle; use of data and models relating in particular to materials, manufacturing processes, energy, transport and end-of-life; possibility of defining specific rules by product category through Product Environmental Footprint Category Rules (PEFCR).

Link:

- https://environment.ec.europa.eu/document/download/cb899bd7-bb06-491d-9989-c856a401fcd0_en

---

S19 European Union — Carbon footprint and Digital Battery Passport

Organization: European Parliament and Council of the European Union

Document: Regulation (EU) 2023/1542 of July 12, 2023 concerning batteries and waste batteries

Used in: Chapter 3

Established elements: progressive requirement to declare the carbon footprint for certain categories of batteries; expression of the footprint in kilograms of CO_2 equivalent per kWh of energy provided over the expected service life; breakdown of the footprint according to different life cycle stages; calculation based in particular on data specific to the battery model and production plant; consideration of raw material acquisition and pre-processing, production, distribution and end-of-life; use of the climate change impact assessment method derived from the Product Environmental Footprint; progressive association of this information with the digital system established for batteries.

Link:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32023R1542

S20 European Union — Architecture and operation of the Digital Product Passport registry

Organization: European Commission

Document: Implementing Regulation (EU) 2026/1778 on the implementation arrangements for the Digital Product Passport registry

Used in: Chapter 3

Established elements: operational architecture of the European Digital Product Passport registry; secure interface; API enabling passport registration and the receipt of information from the registry; verification platform; user identification and authorization mechanisms; generation of unique registration identifiers; semantic repository; logging of operations; verification of economic operators and other actors in the value

chain; possibility of delegating access rights; automated communication of the unique registration identifier through an interface or API response; retention and versioning of certain registration data; possibility of integration with other Union information systems that have an equivalent or identical identity verification process.

Link:

- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32026R1778

S21 European Commission — EBSI / e-Origin: commercial transactions, traceability and Digital Product Passport

Organization: European Commission — European Blockchain Services Infrastructure (EBSI)

Document: e-Origin

Used in: Chapter 3

Established elements: existence of a European pilot involving, in particular, VAT administration, marketplaces, online sellers, customs brokers and customs authorities; storage and sharing of proofs of commercial transactions; recognition of these proofs by customs authorities to facilitate customs clearance; secure data sharing between sellers, marketplaces and authorities; development, within the EBSI-ELSA project, of traceability capabilities using the Digital Product Passport.

Link:

- https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/e-Origin

---

S22 European Commission — Proposal for a Regulation establishing the digital euro

Organization: European Commission

Document: Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro — COM(2023) 369 final

Date: June 28, 2023

Used in: Chapter 4

Established elements: proposed legal framework for the digital euro; status as central bank money; distribution through payment service providers; digital euro accounts and payment instruments; funding and defunding operations; possibility for the ECB to set certain holding limits; organization of digital euro payment services.

Link:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52023PC0369

S23 European Central Bank — Architecture and progress of the digital euro

Organization: European Central Bank

Document: Digital euro FAQ

Latest update examined: August 17, 2026

Used in: Chapter 4

Established elements: envisaged technical architecture based on a centralized settlement platform; processing and verification of settlements and holdings by the Eurosystem; no use of DLT or blockchain infrastructure as the foundation of the system; architecture relying on multiple regions and multiple servers to ensure resilience; user access through a bank or public intermediary; possibility of online and offline payments; project still under development and, at this stage, no final decision to issue the digital euro.

Link:

- https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.fr.html

---

S24 European Central Bank — Digital euro rulebook and participant architecture

Organization: European Central Bank

Document: Digital euro scheme rulebook v0.91 and technical annexes

Date: July 2, 2026

Used in: Chapter 4

Established elements: functional and technical organization of the envisaged digital euro system; definition of actors and end-to-end flows; requirements applicable to distributing and acquiring payment service providers; acceptance arrangements; common services; data management and exchange; risk and fraud management; transaction settlement; interfaces and technical standards enabling communication between the different components of the system.

Link:

- https://www.ecb.europa.eu/euro/digital_euro/timeline/rulebook/html/index.fr.html

---

S25 European Central Bank — Digital euro data model, dictionary and exchanges

Organization: European Central Bank

Document: Digital euro scheme rulebook v0.91 — Annex D1 Front-end implementation specification #7 “Data management”; Annex D2 Back-end implementation specification #6 “Data exchange”; Annex D2 Back-end implementation specification #8 “Data dictionary”

Date: July 2, 2026

Used in: Chapter 4

Established elements: envisaged data model for individual and business users, accounts, devices and transactions; transaction identifiers and end-to-end identifier; amount, date and time, currency, direction, type, environment and additional transaction information; payer and payee identifiers; initiation methods; merchant identification and categorization; Merchant Category Code; points of interaction and certain location data; management of risk and fraud scores; use of pseudonymous identifiers; data exchange service enabling the DESP to provide PSPs with reports and queries according to their roles, including for operational, analytical and statistical purposes.

Link:

- https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/html/index.en.html

---

S26 European Central Bank — Operation and privacy of offline digital euro payments

Organization: European Central Bank

Document: Preparation phase of a digital euro — Closing report; documentation relating to digital euro privacy and technical work on offline functionality

Date of elements examined: October 2025 to August 2026

Used in: Chapter 4

Established elements: distinct architecture for online and offline payments; possibility of making offline payments without an Internet connection; direct transfer between devices using cryptographically secured values; local storage of value and sensitive information in a secure hardware element; no transmission of transaction details to PSPs or the Eurosystem during or after the offline payment; knowledge of personal transaction details limited to the payer and payee; anti-money laundering controls performed by the PSP during funding and defunding operations; technical work focusing in particular on embedded Secure Elements and eSIMs; preparation of a pilot including offline payments.

