SIRIUS EU Electronic Evidence Situation Report

2024

SIRIUS EU ELECTRONIC EVIDENCE SITUATION REPORT 2024

The Hague, November 2024

EUROPOL EUROJUST EUROPEAN JUDICIAL NETWORK Connecting Justice

6th ANNUAL SIRIUS EU ELECTRONIC EVIDENCE SITUATION REPORT

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under contribution agreement No PI/2020/417-500.
This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

YOUR FEEDBACK MATTERS

By clicking on the following link or scanning the embedded QR code you can share your feedback regarding this report. Your input will help us further improve our products.
https://ec.europa.eu/eusurvey/runner/SIRIUS_REPORT_FEEDBACK

INDEX

FOREWORD

It is with great pleasure that I present the SIRIUS European Union (EU) Digital Evidence Situation Report 2024. In its sixth year of implementation, the SIRIUS Project has consolidated as a recognised centre of excellence for electronic evidence within the European Union. The SIRIUS EU Electronic Evidence Situation Report highlights the partnership between Europol and Eurojust, supported by the European Judicial Network. This collaboration guarantees a solid and diversified stakeholder approach comprising all actors involved in the investigation and prosecution of crime. Since its creation in 2017, SIRIUS reports have provided, year after year, an increasingly detailed picture of developments in the field of cross-border access to electronic evidence in criminal investigations. As the widespread use of online services by criminals remains a constant feature of the contemporary EU criminal landscape, the investigation and prosecution of crime cannot be disconnected from the need to access digital data, underlining the reliance on electronic evidence. Social media platforms, messaging apps and crypto exchanges have become highly relevant in criminal investigations, as they are most often abused by criminals in actions ranging from terrorism to cybercrime.

As the need to access electronic evidence records a new height, strong public-private cooperation is ever more necessary to guarantee smooth investigations. Meanwhile, legislative developments at EU level are set to significantly enhance access to electronic evidence for law enforcement agencies. The EU Electronic Evidence legislative package aims to reorganise the process ensuring that authorities can more effectively access electronic evidence in their investigations. However, existing and new challenges related to fast-evolving and decentralised technologies further complicate the work of EU criminal investigators. By investing further in the efforts of the SIRIUS Project, Europol remains committed to support its partners on both EU and Member State levels in the field of electronic evidence to deliver security in partnership towards a safer EU digital space.

Catherine De Bolle
EXECUTIVE DIRECTOR, EUROPOL

Over a year has passed since the EU Electronic Evidence legislative package was adopted in July 2023, and important strides have been made in preparing for its implementation set to take effect in August 2026. It is therefore a great pleasure to present to you the SIRIUS EU Electronic Evidence Situation Report 2024, which serves to highlight some of the progress made thus far.

Challenges remain however, for instance in relation to the absence of a data retention framework for law enforcement purposes at the EU-level and service providers' cross-border policies. With a keen sense for further promoting interdisciplinary cooperation, an important part of the present report's value lies in the many recommendations it develops for all stakeholders involved.

From a judicial perspective and as we anticipate the introduction of the EU Electronic Evidence package and the Second Additional Protocol to the Budapest Convention on Cybercrime, it is crucial for prosecutors and judges to fully leverage the opportunities these instruments will provide. This is even more so as this new legal framework is set to strengthen the role of the judiciary in requesting cross-border electronic evidence in criminal proceedings. We therefore need to develop new knowledge and skills, and I want to call on the international judicial community to incorporate these as much as possible into both basic and in-service training programs.

The future landscape of cross-border judicial cooperation is shaped today, and I am thankful for the guidance and expertise SIRIUS offers. Its work serves a search light for legal and police practitioners in all corners of our continent faced with an ever-bigger digital dimension in their work. With that in mind, I look forward to much more to come from our colleagues.

Ladislav Hamran
PRESIDENT, EUROJUST

EXECUTIVE SUMMARY

For EU competent authorities, the investigation and prosecution of crime in the current EU landscape cannot be disconnected from the need to access digital data and reliance on electronic evidence. As legislation regulating the EU digital sphere evolves, the panorama of cross-border access to electronic evidence remains largely unchanged compared to previous years, as emerging from the annual editions of this report.

Despite significant advancements, such as the EU Digital Services Act, the EU Electronic Evidence legislative package, and the Second Additional Protocol to the Budapest Convention on Cybercrime, the approach of EU competent authorities towards current instruments of judicial cooperation and voluntary cooperation with foreign service providers remains unchanged. Both channels, despite their advantages, face ongoing challenges. While judicial cooperation proves inadequate due to its cumbersome and lengthy procedures, the immediacy of voluntary cooperation exchanges lacks legal certainty for the entities affected. It may, for example, put service providers in a position where complying with data requests from foreign authorities could conflict with their home jurisdiction's laws. Operating within a fragmented national and international legal framework, EU competent authorities involved in criminal investigations requiring access to cross-border digital data do not yet see their duties simplified.

Pooling together strengths and weaknesses, and threats and opportunities affecting the wide field of cross-border access to electronic evidence for the purpose of EU criminal investigations, this report is based on direct exchange with main stakeholders in the field.

From the perspective of EU law enforcement, the report highlights that direct requests under voluntary cooperation remain the primary tool for acquiring data in electronic format from social media platforms, messaging apps and cryptocurrency exchanges. Confirmed as the most relevant service providers in criminal investigations in 2023, they were mainly targeted for the disclosure of non-content data – such as connection logs, user names and IP addresses. While the relevance of Single Points of Contact (SPoCs) [(1)] in all aspects of cross-border engagement with the industry remains significant in guaranteeing higher compliance rates of requests, EU law enforcement also benefits from a steady increase in the level of training received, year after year, on electronic evidence matters. Challenges, however, persist, particularly in the form of lengthy judicial cooperation procedures as well as fragmentation of companies' policies for cross-border cooperation. The new legislative instruments in the EU Electronic Evidence legislative package, though not yet known in detail by authorities, appear to be met with a mixture of positive expectations, as well as some concerns. The lack of clarity over key concepts, the exact scope or providers covered, as well as the potential transformation of the roles of law enforcement authorities, are some of the issues highlighted by the direct feedback of the EU law enforcement surveyed. From a more general point of view, although not yet a concrete issue, the potential

abuse of AI-related technological developments is expected to present new challenges for investigating authorities.

From the perspective of judicial authorities, judicial cooperation channels remain the preferred method for obtaining electronic data from service providers located abroad. However, these channels often prove inadequate due to their slow processes, which can lead to the loss of crucial data. To mitigate these delays, some EU Member States' authorities have resorted to direct voluntary cooperation with foreign service providers.

