

E-evidence package

what changes for digital
service providers?

```
class FilterNode extends Node {  
  constructor() {  
    this.type = 'LPF filter';  
    this.input = new InputSocket('audio_in');  
    this.output = new OutputSocket('audio_out');  
  }  
  
  process(audio) {  
    // Low-pass filter implementation  
    // ...  
  }  
}
```

Contents

1. Key provisions	→ Read more
1.1 What is the e-Evidence Package?	→ Read more
2. Background of the regime	→ Read more
2.1 What makes up the e-Evidence Package?	→ Read more
2.2 How do the new rules differ from the previous ones?	→ Read more
2.3 Why is the legislation particularly important for digital companies?	→ Read more
3. The new rules: how does the new EU mechanism for obtaining digital evidence work?	→ Read more
3.1 Which categories of data can be requested?	→ Read more
3.2 Which service providers might be covered?	→ Read more
3.3 Who is responsible for receiving and carrying out orders?	→ Read more
3.4 Can a company refuse to comply or object?	→ Read more
4. Implementation in Portugal	→ Read more
4.1 Which authorities are responsible?	→ Read more
4.2 What must be operational by February 2027?	→ Read more
5. Consequences of non-compliance	→ Read more
5.1 The amount of the fine	→ Read more
5.2 How to avoid non-compliance	→ Read more
6. What should you do now?	→ Read more

Since 18 August 2026, a judicial authority in any EU Member State has been able to issue a data production or preservation order to any digital service provider without having to use the traditional channels of judicial cooperation. In Portugal, Law 55/2026 supplements this regime, imposing fines of up to 2% of worldwide turnover. The deadline for appointing the recipient of orders is 25 February 2027.

1. Key provisions

- Already in force: Regulation (EU) 2023/1543 in force since 18 August 2026.
- Short time limits: 10 days to disclose data and 8 hours in urgent cases. Data must be preserved for 60 days, extendable by 30 days.
- Extra-territorial scope: the criterion for application is the provision of services within the EU, with a ‘substantial connection’ to Member State. This does not depend on the location of the registered office or the servers.
- Mandatory recipient: it is necessary to designate an establishment or appoint a legal representative, and to communicate this by 27 February 2027.
- Heavy fines: liability is joint and several. Fines for very serious offences can be up to 2% of worldwide turnover and a mandatory financial penalty of up to €3,000,000 can be applied.

A judicial authority in any EU Member State is able to issue a data production or preservation order to any digital service provider without having to use the traditional channels of judicial cooperation.

1.1. WHAT IS THE E-EVIDENCE PACKAGE?

The increasing digitalisation of the economy means that electronic evidence is now a crucial part of criminal investigations. However, data relevant to an investigation is often stored by service providers located in different EU Member States or outside the EU altogether. This complicates and lengthens the process of obtaining it.

Against this backdrop, the European Union adopted the **e-Evidence Package**, which introduces a new mechanism for the cross-border collection and preservation of electronic evidence in criminal proceedings. The aim is to enable faster and more effective cooperation between the relevant judicial authorities and service providers. This will be achieved by issuing orders directly to the designated establishment or the service provider’s legal representative.

Although the new regime is intended for criminal investigations, it will directly impact on businesses that store, process or make data available electronically. This may be particularly relevant for providers of electronic communications services, cloud computing, software as a service (SaaS), digital platforms, marketplaces, social media and hosting services.

Whether the regime applies does not necessarily depend on the location of the company’s registered office or servers. Rather, it depends on how services are made available within the European Union and whether there is a substantial connection to one or more Member States. For this reason, many organisations may be covered without realising it.

2. Background of the regime

2.1. WHAT MAKES UP THE E-EVIDENCE PACKAGE?

The e-Evidence Package is based on three complementary EU instruments:

- **Regulation (EU) 2023/1543**, which has applied since 18 August 2026 and created European Production and Preservation Orders for electronic evidence.
- **Directive (EU) 2023/1544**, which harmonised the obligation to indicate a designated establishment or legal representative to receive and carry out these orders. The deadline for transposition is 18 February 2026.
- **Commission Implementing Regulation (EU) 2025/1550**, which establishes the technical rules for electronic communications through the e-CODEX infrastructure.

In Portugal, Directive (EU) 2023/1544 was transposed into national law by **Law 55/2026 of 20 August**, which came into force on 25 August 2026. Law 55/2026 also sets out penalties for the Directive and Regulation, and amends Laws 144/99 (International Judicial Cooperation in Criminal Matters) and 109/2009 (the Cybercrime Law).

2.2. HOW DO THE NEW RULES DIFFER FROM THE PREVIOUS ONES?

Until now, accessing data held by service providers located in another EU Member State or outside the EU has usually depended on traditional international judicial cooperation mechanisms. This process involved several different authorities and could take weeks or even months.