Link:

- https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202510.en.html

---

S27 European Central Bank — Conditional payments and distinction from programmable money

Organization: European Central Bank

Documents: Preparation phase of a digital euro — Closing report; Digital Euro Innovation Platform — Outcome report; ECB documentation and communications relating to conditional payments

Date of elements examined: September 2025 to July 2026

Used in: Chapter 4

Established elements: explicit exclusion of programmable money; distinction between programmability of money and conditional payments; funds reservation functionality provided by the Eurosystem infrastructure; separation between a settlement layer provided by the Eurosystem and a conditionality layer developed by market participants; possibility of external verification triggering the condition; transfer of funds when the condition is verified; cancellation or expiration of the reservation when the condition is not fulfilled; experimentation with conditional payments in a simulated environment; examples including payment on delivery, pay-per-use, milestone payments, automatic refunds and machine-to-machine payments; possibility for banks and other providers to develop value-added services based on the data available to them.

Links:

- https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202510.en.html
- https://www.ecb.europa.eu/euro/digital_euro/innovation-platform/html/index.en.html

---

S28 European Central Bank — Experimentation with external conditions and integration with market participants' platforms

Organization: European Central Bank

Document: Digital euro innovation platform — Outcome report: pioneers and visionaries workstreams

Date: September 26, 2025

Used in: Chapter 4

Established elements: technical experimentation with conditional payments in an environment simulating the digital euro back-end; connection of participants' platforms to simulated interfaces through APIs; provision by the Eurosystem of core technical functions, including funds reservation; definition and management of conditional logic by PSPs and other market participants; possibility of external monitoring triggering conditions; experimentation with scenarios in e-commerce, financial services, transport and Industry 4.0; payment on delivery, pay-per-use and milestone payments; machine-to-machine payments; automation of certain refunds and settlements; exploration of electronic receipts and other payment-related value-added services.

Link:

- https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.deprep250926_innovationplatform.en.pdf

---

S29 European Commission and European Central Bank — EUDI Wallet, payment authentication and digital euro

Organizations: European Commission; European Central Bank

Documents: EU Digital Identity Wallet — Payment Authentication Manual; EU Digital Identity Wallet Pilot implementation; FAQs on the digital euro pilot

Latest updates examined: July-August 2026

Used in: Chapter 4

Established elements: use of the European Digital Identity Wallet for online and in-store payment authentication; integration with existing payment infrastructures; use of verifiable attestations enabling the wallet to be linked to a payer and a payment account; possibility of presenting certain attributes such as age or residence through selective disclosure; presentation of attestations to a bank, acquirer or merchant; progressive obligation to accept the EUDI Wallet for certain strong authentication procedures when requested by the user; explicitly provided possibility for PSPs participating in the digital euro pilot to use the EUDI Wallet as a strong authentication method for online payments.

Links:

- https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/935397429/Payment%2BAuthentication
- https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation
- https://www.ecb.europa.eu/euro/digital_euro/pilot/html/ecb.faq-digital-euro-pilot.en.html

---

S30 European Commission — European Business Wallets and interoperability with European digital infrastructures

Organization: European Commission

Document: Proposal for a Regulation establishing European Business Wallets — COM(2025) 838 final; Staff Working Document SWD(2025) 837 final

Date: November 19, 2025

Used in: Chapter 5

Established elements: proposed creation of a harmonized infrastructure enabling economic operators to identify and authenticate themselves, store, manage and exchange verifiable data and attestations with public administrations and other economic operators; architecture designed in alignment with the European Digital Identity framework and the EUDI Wallet; explicit pursuit of interoperability with existing European digital infrastructures; possibility of securely and verifiably storing and exchanging VAT-related attestations and transaction data in the context of VAT in the Digital Age to support real-time reporting and trusted invoicing; possibility of integration with existing IT systems of businesses and public administrations.

Links:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52025PC0838
- https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-establishment-european-business-wallets

---

S31 European Commission — Single Market Strategy: DPP, eInvoicing, Business Wallet and data reuse

Organization: European Commission

Document: The Single Market: our European home market in an uncertain world — A Strategy for making the Single Market simple, seamless and strong — COM(2025) 500 final

Date: May 21, 2025

Used in: Chapter 5

Established elements: presentation of the

Digital Product Passport, eInvoicing, the future European Business Wallet, the Single Digital Gateway, the Once-Only Technical System, the Business Register Interconnection System and other initiatives as components of a coherent ecosystem of digital solutions intended to create synergies and facilitate data exchange; intention to increase the reuse of data generated through electronic invoicing; pilot project for reusing eInvoicing data for sustainability reporting; project to link eInvoicing data with customs data in connection with the development of the EU Customs Data Hub.

Links:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52025DC0500
- https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/einvoicing_en

---

S32 European Union — Standards, identifiers, APIs and interoperability mechanisms

Organizations: European Commission; European Union

Documents: European documentation relating to eInvoicing interoperability and the EN 16931 standard; Regulation (EU) 2024/1781 on ecodesign for sustainable products; Implementing Regulation (EU) 2026/1778 relating to the Digital Product Passport registry; proposal for a Regulation relating to European Business Wallets

Dates of elements examined: 2024 to 2026

Used in: Chapter 5

Established elements: use of structured data and common semantic models in eInvoicing; requirements for persistent unique identifiers and open, structured, machine-readable and interoperable formats in the Digital Product Passport; implementation of a DPP registry API, a semantic repository, identification and authorization mechanisms and unique product and operator identifiers; use of APIs, verifiable electronic attestations, access control mechanisms and interoperability standards in the proposed architecture of European Business Wallets; broader European strategy aimed at interoperability between public digital infrastructures.