Significant advancements are anticipated with the introduction of the EU Electronic Evidence legislative package and the Second Additional Protocol to the Budapest Convention on Cybercrime. Designed to be more efficient and flexible than existing judicial cooperation tools, these instruments will significantly enhance the toolkit available to EU judicial authorities, providing more robust and streamlined mechanisms for accessing electronic evidence across borders. However, these new legal frameworks will not address one of the key challenges identified by EU judicial authorities: the absence of a data retention framework for law enforcement purposes.

Additionally, the report underscores the importance of continuous capacity building on both existing and forthcoming data acquisition modalities. This is crucial for enabling EU judicial authorities to navigate the complexities of the legal landscape and maximise the benefits of the new instruments for effective cross-border access to electronic evidence.

From the perspective of service providers, the volume of requests for data disclosure has increased, but the processes for direct and voluntary cooperation have not recorded additional challenges as reported in the past, as this report shows. Conversely, as public-private cooperation improves, the challenges reported – such as overly broad requests, lack of contextual information or misunderstandings of services and policies provided, appear solvable through better communication and more targeted educational effort. SPoCs remain, also in the eyes of the industry, an efficient model to be multiplied and expanded within the current legislative framework and maintained in the future framework following the implementation of the EU Electronic Evidence legislative package.

On legislative developments affecting the electronic evidence field, while feedback remains varied, providers are more vocal about their expectations for improved quality and frequency of efforts by main EU Institutions responsible for policy implementation. Recognising the substantial changes the new framework will introduce, providers regard the envisaged decentralised IT system for secure digital communication and data exchange as raising the biggest concerns.

Finally, all public and private stakeholders involved in the preparation of this report view the SIRIUS Project, with its knowledge acquired and developed thus far, and its pivotal role as a centre of excellence in the EU on electronic evidence matters, as an essential actor in the present and future of the electronic evidence field.

RECOMMENDATIONS TO STAKEHOLDERS

The report concludes with a set of recommendations to improve existing processes today, and to prepare for the application of new rules in the future.

For EU law enforcement agencies

- Prepare for and adapt to the EU Electronic Evidence legislative package;
- Broaden training efforts on cross-border access to electronic evidence covering current framework and future developments;
- Reinforce SPoC approach and ensure active engagement with the SIRIUS SPoC Network.

For EU judicial authorities

- Enhance knowledge and capacity on available legal instruments for cross-border access to electronic evidence;
- Prepare judicial authorities to effectively use new instruments under the forthcoming EU Electronic Evidence legislative package, as well as other legislative changes concerning the cross-border acquisition of electronic evidence;
- Strengthen mutual trust and knowledge sharing among EU judicial practitioners on cross-border gathering of electronic evidence.

For service providers

- Prepare for compliance with the EU Electronic Evidence legislative package and share early updates with EU authorities;
  Engage closely with the SIRIUS Project and share policy updates with the SIRIUS Team.

For actors implementing the EU Electronic Evidence legislative package at the EU and Member State level

- Engage with the broad community of EU competent authorities and service providers;
- Leverage SIRIUS' expertise via early involvement in implementation.

KEY FINDINGS

PERSPECTIVE OF LAW ENFORCEMENT IN THE EU

Social media, messaging apps and crypto exchanges remain the most relevant online services in criminal investigations.

74% of officers are satisfied with the SPoC process, in agencies where these are established.

Only 4% of officers consider themselves very familiar with the EU Electronic Evidence legislative package adopted in July 2023.

The SIRIUS Platform remains the highest-ranked source of information in relation to direct requests to service providers.

What are the law enforcement officers saying about the EU Electronic Evidence legislative package?

"I think the new legislative EU E-evidence package will make the process of obtaining electronic evidence more efficient, predictable, and legally secure, which is crucial for law enforcement agencies to be able to combat crime in a more effective way." (Belgium).

"As far as we are aware, only judicial requests will be possible in the future. This leads to considerable problems in purely police-related cases, as no public prosecutor's office is involved in these [cases]. This can lead to information deficits." (Germany)

PERSPECTIVE OF JUDICIAL AUTHORITIES IN THE EU

Judicial assistance (MLA/EIO) is the primary and most reliable method for EU judicial authorities to legally obtain electronic evidence across borders.

Lengthy judicial assistance procedures and the absence of an EU-wide data retention framework continue to be the primary challenges.

37% of EU judiciary are unfamiliar with existing cross-border data acquisition methods, and 46% lack familiarity with the EU Electronic Evidence legislative package and the Second Additional Protocol.

Capacity building is crucial for the EU judiciary to enhance awareness, knowledge and skills.

What are the judicial authorities saying about the EU Electronic Evidence legislative package?

"The new possibilities for the national competent authorities, provided by the EU Electronic Evidence legislative package are of a critical importance to the evidence gathering process, as they would ensure rapid and timely preservation of the electronic evidence and provide certainty for all judicial and law enforcement authorities that the required data will be saved, whether encrypted or not. Addressing European Production Orders and European Preservation Orders directly to a service provider in another Member State, as well as having short deadlines for execution, will facilitate investigations - not only of cybercrimes. The creation of designated establishments or legal representatives for the service providers in the EU is also a step in the right direction. We look forward to the EU Electronic Evidence legislative package becoming applicable due to the need for investigations to take such an approach." (Bulgaria)

PERSPECTIVE OF SERVICE PROVIDERS

The volume of EU data disclosure requests increased by 22% from 2022 to 2023.

The success rate of EU requests in 2023 was 74%, which is the best result since the first edition of this report.

The perceptions and the concerns of service providers around the EU Electronic Evidence legislative package vary a lot.

Service providers expect EU legislators to provide clear guidance and set up outreach and cooperation programmes ahead of August 2026.

What are the service providers saying about the EU Electronic Evidence legislative package?

"The E-evidence legislative package and the new processes introduced will bring more legal certainty to data disclosure in criminal investigations."

"The EU Commission should outreach more and create programmes to prepare stakeholders. Preparatory work requires detailed guidance from legislators as providers are hugely affected by new legislation."

INTRODUCTION

About the SIRIUS Project

In its sixth year of implementation, the SIRIUS Project is an established centre of excellence in the field of cross-border access to electronic evidence in the EU. Implemented by Europol and Eurojust, the project assists over 7,800 law enforcement officers and over 550 judicial authorities from all 27 EU Member States, as well as 23 third countries, in the process of requesting data from service providers, in the context of criminal investigations.