The new regime addresses the increasing demand for the rapid collection of digital evidence. In certain circumstances, it enables a judicial authority in one Member State to issue an order directly to a service provider or representative in another Member State.

Despite its importance, the e-Evidence Package complements, rather than replaces, traditional instruments of international judicial cooperation.

2.3. WHY IS THE LEGISLATION PARTICULARLY IMPORTANT FOR DIGITAL COMPANIES?

Because it transforms the ability to respond to requests from the authorities into a regulated obligation that is subject to specific organisational, operational, and legal requirements.

Companies potentially covered by this legislation must now ensure that they have a formal point of contact for receiving orders, as well as internal validation and response mechanisms, data retention procedures, and the capacity to meet particularly demanding deadlines, which, in certain situations, may be measured in hours.

3. The new rules: how does the new EU mechanism for obtaining digital evidence work?

Thanks to Regulation (EU) 2023/1543, certain judicial authorities in a Member State can now request the production or preservation of relevant data from service providers covered by the Regulation directly, without the need for an intermediary. This significantly reduces reliance on traditional mechanisms of international judicial cooperation.

The new system is based on two main instruments in particular:

- The **European Production Order allows data stored by the service provider to be requested. This is** usually within 10 days, or within a maximum of 8 hours in an emergency.
- The **European Preservation Order is precautionary in nature. It enables the preservation of identified data** for up to 60 days, with the option of an additional 30 days or until the data is produced, if a subsequent request is confirmed. This prevents the alteration or deletion of the data until it is requested by the competent authorities.

3.1. WHICH CATEGORIES OF DATA CAN BE REQUESTED?

It is important to distinguish between the four categories of data that can be requested. These are organised in ascending order of intrusiveness, with different requirements for the issuance of a warrant for each category:

- Subscriber data
- User identification data
- Traffic data
- Content data

The category of data in question influences the conditions under which an order may be issued, the level of judicial oversight required, and the applicable safeguards.

3.2. WHICH SERVICE PROVIDERS MIGHT BE COVERED?

The scope of the regime is deliberately broad. It is not limited to large, global technology platforms or traditional electronic communications operators.

The Regulation applies to service providers offering services within the European Union. This includes providers of electronic communications services, internet domain name services, IP numbering services and other services that enable communication between users, or the retention or processing of data on their behalf. The latter is a key component of the service.

The Regulation applies to service providers offering services within the European Union. This includes providers of electronic communications services, internet domain name services, IP numbering services and other services that enable communication between users, or the retention or processing of data on their behalf.

The regime may apply to service providers based outside the European Union if they offer services within the Union and have a significant link to at least one Member State.

Financial services, as well as services in which storage is not an essential component, are excluded. Furthermore, the Directive does not apply to service providers established in a single Member State who offer services exclusively within that state. Additionally, Denmark does not participate in the regime.

Therefore, the assessment must be carried out on a case-by-case basis, as the same organisation may simultaneously provide both covered and non-covered services.

3.3. WHO IS RESPONSIBLE FOR RECEIVING AND CARRYING OUT ORDERS?

One of the cornerstones of the new regime is the identification of a formal recipient responsible for receiving, managing and ensuring compliance with orders issued by the competent authorities.

To this end, service providers offering covered services must appoint a ***designated establishment or legal representative. In both cases, the recipient must be established in a Member State in which the services are offered, and in which enforcement proceedings may be brought against them. The designated establishment or legal representative must have the powers, resources and effective access to information necessary to receive and analyse orders, identify and preserve the requested data, communicate with the competent authorities and invoke grounds of impossibility or non-compliance, where applicable.***

In Portugal, this designation must be made by 25 February 2027. The Directive provided for designation by 18 August 2026. The later Portuguese deadline is due to the delayed transposition of the Directive into national law. If the recipient is designated in another Member State, the law and time limits of that Member State apply.

Meanwhile, Regulation (EU) 2023/1543 has been directly applicable since 18 August 2026. This means that entities covered by the regulation are already subject to orders transmitted in the normal course of business.

In Portugal, this designation must be made by 25 February 2027.

3.4. CAN A COMPANY REFUSE TO COMPLY OR OBJECT?

As a general rule, recipients cannot unilaterally refuse to comply. Receipt of a European Production or Preservation Order always requires the service provider to take action within the applicable time limits. The order must not be disregarded, even if its validity or enforceability is in doubt. In the case of traffic and content data, it should also be noted that the Regulation provides for notification to the executing state authority, which may invoke grounds for refusal.

However, the Regulation provides for situations in which the recipient may request further clarification. It also sets out procedures for informing the issuing authority that the order cannot be executed, providing reasons. Additionally, it establishes specific mechanisms to address conflicts between compliance with the order and obligations imposed by third-country legislation.