Links:

- https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467108973/Interoperability%2Bof%2BeInvoicing
- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1781
- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32026R1778
- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52025PC0838

S33 ECB / European Commission — Actors, consortia and joint experiments

Organizations: European Central Bank; European Commission; WE BUILD Large Scale Pilot

Documents: Digital euro innovation platform — Outcome report; official documentation relating to the EUDI Wallet Large Scale Pilots; documentation and Architecture & Integration Blueprint of the WE BUILD consortium

Dates of elements examined: September 2025 to August 2026

Used in: Chapter 5

Established elements: participation of approximately 70 market participants in the ECB's Digital Euro Innovation Platform, including banks, payment service providers, fintechs, technology companies, merchants and other private actors; experimentation by these participants with functionalities and services based on the simulated digital euro infrastructure; existence of the European WE BUILD consortium bringing together more than 200 public and private organizations around use cases relating to businesses, supply chains and payments; experimentation within the same architecture with processes including digital identity, Business Wallet, business data, electronic invoicing, banking services and payments; participation of financial and technology actors in several European initiatives relating to identity and payments.

Links:

- https://www.ecb.europa.eu/euro/digital_euro/innovation-platform/html/index.en.html
- https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.deprep250926_innovationplatform.en.pdf
- https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487808/What+are+the+Large+Scale+Pilot+Projects
- https://www.webuildconsortium.eu/
- https://webuild-consortium.github.io/wp4-architecture/blueprint/blueprint.html

---

S34 WE BUILD — Experimental chains linking identity, payment, digital receipt and taxation

Organizations and sources: WE BUILD Consortium; technical documentation published by iGrant.io as a participant in the WE BUILD consortium

Documents: WE BUILD documentation relating to Business Payments and the European Business Wallet; presentation of WE BUILD use cases; documentation of the PA4 use case “Trusted eReceipts for B2B Payments”

Dates of elements examined: March to September 2026

Used in: Chapter 5

Established elements: experimentation within WE BUILD with B2B chains combining business identity, EUDI Wallet, European Business Wallet, opening or use of a bank account, IBAN attestation, payment and issuance of an electronic receipt; presence, within the same programme, of use cases relating to business payments,

eInvoicing and cross-border tax declarations; demonstration by a consortium participant of a PA4 use case in which an account or card payment authenticated using the EUDI Wallet results in the issuance of a verifiable eReceipt to the purchasing company's European Business Wallet; the receipt includes, in particular, purchase lines, amounts, VAT information and payment reference; connection of the receipt to an accounting system and demonstration of VAT reconciliation with a demonstration tax service.

Methodological precaution: the general chain business identity → account/IBAN → payment → eReceipt is documented by the WE BUILD consortium. The details of the PA4 use case through to automated VAT reconciliation are documented by iGrant.io, a participant that developed the pilot with other WE BUILD partners. This second level constitutes evidence of technical experimentation by a project participant and must not be presented as evidence of the operational deployment of such a system by an actual national tax administration.

Links:

- https://www.webuildconsortium.eu/news/we-build-joins-global-digital-collaboration-2026-discover-our-sessions
- https://igrant.io/articles/trusted-ereceipts-for-b2b-payments-taking-eudi-wallet-payments-from-the-consumer-to-the-company

---

S35 CEN/TS 16931-8:2024 — eReceipts, DPP identifier and environmental product information

Organization: European Committee for Standardization (CEN)

Document: CEN/TS 16931-8:2024 — Electronic invoicing — Part 8: Semantic data model of the elements of an e-receipt

Date: 2024

Used in: Chapter 5

Established elements: European semantic model for electronic receipts; description of a process in which the buyer selects a payment method, makes or initiates the payment and then receives an eReceipt generated by the seller; possibility of including specific product-related information in certain environments; explicit reference to the Digital Product Passport for the relevant product categories; use of a DPP identifier enabling the receipt to be linked to verified product information; inclusion among this information of material durability as well as social and environmental impacts related to the materials, production, use and end-of-life of the product.

Methodological precaution: the existence of a field or mechanism enabling an eReceipt to be linked to the DPP demonstrates the standardized possibility of establishing this connection. It does not demonstrate that every eReceipt will contain a DPP identifier, that the corresponding environmental data will be systematically retrieved, or that such data will be used by a payment system.

Link:

- https://norminfo.afnor.org/norme/cents-16931-82024/facturation-electronique-partie-8-modele-semantique-de-donnees-des-elements-dun-recu-electronique-ou-dune-facture/307488

S36 General Data Protection Regulation — principles applicable to processing

Organization: European Union

Document: Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 — General Data Protection Regulation (GDPR)

Used in: Chapter 6

Established elements: principles of lawfulness, fairness and transparency; purpose limitation; data minimization; legal basis for processing; safeguards applicable to processing carried out in the performance of a task in the public interest; rules governing automated individual decision-making and profiling; obligation to collect data for specified, explicit and legitimate purposes and not to further process them in a manner incompatible with those purposes; obligation to limit data to what is necessary in relation to the purposes pursued.

Link:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

S37 CNIL — Integration of electronic invoicing data into the CFVR algorithmic processing system

Organization: French Data Protection Authority (CNIL)

Document: Deliberation No. 2026-068 of June 18, 2026 issuing an opinion on a draft order amending the automated anti-fraud processing system “fraud targeting and query enhancement” (CFVR)

Publication: July 24, 2026

Used in: Chapter 6

Established elements: integration of data derived from electronic invoicing into the categories of personal data used by CFVR; substantial increase in the volume of data processed, estimated by the DGFiP at approximately 2 to 3 billion electronic invoices per year; feeding of the DGFiP's secure data platform; possible use of these data to identify anomalies and businesses presenting certain tax risks; possible cross-referencing of query results with other data processed by the system; intention, ultimately, for all data processed by CFVR to feed this platform; use of algorithmic and machine-learning methods, including unsupervised learning; identification by the CNIL of risks of bias and amplification of such biases; need to maintain human analysis prior to the opening of a tax audit; requirements relating to data minimization, access, retention periods, information provided to individuals and data security.