SIRIUS promotes multi-stakeholder dialogue and fosters cooperation by deploying strong outreach efforts, organising international events for experts and practitioners, preparing public and restricted knowledge resources, as well as delivering restricted online and in-loco training activities for law enforcement and judicial authorities. Through these activities, SIRIUS helps the community of EU competent authorities navigate legal and policy developments in the field of electronic evidence. SIRIUS regularly provides guidance to authorities ahead of the introduction of new rules stemming from the *EU Electronic Evidence legislative package*, as well as the *Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and disclosure of Electronic Evidence* (Second Additional Protocol), as well as other legislative developments. Some SIRIUS resources (for example, legal and policy reviews) are publicly available on Eurojust's website, whereas most resources are disseminated to authorities only via the restricted SIRIUS platform, hosted on the Europol Platform for Experts.

Funded by the European Commission's Service for Foreign Policy Instruments since 2018, SIRIUS has been able to achieve its results by partnering with international stakeholders to promote the standardisation of processes and templates, and to contribute to international capacity building activities in the EU, as well as in several events worldwide.

Furthermore, through the annual *SIRIUS EU Electronic Evidence Situation Report*, the project promotes transparency towards stakeholders and the general public, by collecting and analysing available data in relation to cross-border access to electronic evidence for the purpose of criminal investigations and proceedings. The image below highlights some of the most important achievements of the SIRIUS Project since its creation. The current phase of the SIRIUS Project ends in December 2024.

Context

2023 marked an important year in the field of cross-border access to electronic evidence, as the new EU Electronic Evidence legislative package was adopted [(2)]. Whereas the new legislation will apply only as of mid-2026 [(3)], its adoption sets a clear path for EU Member States and service providers to adapt existing processes and procedures, bringing more legal certainty and efficiency to the process of obtaining electronic evidence across borders in the future. The Electronic Evidence Regulation, in particular, will enhance judicial cooperation with the introduction of European Production Orders and European Preservation Orders. At the same time, specific and practical aspects of the future processes remain unclear, including whether direct requests under voluntary cooperation will still be accepted by service providers and how authorities can, in general, remain up-to-date with the evolving changes. There included, in the current investigative panorama, the particularities of each service provider (e.g. which datasets can be requested, what are valid identifiers per service provider etc).

Additionally, other policy developments unfolded in the field of electronic evidence in the EU and beyond, such as the advancements in the signature and ratification process of the Second Additional Protocol [(4)] and the application of the Digital Services Act (DSA) and its provisions [(5)]. The DSA, in particular, addresses some of the concerns arising from the current fragmented legal landscape as far as cross-border access to electronic evidence is concerned, by introducing common rules to the content and format of cross-border orders for data disclosure directed at service providers. Without setting out a legal basis for such orders, which must be based on either EU or national law, Article 10 of the DSA sets minimum conditions that such orders must meet and establishes complementary requirements for processing them. This regulatory framework aims to harmonise procedures and reduce legal ambiguities, but challenges remain.

2024 was equally prolific in terms of the adoption of new pieces of EU legislation and full implementation of already-passed ones. On one hand, the DSA became fully applicable as of February 2024, while designated gatekeepers under the Digital Markets Act [(6)] had until March 2024 to comply with its requirements. On the other hand, new EU rules in the field of Artificial Intelligence (AI) were adopted [(7)]. Although these pieces of legislation do not directly impact the gathering of electronic evidence by EU competent authorities, they significantly affect the industry, making them relevant for authorities as well.

Against this background, and facing the constant need to access electronic data in criminal investigations and proceedings, the expectations of EU competent authorities regarding new legal instruments have been steadily increasing. However, the current landscape for cross-border access to electronic evidence remains largely unchanged compared to previous years.

While judicial cooperation channels remain a relevant modality to obtain electronic data from service providers located abroad, EU competent authorities still resort to requesting disclosure of non-content data directly from service providers under voluntary cooperation in jurisdictions where this is possible. However, this approach lacks uniform regulation across all EU Member States, and competent authorities often find themselves dealing with different legal requirements – on top of those established by each service provider – and with uncertainty as to whether the data so obtained

can be admissible as evidence in court. In addition, not all service providers cooperate voluntarily with foreign authorities, either because of their legal obligations under domestic law, or due to lack of resources or unwillingness.

For competent authorities, obtaining targeted user data from service providers can therefore be a complex and time-consuming task, even when using judicial cooperation instruments. As these were created before the era of cloud computing and the widespread use of online services, EU competent authorities must deal with cumbersome legal procedures, which do not provide the necessary speed for obtaining electronic evidence.

At the same time, the widespread use of online services by criminals remains a constant feature of the contemporary EU criminal landscape, requiring law enforcement and judicial authorities to constantly adapt to new challenges in order to prevent, detect, investigate and prosecute crimes. The increasing availability of communication services with built-in end-to-end encryption and the general shift towards a decentralised internet further complicates their efforts, as does the lack or limited scope of regulatory frameworks around, for example, lawful access to criminal communications [8].

Last but not least, the successful implementation of the new legal frameworks requires enhanced knowledge and capacity among competent authorities, enabling them to navigate the complexities of the evolving legal landscape and maximise the benefits of the new instruments for effective cross-border access to electronic evidence.

While acknowledging the main legislative developments and the opportunities they may bring in the future, this report primarily reflects on 2023, using the most up-to-date data available to describe the state of play regarding the use of electronic evidence in the EU over a year-time. The report provides a trend analysis that can serve as a baseline for authorities and service providers alike as they prepare for the implementation of the new legal instruments.

Methodology

The methodology used for this report is similar to previous editions. The SIRIUS Project privileges a multi-stakeholder approach and presents perspectives from law enforcement, judicial authorities and service providers collected via surveys and dedicated interviews, as further detailed below.

Surveys with law enforcement authorities

Europol conducted a survey among law enforcement agencies and collected 360 responses from representatives from all EU Member States, between April and May 2024.

The survey was also open to law enforcement authorities from non-EU Member States which have operational or working agreements with Europol. 60 responses were received from Albania, Bosnia and Herzegovina, Canada, Colombia, Iceland, Japan, Montenegro, Norway, Republic of North Macedonia, Serbia, Switzerland, Ukraine and

the United States of America. The results relating to contributions from non-EU Member States are presented in a dedicated section in this report for comparison purposes, and they are not considered in the overall results of the chapter Perspective of Law Enforcement.