This matter is particularly important for multinational groups that are subject to both the e-Evidence rules and other legal frameworks, such as the US Stored Communications Act and the CLOUD Act, as well as restrictions on the disclosure of information imposed by the legal systems of third countries. Negotiations on the EU-US agreement on access to electronic evidence are ongoing and have not yet been finalised. Therefore, if there is any doubt regarding the validity, enforceability or compatibility of an order with other applicable legal obligations, it is advisable to conduct a specialist legal analysis before responding to the issuing authority.

4. Implementation in Portugal

4.1. WHICH AUTHORITIES ARE RESPONSIBLE?

- **ANACOM: the central authority for communications relating to designated establishments and legal representatives.** ANACOM also supervises, initiates proceedings and imposes fines and ancillary penalties.
- **Attorney General's Office: is the central authority for the purposes of the Regulation.**
- **Judicial authorities: issue, validate and enforce orders.**

4.2. WHAT MUST BE OPERATIONAL BY FEBRUARY 2027?

The **25 February 2027** deadline only applies to service providers who were offering services in the European Union on 18 February 2026. This deadline relates to their obligation to designate a place of business or appoint a legal representative, and to notify the competent central authority. The remaining obligations have applied since 18 August 2026.

In practical terms, the organisations concerned must, with immediate effect, ensure at least the following:

- **A formally identified recipient** with the necessary powers and resources to receive and execute orders, without prejudice to the legal deadline applicable to their designation or appointment;
- **An internal procedure for the receipt, validation and processing of orders** with clearly defined responsibilities and decision-making flows.
- **A legal team or specialised verification mechanism** capable of swiftly analysing issues relating to validity, scope, and conflicts of law.

- **An up-to-date inventory of systems, applications, and data categories**, enabling relevant information to be identified and located immediately.
- **Mechanisms for urgently preserving data**, capable of responding to European Preservation Orders within the required timeframes.
- **Periodic tests and internal response exercises**, enabling the effectiveness of implemented procedures to be validated.
- **Technical capability to use applicable communication channels**, including alternative means permitted by the Regulation. When mandatory, there must also be integration with the e-CODEX infrastructure.



5. Consequences of non-compliance

5.1. THE AMOUNT OF THE FINE

For legal persons, fines may amount to 2% of the total worldwide turnover in the previous financial year in the event of failures to retain or transmit data, and 1% in the event of inadequate confidentiality and security measures.

Additionally, failing to comply with obligations under the e-Evidence Package may result in daily penalty payments of up to €3,000,000 for up to 30 days.

In the case of very serious administrative offences, an additional penalty of prohibition from acting as a service provider within the country for a maximum period of two years may also be imposed. Failure to comply with this prohibition constitutes the offence of aggravated disobedience.

The service provider, the designated establishment and the legal representative are jointly and severally liable for compliance with the obligations relating to the provision of services. Consequently, the mere existence of a legal representative or designated establishment does not negate the need for effective coordination between the various entities involved.

5.2. HOW TO AVOID NON-COMPLIANCE

Organisations that are potentially covered by the regime should assess whether their services fall within its scope. They should also identify the appropriate model for a designated establishment or legal representative, review their internal procedures and test their ability to respond to orders to produce and preserve electronic evidence. In many cases, this analysis will require a multidisciplinary legal and operational assessment in order to understand the organisation's specific exposure and define a proportionate implementation plan.

6. What should you do now?

Regardless of how many requests each organisation receives, one thing is clear: the e-Evidence Package means that responding to judicial authorities is no longer voluntary, but a legal obligation. Furthermore, the deadlines are measured in days or hours, with significant penalties for non-compliance.

Digital service providers operating within the EU must assess whether their activity falls within the scope of the regime on a service-by-service basis. Additionally, where applicable, service providers must designate and provide the necessary resources to the designated establishment or legal representative by 25 February 2027. It is equally essential to adopt internal procedures that allow data to be received, validated, stored and transmitted within the statutory time limits. Service providers must also identify any potential conflicts with the laws of third countries or data protection rules in good time.

Those who prepare before receiving the first order often determine the quality and security of their response when it comes to electronic evidence. In the context of growing regulatory demands, having a tested response model is now critical in mitigating the risk of sanctions, operational risks and reputational risks. PLMJ can support each organisation in assessing its specific exposure and drawing up a tailored implementation plan.

About PLMJ

→ Who we are

“PLMJ is the most organised firm and the most committed at doing things on schedule and to the time that is asked. They are the most up to date and one of most professional law offices that work with us.”

CLIENT REFERENCE FROM
CHAMBERS AND PARTNERS

About Dispute Resolution

→ What we do

KEY CONTACTS



Paulo Farinha
Alves

Partner

+351 213 197 530
paulo.farinhaalves@plmj.pt



Raquel Cardoso
Nunes

Managing associate

(+351) 213 197 566
raquel.cardosonunes@plmj.pt