Methodological precaution: this opinion does not conclude that the processing is unlawful. It does, however, confirm that data derived from electronic invoicing is effectively intended to feed a tax analysis and targeting infrastructure using, in particular, algorithmic processing.

Link:

- https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000054466005

S38 Decree on the generalization of electronic invoicing — consideration of the GDPR and CNIL opinion

Organization: French Republic

Document: Decree No. 2022-1299 of October 7, 2022 relating to the generalization of electronic invoicing in transactions between persons subject to VAT and to the transmission of transaction data

Date: October 7, 2022

Used in: Chapter 6

Established elements: explicit reference to the General Data Protection Regulation in the decree organizing the reform; adoption of the decree following the opinion of the French Data Protection Authority of June 23, 2022; integration of data protection considerations into the regulatory process. However, this consultation and reference do not make it possible to conclude that any subsequent development of processing activities or any new reuse of the data would automatically be compatible with the GDPR.

Link:

- https://www.legifrance.gouv.fr/loda/id/JORFTEXT000046383394

S39 Proportionality review of data processing by public authorities

Organizations: Court of Justice of the European Union; French Constitutional Council

Documents: case law of the Court of Justice of the European Union relating to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union; case law of the French Constitutional Council relating to the review of the necessity and proportionality of personal data collection and processing systems

Used in: Chapter 6

Established elements: the protection of personal data and privacy does not prevent public authorities from implementing processing activities pursuing an objective of general interest; such processing remains subject to a review of necessity and proportionality; limitations on data protection must be restricted to what is strictly necessary and the objective of general interest must be balanced against the seriousness of the interference with the rights concerned; constitutional review takes into account, in particular, the purposes pursued, the nature and extent of the data collected and the safeguards governing their use.

Official references:

- CJEU: case law relating to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.
- https://curia.europa.eu/juris/liste.jsf?num=C-175/20
- French Constitutional Council: review of the necessity and proportionality of personal data collection and processing systems.
- https://www.conseil-constitutionnel.fr/decision/2012/2012652DC.htm

---

S40 European Union — CE-RISE: DPP, reuse, repair and recycling

Organization: European Commission — CORDIS / Horizon Europe

Project: Circular Economy Resource Information System (CE-RISE)

Used in: Chapter 3

Established elements: development and experimentation of an information system intended to promote the reuse, recovery and recycling of materials; definition of criteria for assessing possibilities for reuse, repair, refurbishment and recycling; integration of this information and product composition into the Digital Product Passport to ensure material traceability throughout the value chain; integration of the DPP with information relating to the environmental footprint of products; experimentation with the system across four use cases.

Link:

- https://cordis.europa.eu/project/id/101092281

S41 European Union — QUASAR: DPP and end-of-life traceability

Organization: European Commission — CORDIS / Horizon Europe

Project: QUASAR — 70%plus eco-efficiency gains in the PV EOL supply chain by closed loop systems with enhanced recycling rates, systematic collection and management utilising digital twins

Used in: Chapter 3

Established elements: use of a Digital Product Passport to contribute to the tracking of photovoltaic modules at end-of-life; use of the DPP and assessment methods to guide decisions between reuse, repair and recycling; experimentation with repair and second-life solutions; use of digital traceability tools within a circular value chain.

Link:

- https://cordis.europa.eu/project/id/101122298

S42 European Commission — Launch of the Digital Product Passport Registry

Organization: European Commission — Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

Document: The Digital Product Passport Registry is now live

Date: July 20, 2026

Used in: Chapter 3

Established elements: launch of the European Digital Product Passport Registry on July 20, 2026; simultaneous launch of a test environment; possibility of registering passports through a secure interface or an API; storage of unique identifiers and registration metadata; availability of a semantic repository and documented APIs; presence of verification and logging mechanisms; access to technical documentation and resources intended to support implementation of the system.

Link:

- https://single-market-economy.ec.europa.eu/news/digital-product-passport-registry-now-live-2026-07-20_en

---

S43 General Data Protection Regulation — principles, legal bases and safeguards applicable to processing

Organization: European Union

Document: Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 — General Data Protection Regulation (GDPR)

Used in: Chapter 6

Established elements:

- Article 5 imposes, in particular, the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability of the controller;
- personal data must be collected for specified, explicit and legitimate purposes and not be further reused in a manner incompatible with those purposes;
- the data processed must be adequate, relevant and limited to what is necessary in relation to the purposes pursued;
- Article 6 provides several legal bases allowing processing to be lawful, including compliance with a legal obligation and the performance of a task carried out in the public interest or in the exercise of official authority;
- where processing based on a legal obligation or a task carried out in the public interest is based on Union law or the law of a Member State, that law must determine the purpose of the processing or govern its exercise in accordance with the GDPR;
- Article 22 governs decisions based solely on automated processing, including profiling, where they produce legal effects or similarly significantly affect an individual;
- Article 23 allows Union or national law to restrict certain rights and obligations provided for by the GDPR, including for certain objectives of public interest, but requires that such a restriction respect the essence of fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society;
- Article 25 requires data protection by design and by default and provides, in particular, that only data necessary for each specific purpose be processed by default, this requirement applying notably to the amount of data, the extent of processing, the period of storage and accessibility;
- Article 32 requires technical and organizational measures appropriate to the level of risk presented by the processing;
- Article 35 requires a data protection impact assessment where a type of processing, in particular using new technologies and taking into account its nature, scope, context and purposes, is likely to result in a high risk to the rights and freedoms of natural persons.

Relevance to the investigation: The existence of a legal basis allowing data collection does not, in itself, constitute a general authorization permitting any reuse, any cross-referencing or any extension of purpose.