Furthermore, direct and continued engagement with law enforcement authorities serving as SPoCs yielded relevant insights. The SPoC community belonging to the SIRIUS SPoC Network provided inputs on different occasions, above all during the SIRIUS SPoC Network Meeting organised in cooperation with the Irish An Garda Síochána [(9)].

Surveys with judicial authorities

Eurojust collected feedback from judicial authorities from 25 EU Member States [(10)]. A survey was administered between April and May 2024, reaching out to the judicial community on the SIRIUS Platform, as well as European Judicial Cybercrime Network (EJCN) and European Judicial Network (EJN) Contact Points. In total, 46 in-depth responses were received reflecting the situation in 25 EU Member States. This compilation of information forms the basis for the analysis and recommendations presented in this report.

Furthermore, this report includes a substantial contribution from the EJN discussing the transmission of electronic evidence through the e-EDES Platform. It reflects the outcome of discussions that took place in November 2023 during one of the workshops held at the 61st Plenary Meeting of the EJN under the Spanish Presidency of the Council of the EU.

Interviews with service providers

Between April and June 2024, Europol and Eurojust collected inputs from representatives of 19 service providers, namely: Airbnb, Apple, Booking.com, Coinbase, eBay, Google, Mega, Meta, Microsoft, PayPal, Rakuten, Riot Games, Snap, TikTok, Uber, Vodafone, Western Union, X and Yahoo [(11)]. The findings presented in this report should not be taken as the formal position of any of the private entities.

The main topics discussed with these companies were:

- Main reasons for refusals or delays in processing data requests from EU authorities in criminal investigations;
- Current and future challenges in the area of cross-border data disclosure requests;
- SPoC approach for cross-border data disclosure requests under voluntary cooperation; and
- Policy developments in the area of electronic evidence.

Information from companies' publicly available transparency reports regarding governmental requests for data disclosure

The transparency reports analysed for the purpose of this report were those of Airbnb, Google, LinkedIn, Meta, Reddit, Snapchat, TikTok and Yahoo. The numbers presented in this report for the years 2018 – 2021 differ from the results presented in previous reports. This is because data from Apple, Microsoft and X (formerly known as Twitter) have been removed from the analysis, since their transparency reports for the full year of 2023 had not been published by 20 October 2024, when the draft of this report was finalised.

Additionally, as following the entry into force of the DSA, service providers falling within the scope of the Regulation are required to fulfil specific transparency requirements, reference to the DSA transparency reports of Facebook, Instagram, Google (inclusive of Google Search, Google Maps, Google Play, Google Shopping and YouTube), TikTok, Snapchat and LinkedIn were added to this edition of the SIRIUS Electronic Evidence Situation Report. For the sake of consistency, the selection of DSA transparency reports was limited to those same providers whose transparency reports regarding governmental requests for data disclosure were analysed.

PERSPECTIVE OF LAW ENFORCEMENT

Examples of real cases

Europol requested EU law enforcement officers to share examples where electronic data was deemed crucial evidence in criminal investigations. It is often the case that data disclosed by service providers is the only investigative lead. The cases listed below further demonstrate how access to specific data from targeted users can be critical when investigating different crime areas [12].

*"As our unit primarily investigates **hate speech, terrorist propaganda and terrorist threats** in the online world, we are faced with the need to issue direct requests on a daily basis. Due to the nature of our investigations, which often involve an imminent physical threat, the service providers are generally very reactive, resulting in the rapid identification, localisation and apprehension of the suspects involved."*

*"In most of our investigations we have obtained electronic evidence through direct request. Especially in **terrorism-related cases**, which often lead to the quick arrest of the suspects involved."*

*"Based on direct queries to Google for the IMEI address of a smartphone in use, an e-mail address and payment card details were obtained. These supported in identifying the suspect **as a serial offender in the field of computer fraud**, to whom a large number of offences can now be attributed. Currently the perpetrator is in custody."*

"We had very good cooperation with Booking.com and Airbnb. The SIRIUS guidelines were perfect and helped us make contact with these companies. Both service providers offer a user-friendly online platform to receive and send requests. I know we are talking about 2023, but I also need to mention a very successful cooperation with TikTok this year (emergency and direct request as well). In the case we also used the SIRIUS guidelines as a basis for our request creation."

*"Electronic evidence obtained through direct requests was **essential for identifying physical persons in investigations in 80% of cases**."*

*"We had many urgent cases regarding **terrorist activities or in case of child kidnappings**. Our unit is very familiar with getting data from various service providers so we obtained data which was crucial. We always use the SIRIUS database for renewing our information on how to approach the service providers in the correct way. That is a really great project and we hope that it will expand."*

*"We have many cases in which electronic evidence is essential (**business e-mail compromised crime, crypto scams**, etc). But unfortunately, there is no way to go forward because the proceedings to get answers from foreign companies are too complicated. When we have collaboration from that side, investigations can be completed."*

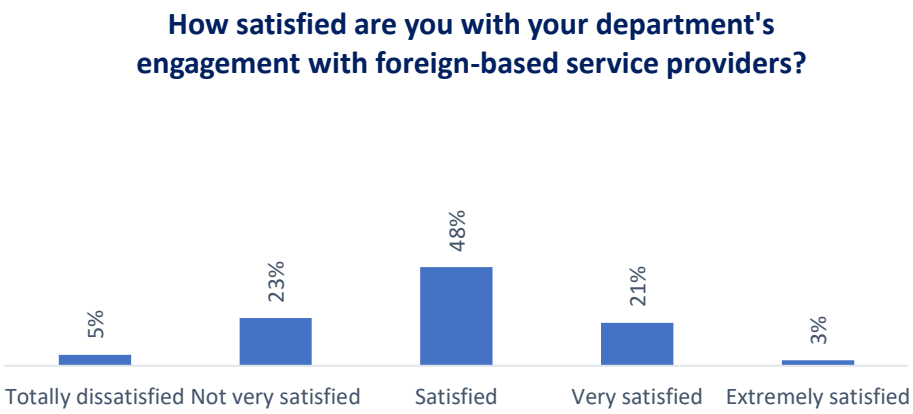
"We have identified the perpetrators with data received from Google, PayPal and Meta platforms. In cases where a MLA [Mutual Legal Assistance] request was needed, it took too long and by then the data obtained was not relevant anymore."

*"The SIRIUS guidelines helped me to clarify precisely what information I was able to obtain from Meta for a **recent murder investigation**. As a result of obtaining a court order for the release of available information, we obtained vital evidence in respect of a murder suspect who is currently before the court."*

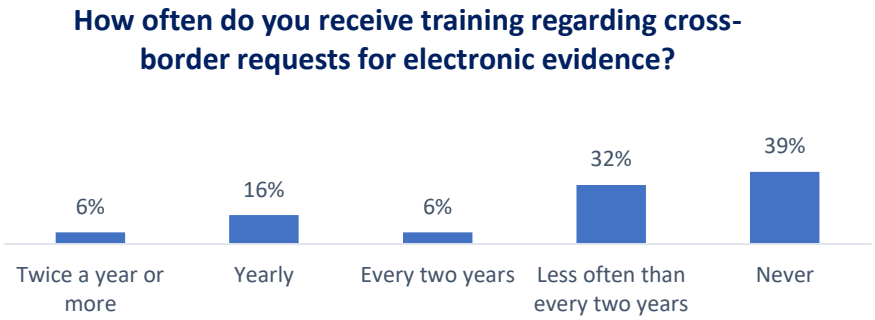
Engagement of EU law enforcement with foreign-based service providers

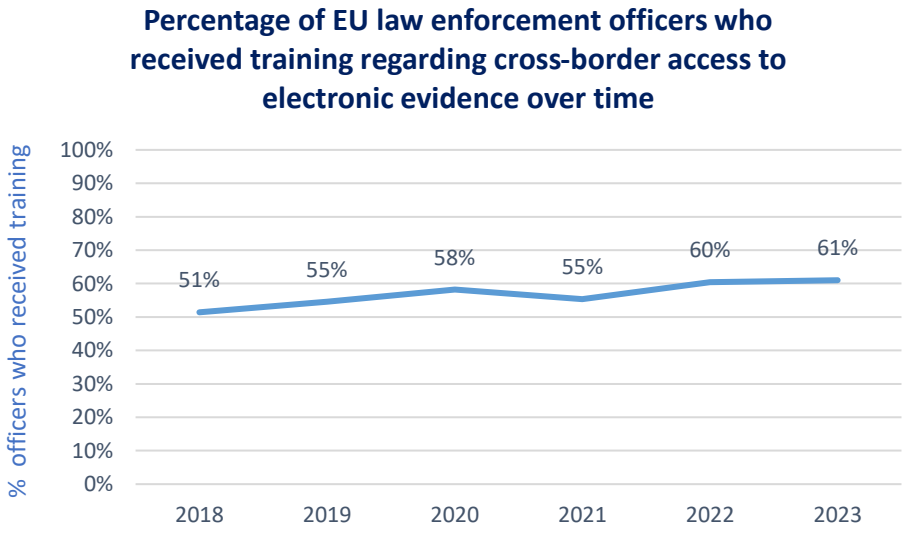
When dealing with requests for data disclosure to service providers, law enforcement officers must ensure compliance with their own domestic legislation. However, there is also an additional layer of complexity, as they must also take into consideration international legislation as well as law of the jurisdiction where the targeted service provider is based. Moreover, whenever the issuance of direct requests for voluntary cooperation is possible, officers must also consider the different requirements established by each service provider.

In spite of the complex landscape in which they currently operate and the persisting challenges [(13)], 72% of EU law enforcement officers reported being satisfied, very satisfied or extremely satisfied with their department's engagement with foreign-based service providers in 2023. The satisfaction rate of 2023 saw a 2% decrease in comparison with the results for 2022 [(14)].

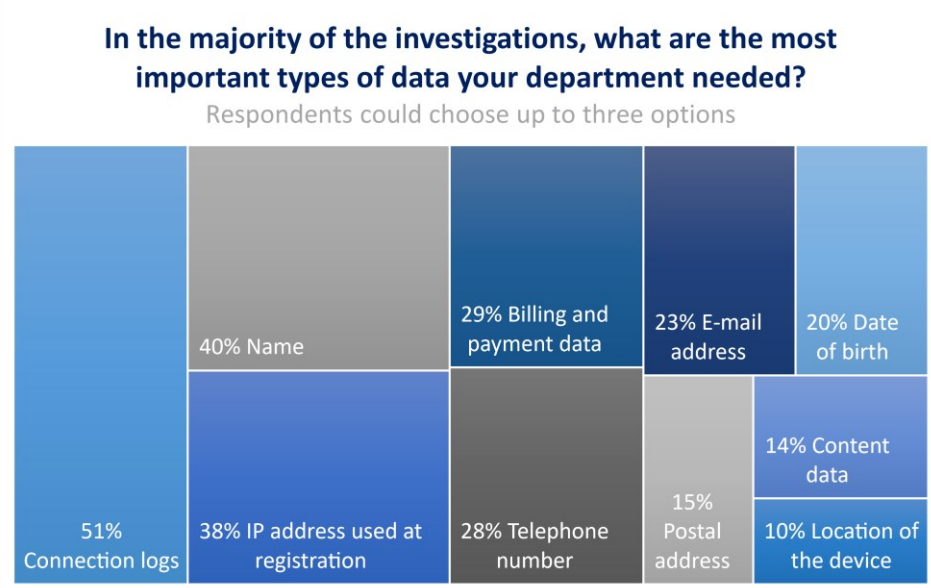


In 2023, the majority of EU law enforcement officers (61%) reported having received some training regarding cross-border access to electronic evidence. This year's result shows a slight increase compared to what was reported for 2022 and constitutes a considerable improvement in comparison with 2018, when only 51% of officers reported having received some training on this matter.