Conversely, the GDPR does not prohibit in principle processing carried out by a public administration without consent where such processing is based on another legal basis provided for in Article 6.

The legal analysis must therefore examine each processing activity concerned, its purpose, its legal basis, the data actually necessary, their retention period, their recipients, their access arrangements and the applicable safeguards.

Link:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

S44 CJEU and French Constitutional Council — necessity, minimization and proportionality of data processing

Organizations: Court of Justice of the European Union / French Constitutional Council

Used in: Chapter 6

Established elements: The Court of Justice of the European Union recalls that any processing of personal data must comply with the principles set out in Article 5 of the GDPR and satisfy one of the conditions for lawfulness laid down in Article 6.

It also recalls that the purposes of processing must be specified, explicit and legitimate and that the controller must be able to demonstrate compliance with these principles.

In its case law relating to Articles 5 and 6 of the GDPR, the Court links the principle of data minimization to the proportionality assessment. Assessing the necessity of processing may, in particular, require determining whether the objective pursued can be achieved by equally effective means that are less intrusive with regard to the protection of personal data.

In Case C-175/20, Valsts ieņēmumu dienests, specifically concerning data processing for tax purposes, the Court recalls the application of the principles of purpose limitation and data minimization to requests for and processing of data carried out by a tax administration.

In Case C-268/21, Norra Stockholm Bygg, the Court recalls that the principle of data minimization gives expression to the principle of proportionality and that the competent authority must, in particular, examine whether the objective pursued can be achieved by means that are less intrusive with regard to the protection of personal data.

The French Constitutional Council, for its part, considers that the right to respect for private life requires the collection, recording, storage, consultation and communication of personal data to be justified by a reason of public interest and implemented in a manner that is adequate and proportionate to that objective.

Relevance to the investigation: The existence of an objective of public interest, including the fight against tax fraud, is therefore not sufficient to make all possible methods of collecting, retaining, cross-referencing or using data automatically proportionate.

The legal review may concern, in particular, the scope of the data processed, their necessity in relation to the purpose pursued, their retention period, their recipients, the cross-referencing performed and the possible existence of less intrusive means capable of effectively achieving the same objective.

Links:

- https://curia.europa.eu/juris/liste.jsf?num=C-175/20

- https://curia.europa.eu/juris/liste.jsf?num=C-268/21

S45 France — Integration of electronic invoicing data into the CFVR processing system

Organization: French Republic — Ministry of the Economy and Finance

Document: Order of July 10, 2026 amending the Order of February 21, 2014 establishing an automated anti-fraud processing system by the Directorate General of Public Finances known as “fraud targeting and query enhancement” (CFVR)

Used in: Chapter 6

Established elements:

- amendment of the regulatory framework applicable to the CFVR processing system;
- addition of data from electronic invoicing to the data that may be processed within the system;
- evolution of the processing system in connection with data exchanges between public administrations and the organization of the data analysis system;
- regulatory incorporation of electronic invoicing data into the DGFiP's automated anti-fraud processing system.

Relevance to the investigation: The integration of electronic invoicing data into CFVR is no longer merely described in a draft submitted to the CNIL for its opinion.

It is now provided for by a regulatory text adopted in July 2026.

The lawfulness of the existence of this processing system does not, however, remove the need to examine separately the safeguards applicable to its practical implementation: purposes, categories of data, retention, cross-referencing, access, security, minimization, proportionality and algorithmic processing.

Link:

- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054450882

S46 GDPR — further processing and compatibility of purposes

Organization: European Union

Document: Regulation (EU) 2016/679 — Article 6(4)

Used in: Chapter 6

Established elements: The GDPR does not prohibit in principle all further processing pursuing a purpose different from that which justified the initial collection.

Where the further processing is based neither on the data subject's consent nor on Union or Member State law constituting a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller must determine whether the new purpose is compatible with the initial purpose.

Article 6(4) provides, in particular, that the following must be taken into account:

- any link between the initial purposes and the purpose of the intended further processing;
- the context in which the data were collected, in particular the relationship between the data subjects and the controller;
- the nature of the personal data concerned;
- the possible consequences of the further processing for the data subjects;
- the existence of appropriate safeguards, including encryption or pseudonymization.

Relevance to the investigation: A new use of personal data is therefore not automatically prohibited solely because it differs from the initial use.

Two situations must notably be distinguished:

1. the further processing is based on a purpose compatible with the initial purpose, following application of the compatibility test provided for by the GDPR;
2. the further processing is based on Union or Member State law meeting the conditions laid down by the GDPR.

The principle of purpose limitation therefore constitutes a genuine legal safeguard, but it does not constitute an absolute prohibition on any evolution of uses.

Link:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

S47 GDPR — restrictions for tax objectives and supervisory tasks

Organizations: European Union / French Republic

Documents: Regulation (EU) 2016/679, Article 23; Order of July 10, 2026 amending the CFVR processing system

Used in: Chapter 6

Established elements: Article 23 of the GDPR allows Union or Member State law to restrict, by way of a legislative measure and under certain conditions, the scope of several obligations and rights provided for by the GDPR.

Such a restriction must:

- respect the essence of fundamental rights and freedoms;
- constitute a necessary and proportionate measure in a democratic society;
- pursue one of the objectives provided for in Article 23.

These objectives include, in point (e):

- important objectives of general public interest;
- an important economic or financial interest of the Union or of a Member State;
- monetary, budgetary and taxation matters;
- social security.

Point (h) also provides for:

- a monitoring, inspection or regulatory function connected to the exercise of official authority in the areas concerned.

The Order of July 10, 2026 amending CFVR explicitly refers to points (e) and (h) of Article 23(1) of the GDPR in the provisions relating to the processing system.

Relevance to the investigation: The GDPR therefore itself provides a degree of legal latitude allowing the legislature to adjust or restrict certain rights and obligations where justified by a tax objective or a supervisory task.