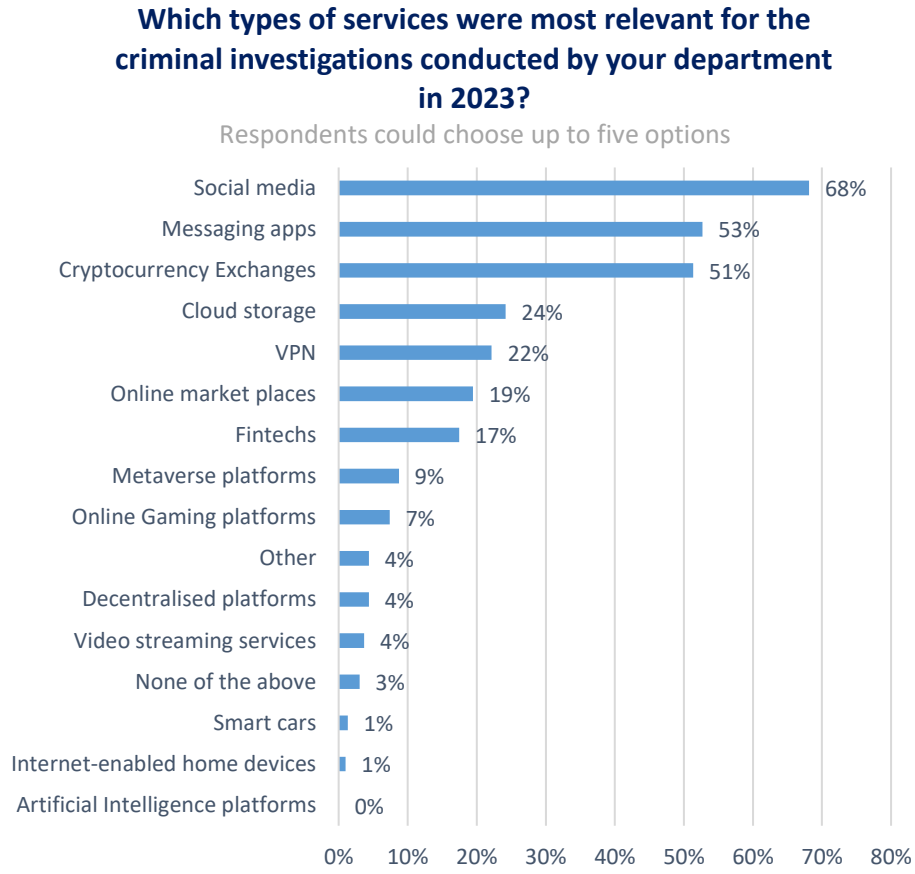




Data disclosure requests in the context of criminal investigations must always be very specific in relation to the persons whose data is requested. Additionally, the requests must abide by the principles of necessity and proportionality by specifying, among other things, the datasets sought and the precise timeframe relevant for the investigation. In 2023, officers found that the three most important datasets for criminal investigations were: connection logs (date, time and Internet Protocol (IP) address of connection to an online service), the name of the user, and the IP address used at the moment of first registration to the service. Although with different percentages, these three data categories rank first since the 2021 edition of this report. It is also worth noting that 14% of officers considered that content data was among the three most important types of data needed in investigations; a 2% decrease compared to the 2022 results.



Providers of many different types of services can be deemed relevant by law enforcement for their investigations. In 2023, the five most important types of service providers were: social media platforms, messaging apps, cryptocurrency exchanges, cloud storage and Virtual Private Network (VPN) providers. The result mirrors what reported for 2022.



Providers of AI-related services, internet-enabled home devices, smart cars and *metaverse* platforms did not figure among the most important ones in criminal investigations carried out in 2023. Notably, AI platforms were not selected by any respondent.

Despite the above findings, the law enforcement community surveyed observed ongoing developments in these areas with great interest, especially when reflecting on the impact of AI on their work. The opportunities that new technologies could bring about are only equal to the challenges.

For instance, officers mentioned that AI could facilitate their work and lead to more effective and accurate investigations when dealing with a huge volume of data. On the other hand, officers also voiced their concerns over the challenges that could result from implementing such technologies from an organisational, technical, and legislative point of view. For example, there is a lot of concern in relation to the use of *deep fakes* and automatic generation of disinformation for criminal purposes. Surely, a significant effort in training activities and specialisation will be required.

Some of the comments provided by officers in this regard are listed below:

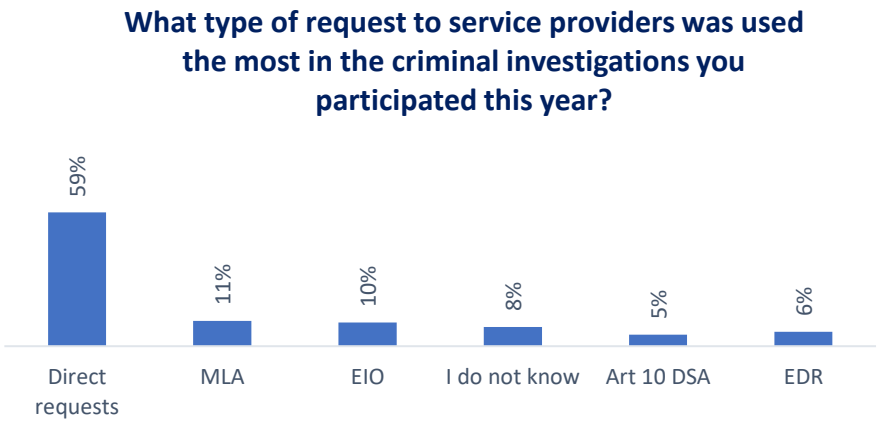
> *"It will become **more difficult for law enforcement agencies to detect crimes at an early stage**, as LEAs [Law Enforcement Agencies] will have limited access to these environments. On the other hand, AI and VR/AR [Virtual Reality and Augmented Reality] will make it easier for criminals to have a wider impact on society, potentially creating many more victims which will affect the workload for LEAs as well."*
>
> *"I think this presents new challenges and requires raising the knowledge and readiness of the police to a higher level. I also think that **we are not adapting to new challenges fast enough**."*
>
> *"Investigations will become more specialised in the future and require higher qualifications. On the other hand, **our law enforcement agency is becoming increasingly outdated. Prosecution will become even more difficult**. It will become easier to conceal perpetrator structures. At the same time, law enforcement agencies traditionally lag behind the perpetrators, technologically and also in terms of expertise in the field of cybercrime."*
>
> *"There will be **more data to process**. It may take time to adapt to these new technologies and I hope for specialised training on these tasks. Hopefully SIRIUS will be a part of this process."*
>
> *"The **first problem is the recognition of AI-generated products**, because these are getting better. These products can be used for propaganda, blackmailing, fraud, etc. But for high-quality products, the maker/owner has to be subscribed for an appropriate AI tool. Here is the evidence: the AI service provider will need to have the user registration data and billing data. These can identify the user, so we have to turn to the AI service providers with our requests."*
>
> *"Personally, I think **criminals are getting better at using AI technology than law enforcement agencies** and they get better training in the private sector, which means they do not have all the legal obstacles that we, law enforcement agents have."*

"AR/VR [Augmented Reality/Virtual Reality] can provide opportunities for training activities. AI could be partially used in analysis (pre-digest, summaries, automation) "

Submission of cross-border requests

Direct requests for voluntary cooperation to service providers for disclosure of non-content data have become the primary channel for public-private engagement, especially when compared with other means of obtaining data. Like in previous years, the majority of officers (59%) reported that, in 2023, direct requests were the most used type of requests to service providers in the criminal investigations that they participated in.

When direct requests are not possible, officers must work together with judicial authorities to obtain the necessary data to continue their investigations via MLA (Mutual Legal Assistance) or European Investigation Orders (EIOs). It is important to note that the use of international judicial cooperation is a requirement in some countries to ensure that the data obtained from a foreign-based service provider is admissible as evidence. In other circumstances, different type of requests might be used within one unique case – when, for example, authorities complement a direct request via judicial cooperation channels. Additionally, there are many service providers that refuse to cooperate with foreign authorities on a voluntary basis, or that are unable to do so in accordance with domestic regulations. Emergency Disclosure Requests – direct requests for voluntary cooperation in emergency circumstances, usually those involving an imminent threat to life – were considered to be the most important type of request by 6% of officers in 2023.

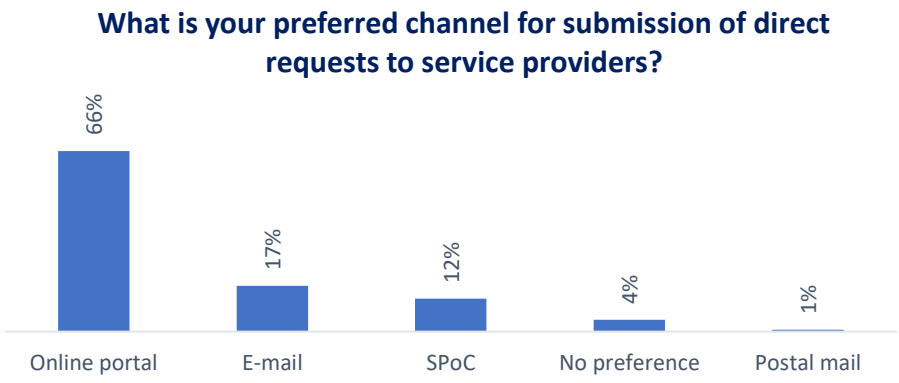


Although the DSA has been fully applicable only as of February 2024, the first Very Large Online Platforms and Very Large Online Search Engines (VLOPs and VLOSEs, respectively [15]) designated as such by the Commission have been subject to its rules as of April 2023 [16]. In 2023, EU law enforcement could therefore submit orders to provide information pursuant to Article 10 of the DSA, in combination with a legal

basis under EU or national law, to VLOPs and VLOSEs established by then. Despite the short timeframe, it is notable how a small percentage (5%) of EU law enforcement surveyed referred to the DSA as the most used type of request.

Because direct requests are considered voluntary cooperation, service providers may set up their own rules and requirements for competent authorities to adhere to. The channel for submitting requests is one such requirement that varies among service providers. Some choose to create dedicated online law enforcement portals to submit their requests – such as Airbnb, Google, Microsoft, Meta, Uber, X, WhatsApp, and Zoom. Other service providers – such as Binance, Bumble, Coinbase, Discord, LinkedIn and Roblox, do not have their own online law enforcement portal, but accept requests via third-party online portals offered by specialised companies.

The majority of officers surveyed (66%) prefer submitting their requests via online portals, rather than via e-mail, which constitutes a 7% increase compared to last year's results. The benefits of using online portals often include the possibility to consult the status of each request, securely download responses, and streamline the communication between competent authorities and representatives of service providers. The preference to submit requests via national SPoCs records a 3% decrease compared to last year.



The SIRIUS Platform remains the first ranked source of information in 2023 for law enforcement officers who need assistance to prepare direct requests. This is followed by SPoCs and, differently from last year, when the third preferred option was consulting foreign-based service providers themselves, by law enforcement national central units.

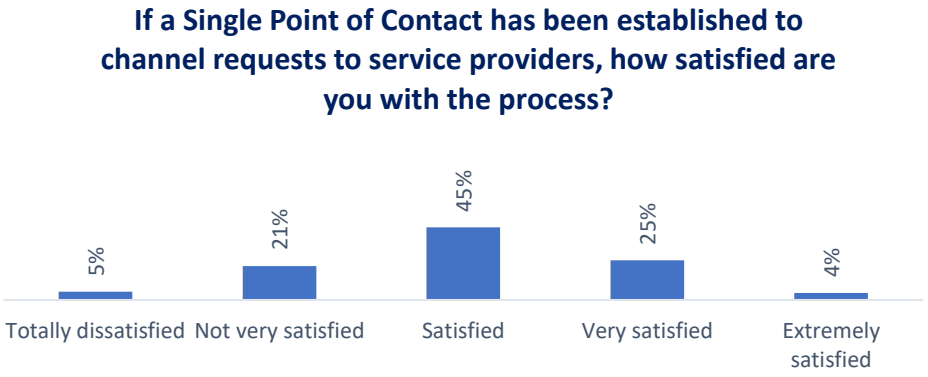
When it comes to assistance relating to MLA, in 2023, SPoCs became the most consulted by law enforcement officers, followed by national judicial authorities. In this case, SIRIUS was mentioned as a source of information by 24% of respondents in 2023, a 3% increase compared to last year.

Among the law enforcement officers surveyed, 74% are satisfied or more than satisfied with the processes established. In addition to their function of centralising and streamlining the submission of direct requests to foreign-based service providers, other benefits of SPoCs are:

- The establishment of a SPoC process contributes to increased quality of requests, as the persons or units designated as SPoCs are specialised in electronic evidence matters. Consequently, it leads to a decrease in response time from the side of service providers.

SPoCs have, for example, a very good understanding of the applicable requirements, the type of information that must be included in requests, and the datasets that can be requested from each service provider.