This latitude is not, however, general or unconditional.

It remains subject, in particular, to respect for the essence of fundamental rights and to a review of necessity and proportionality.

The legal framework applicable to CFVR explicitly relies on this possibility.

Links:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679
- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054450882

S48 GDPR — security of processing, impact assessment and risk reassessment

Organization: European Union

Document: Regulation (EU) 2016/679 — Articles 32 and 35

Used in: Chapter 6

Established elements: Article 32 of the GDPR requires the controller and the processor to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

The assessment must notably take into account:

- the state of the art;
- the nature of the processing;
- its scope;
- its context;
- its purposes;
- the likelihood and severity of the risks to the rights and freedoms of individuals.

Possible measures include, in particular:

- pseudonymization and encryption;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems;
- the ability to restore the availability of and access to data following an incident;
- regular procedures for testing, assessing and evaluating the effectiveness of security measures.

The assessment must notably take into account the risks of destruction, loss, alteration, unauthorized disclosure of or unauthorized access to data.

Article 35 provides that a data protection impact assessment must be carried out where processing is likely to result in a high risk to the rights and freedoms of natural persons, taking into account, in particular, its nature, scope, context, purposes and the use of new technologies.

Article 35 also provides that a review must be carried out, where necessary, to assess whether the processing remains in accordance with the data protection impact assessment, at least when there is a change in the risk represented by the processing operations.

Relevance to the investigation: The security of processing is not a fixed assessment carried out only once when the processing system is created.

A substantial increase in volumes, the addition of new sources, new cross-referencing, new parties with access or new infrastructures may alter the risk presented by the processing and make a reassessment of the safeguards implemented relevant.

Link:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

S49 CNIL — large-scale processing, data matching and high-risk criteria

Organization: French Data Protection Authority (CNIL)

Document: CNIL documentation relating to Data Protection Impact Assessments (DPIAs)

Used in: Chapter 6

Established elements: The CNIL recalls that a data protection impact assessment is mandatory where processing is likely to result in a high risk to the rights and freedoms of the individuals concerned.

The criteria used to assess the existence of a high risk include, in particular:

- evaluation or scoring, including profiling;
- automated decision-making producing legal effects or similarly significant effects;
- systematic monitoring;
- processing of sensitive or highly personal data;
- processing of personal data on a large scale;
- matching or combining datasets;
- processing of data concerning vulnerable individuals;
- innovative use of technologies or organizational solutions;
- exclusion from the benefit of a right, service or contract.

The CNIL indicates that where at least two of these criteria are present, a DPIA must in principle be carried out, subject to a concrete assessment of the risk.

The DPIA must notably include:

- a description of the processing operations;

- an assessment of their necessity and proportionality;
- an assessment of the risks to individuals;
- the measures envisaged to address those risks and ensure data security.

Relevance to the investigation: Large-scale processing and the matching of datasets are not legally neutral when assessing risks.

Where an infrastructure combines several of these criteria, the existence, scope and updating of the impact assessment become important elements in assessing the compliance of the processing.

Link:

- https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

---

S50 CNIL — state of the art in personal data security

Organization: French Data Protection Authority (CNIL)

Document: Personal Data Security Guide — 2024 edition

Used in: Chapter 6

Established elements: The CNIL recalls that Article 32 of the GDPR requires a level of security appropriate to the risk and presents its security guide as a reference used to assess the security of personal data processing.

The recommended measures include, in particular:

- the use of individual user accounts;
- the limitation and management of access rights;
- user authentication;
- securing servers and networks;
- encryption of data exchanges;
- logging of operations;
- risk analysis;
- management of incidents and data breaches;
- backup and recovery capabilities;
- maintaining a business continuity and disaster recovery plan;
- regular reviews of the effectiveness of security measures.

The CNIL also recommends regularly reviewing risk analyses to take into account changes in the processing and in threats.

Relevance to the investigation: The security obligation is not limited to preventing direct access to a database.

It requires an organized and ongoing defense covering, in particular, identities, access rights, exchanges, logging, incident detection, resilience and evolving threats.

Link:

- https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles

S51 CJEU — SCHUFA: an automated score may itself constitute an automated decision when it plays a determining role

Organization: Court of Justice of the European Union

Document: Judgment of December 7, 2023, SCHUFA Holding (Scoring), C-634/21

Used in: Chapter 6

Established elements: The Court of Justice interpreted Article 22(1) of the GDPR concerning the automated establishment of a score subsequently used by a third party to make a decision concerning an individual.

The Court held that the automated establishment of a probability value based on personal data may itself constitute an "automated individual decision" within the meaning of Article 22 where the decision subsequently taken by a third party depends to a determining extent on that value.

This case law shows that the formal existence of human intervention or of a subsequent decision taken by a third party is not necessarily sufficient to exclude the application of Article 22.

The actual influence of the automated result on the final decision must be examined.

Relevance to the investigation: The presence of a human agent at the end of an algorithmic chain does not, in itself, make it possible to conclude that the final decision necessarily falls outside the regime applicable to automated decisions.

It is necessary, in particular, to determine whether the agent has a genuine ability to analyze and challenge the result produced by the algorithm or whether that result plays, in practice, a determining role in the final decision.

This case law does not establish that CFVR currently falls within the scope of Article 22.

It does, however, provide a legal criterion for examining the actual influence of alerts, scores, classifications or lists produced by algorithmic processing on a subsequent decision.

Link:

- https://curia.europa.eu/juris/liste.jsf?num=C-634/21

S52 CJEU — right to a comprehensible explanation of the logic of an automated decision

Organization: Court of Justice of the European Union

Document: Judgment of February 27, 2025, Dun & Bradstreet Austria, C-203/22

Used in: Chapter 6

Established elements: The Court of Justice clarifies the scope of the right of access to "meaningful information about the logic involved" provided for by Article 15(1)(h) of the GDPR in the context of automated decision-making.

The data subject must be able to obtain relevant information enabling them to understand the procedure and principles actually applied to their personal data in order to obtain the automated result.

The Court specifies that the complexity of the operations carried out cannot exempt the controller from its obligation to provide a comprehensible explanation.

The mere disclosure of a complex mathematical formula or, conversely, an exhaustive and technical description of all stages of the algorithm does not necessarily constitute a sufficiently intelligible explanation.

In the context of profiling, the Court indicates, in particular, that an explanation may make it possible to understand the extent to which a variation in the data used would have led to a different result.

Relevance to the investigation: Where processing falls within the regime governing automated decisions under the GDPR, transparency cannot be satisfied merely by stating that an algorithm or model is used.

The data subject must be able to understand in an intelligible manner how their data contributed to the result concerning them.

This case law becomes particularly relevant for systems using complex models, including where their internal operation makes explanation more difficult.

Link:

- https://curia.europa.eu/juris/liste.jsf?num=C-203/22

S53 CJEU — processing of data for tax purposes: necessity, minimization and prohibition of general and indiscriminate collection

Organization: Court of Justice of the European Union

Document: Judgment of February 24, 2022, Valsts ieņēmumu dienests (Processing of personal data for tax purposes), C-175/20

Used in: Chapter 6

Established elements: The Court of Justice directly examines the application of the GDPR to the collection of personal data carried out by a tax administration in the performance of its tasks.

It holds that a tax administration remains subject to the principles of Article 5 of the GDPR when it collects a significant amount of personal data from an economic operator.

The Court recalls that derogations from and limitations on the principle of protection of personal data must apply only in so far as is strictly necessary.

It follows that the controller, including when acting in the performance of a task carried out in the public interest:

- may not collect personal data in a general and indiscriminate manner;
- must refrain from collecting data that are not strictly necessary for the purposes pursued;
- must seek to minimize as much as possible the amount of data collected;
- must limit the collection period to what is strictly necessary for the objective of public interest pursued.

The Court also specifies that the controller must be able to demonstrate compliance with these principles.

Finally, it indicates that the legislation serving as the basis for the processing must lay down clear and precise rules governing the scope and application of the measure, as well as minimum safeguards to protect individuals against the risk of abuse.

Relevance to the investigation: The existence of a tax-related task carried out in the public interest is therefore not sufficient to justify any amount of data or any duration of processing.

The administration must be able to justify the necessity of the data in relation to the specific purposes pursued and demonstrate the minimization of the processing.

This case law provides a particularly relevant criterion for examining the large-scale integration of data from electronic invoicing and their cross-referencing with other sources within CFVR.

Link:

- https://curia.europa.eu/juris/liste.jsf?num=C-175/20

S54 French Data Protection Act — restrictions of rights in tax matters and exercise through the CNIL

Organization: French Republic

Document: Law No. 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties — Articles 52 and 118

Used in: Chapter 6

Established elements: For processing carried out by public administrations or persons entrusted with a public service mission responsible for auditing or collecting taxes, Article 52 allows the rights of access, rectification and erasure to be exercised in accordance with the specific procedure provided for in Article 118 where the act establishing the processing provides for such restrictions.

Under this procedure, the request is submitted to the CNIL.

The Commission appoints a member who belongs or has belonged to the Conseil d'État, the Court of Cassation or the Court of Auditors to carry out the necessary investigations and, where necessary, arrange for the appropriate modifications to be made.

The CNIL informs the individual that the necessary checks have been carried out and of their right to seek judicial remedy.

Where the Commission finds, in agreement with the controller, that disclosure of the data does not undermine the purposes protected by the system, certain information may be communicated to the individual.

Relevance to the investigation: French law therefore provides that, in tax matters, certain rights granted to individuals may be restricted in order not to compromise the purposes of the processing.

These restrictions do not eliminate all oversight: a specific procedure for exercising rights through the CNIL and a judicial remedy are provided for.

This architecture nevertheless creates an important distinction between the legal existence of a right and the amount of information that the data subject can actually obtain directly about the processing to which they are subject.

Link:

- https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

S55 eIDAS 2 Regulation — European Digital Identity Wallet and safeguards for data separation

Organization: European Union

Document: Regulation (EU) 2024/1183 of the European Parliament and of the Council of April 11, 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

Used in: Chapter 6

Established elements: The European Digital Identity Wallet must enable the user to request, obtain, select, combine, store, delete, share and present person identification data and electronic attestations of attributes.

The Regulation requires, in particular:

- user control over the data presented;
- selective disclosure of attributes;
- the possibility of using pseudonyms where legal identification is not required;
- a history allowing the user to view the relying parties with which they have established a connection and, where applicable, the data exchanged;
- identification and authentication of relying parties;
- prior registration of the nature of the data that a relying party intends to request;
- prohibition on that party requesting data other than those declared;
- mechanisms allowing suspicious or potentially unlawful requests to be reported to data protection authorities.

The Regulation also provides for an “unobservability” safeguard: the wallet provider must not collect information about its use that is not necessary or have general visibility into the user's transactions.

The provider must not combine identification data or other personal data linked to the wallet with data from other services it provides or from third-party services where such data are not necessary for the wallet service, unless expressly requested by the user.

Providers of electronic attestations of attributes are also subject to data separation obligations.

Finally, access to public or private services must not be restricted or made disadvantageous solely because an individual does not use the European Digital Identity Wallet. Alternative means of identification and authentication must remain available.

Relevance to the investigation: The European digital identity framework therefore expressly provides for several safeguards intended to prevent the wallet from becoming, by itself, a general tool for observing and centralizing its user's activities.

However, the wallet is also designed to present, under the user's control, multiple attestations and attributes to relying parties and to interact with public and private services.

Protection therefore relies largely on control over purposes, access, attribute requests, the user's consent or request, and separation between services.

Link:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1183

S56 ESPR Regulation — Digital Product Passport, interoperability and protection of customer data

Organization: European Union

Document: Regulation (EU) 2024/1781 of the European Parliament and of the Council of June 13, 2024 establishing a framework for the setting of ecodesign requirements for sustainable products

Used in: Chapter 6

Established elements: The Regulation establishes the framework for the Digital Product Passport.

The DPP is associated with a unique product identifier and its data must, in particular, be structured, machine-readable, searchable and transferable through an open interoperable data exchange network.

The system is designed to improve product traceability throughout the value chain.

Data access rights must be defined according to the categories of actors and product groups concerned.

The Regulation explicitly provides that personal data relating to customers must not be stored in the Digital Product Passport without their explicit consent in accordance with the GDPR.

The DPP must be able to operate at model, batch or item level depending on the requirements applicable to the product group.

The system is designed as a decentralized data system, while the Commission must maintain a registry of unique identifiers associated with products placed on the market or put into service.

Competent authorities have access intended, in particular, for compliance monitoring.

Relevance to the investigation: The DPP is therefore designed as an interoperable infrastructure for data relating to the product and its life cycle, but it includes a legally important separation between product information and personal data relating to the customer.

The Regulation does not, by itself, create an “individual environmental passport” for the consumer.

The presence of a unique identifier at product or item level does not mean that this identifier is legally linked to the identity of its purchaser.

Such an association would have to result from another processing operation with its own purpose and its own legal basis.

Link:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1781

S57 Proposal for a Regulation on the digital euro — identity, privacy, conditional payments and prohibition of programmable money

Organizations: European Commission / European Central Bank

Main document: COM(2023) 369 final — Proposal for a Regulation on the establishment of the digital euro

Status as of September 3, 2026: legislative procedure ongoing; Regulation not yet adopted.

Used in: Chapter 6

Established elements:

The proposal establishes an explicit distinction between:

- programmable money;
- and conditional payments.

Programmable money, understood as money whose units would intrinsically include limitations on full fungibility, must be prohibited.

The digital euro must therefore not be intrinsically limited to certain goods, certain services, certain periods or certain beneficiaries.

However, the proposal allows conditional payments.

A conditional transaction is a transaction whose instruction is triggered automatically when predefined conditions agreed between the payer and the payee are met.

The proposal allows the ECB to provide rules, standards and technical functionalities necessary for the execution of such transactions, including the reservation of funds.

The proposal also provides for the digital euro's front-end services to be interoperable with or integrated into European Digital Identity Wallets.

It provides several safeguards relating to privacy and data protection.

For offline payments, the proposed architecture aims to provide a level of privacy comparable to that of cash.

For online payments, data transmitted to the ECB, national central banks or providers of support services must be subject to measures preventing the direct identification of individual users under the conditions laid down in the text.

The proposal also provides for processing necessary, in particular, for the application of holding limits, execution of payments, fraud prevention, compliance with anti-money laundering and counter-terrorist financing obligations and certain tax obligations.

Relevance to the investigation: The prohibition of programmable money constitutes a substantive safeguard: the digital euro must not become money whose value or usability intrinsically depends on the nature of the goods or services purchased.

This prohibition must not, however, be confused with a general prohibition of conditional payments.

On the contrary, the proposed framework explicitly provides for an infrastructure capable of executing payments triggered automatically when agreed conditions are met.

It also provides for a legal and technical interface between the digital euro and the European Digital Identity Wallet.

These capabilities do not establish that environmental data, a DPP or an identity attribute is intended to condition a payment.

They do, however, establish that some of the technical interfaces required for conditional payment services and the use of a digital identity are explicitly envisaged in the proposed architecture.

Links:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52023PC0369
- https://eur-lex.europa.eu/legal-content/FR/HIS/?uri=CELEX:52023PC0369

S58 Successive evolution of the legal scope of the CFVR processing system since 2014

Organization: Directorate General of Public Finances / Légifrance

Documents:

- Order of February 21, 2014 establishing the “fraud targeting and query enhancement” (CFVR) processing system;
- Order of August 28, 2017 amending the CFVR processing system;
- Order of March 8, 2021 amending the CFVR processing system;
- Order of October 21, 2024 amending the CFVR processing system;
- Order of July 10, 2026 amending the CFVR processing system.

Used in: Chapter 6

Established elements: The CFVR processing system has not remained legally unchanged since its creation in 2014.

Its regulatory framework has undergone several successive amendments concerning, in particular:

- the categories of data subjects;
- the categories of data processed;
- the sources supplying the processing system;
- the purposes or methods of use;
- the recipients;
- exchanges with other processing systems or public administrations;
- retention periods;

- the procedures for exercising certain rights.

In 2017, the processing system was notably extended, on an experimental basis, to fraud involving individuals and was authorized to use data concerning individuals with no connection to a business.

In 2021, its interaction with processing systems enabling the collection and use of certain data made public on online platforms was incorporated into its framework.

A further amendment was made in 2024.

In July 2026, the framework was amended again, notably to integrate data from electronic invoicing, new data sources and certain transmissions to social security bodies.

Relevance to the investigation: The history of CFVR demonstrates that a public processing system can retain its institutional continuity while its scope in terms of data, data subjects, sources, recipients and uses evolves through successive legal amendments.

This evolution is not in itself irregular: each amendment remains subject to the applicable legal framework.

It nevertheless shows that a safeguard based on the current legal scope of an infrastructure does not constitute a guarantee that this scope will remain unchanged.

Links:

- 2014 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028684963
- 2017 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036012682
- 2021 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043426791
- 2024 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000050771533
- 2026 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054450882