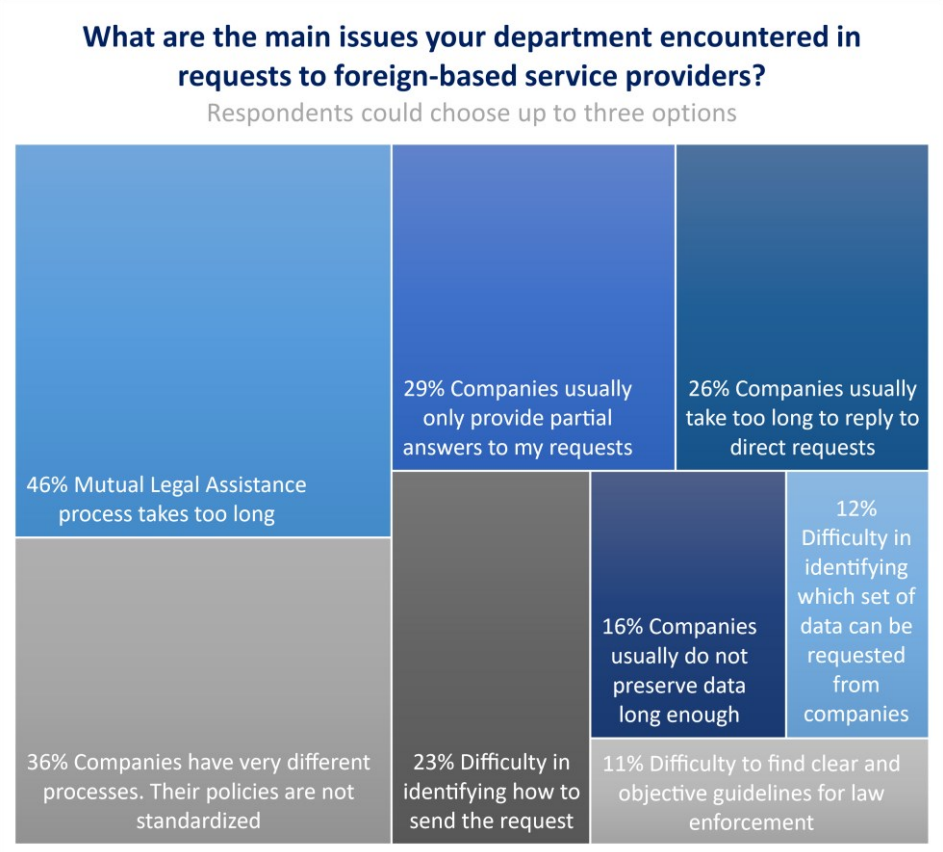
- SPoCs make it possible to establish streamlined communication in emergency circumstances, ensuring faster processing of information.
- Updates, feedback, and training material can be disseminated through a single channel, and questions from the different units can be centralised and routed through the SPoCs. This ensures that all law enforcement officers in that agency benefit from the provided information.
- Establishing SPoCs helps to deconflict investigations and minimise the duplication of requests regarding the same case from different units or even from different law enforcement agencies.
- SPoCs have proven to be effective tools in building greater cooperation between service providers and law enforcement agencies.



Via direct engagement with EU law enforcement authorities, SIRIUS identified 33 law enforcement agencies acting as SPoCs in 22 Member States: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Slovakia, Slovenia, Spain and Sweden. Additionally, SPoCs also exist in Georgia, Iceland, Norway and the United Kingdom.

When it comes to the volume of direct requests handled by SPoCs in 2023, presenting a comprehensive overview appears to be a challenging endeavour. SPoCs have different internal practices or various arrangements in place with different service providers. Additionally, detailed statistics are lacking and even those SPoCs keeping track of the number of direct requests handled, do it in various ways. All of this considered, SIRIUS estimates that, in 2023, a total of 35,146 direct requests were handled by eight SPoCs from six different countries [(17)].

As regards the challenges encountered by law enforcement officers in the submission of direct requests for data from foreign-based service providers, the list remains unchanged in 2023 compared with previous editions of this report. The length of judicial procedures, the lack of standardisation of service providers' policies for cooperation with law enforcement, and the perceived partiality of answers received are now constant features of EU public-private engagement across borders.



Other issues that were mentioned by less than 10% of officers included:

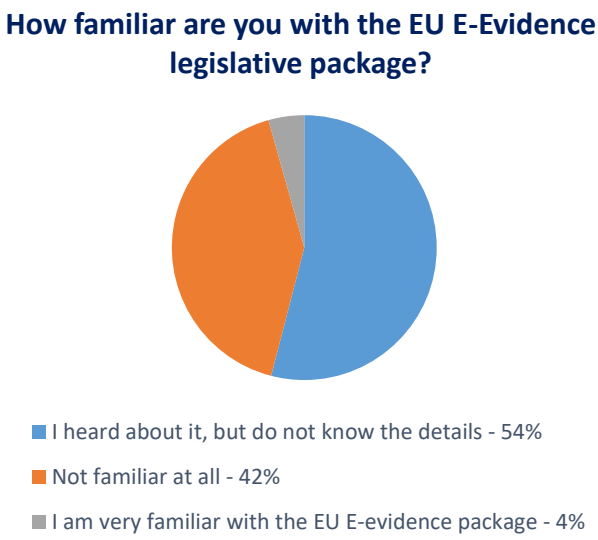
- Information is only available in English, not in my own language;
- Lack of technological resources to analyse responses from service providers;
- Company's user notification policy when a request has been made and the negative effect this has on the investigation; and
- Some service providers refuse to reply to direct requests, even in emergencies.

EU Electronic Evidence legislative package

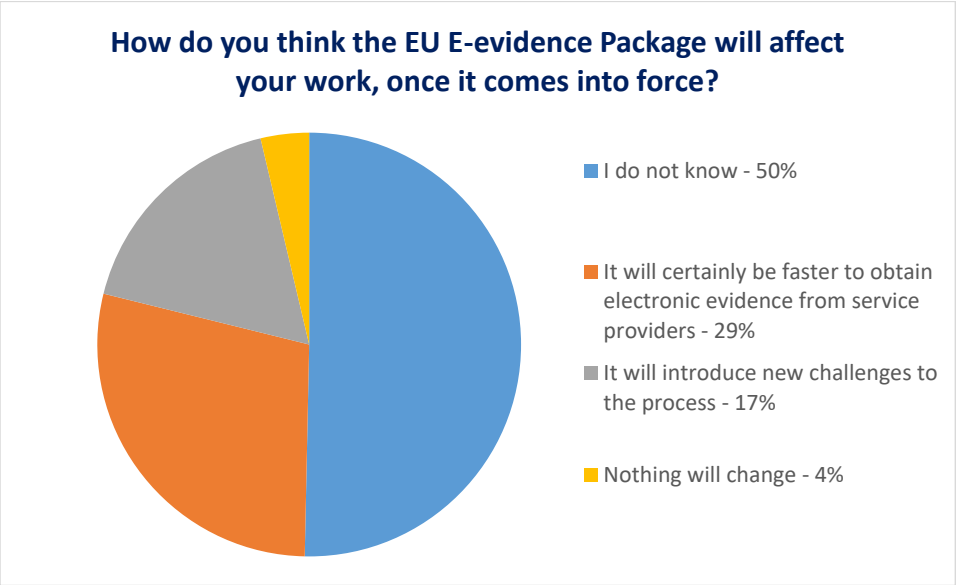
The new EU Electronic Evidence legislative package will introduce new instruments for authorities to request data disclosure from foreign-based service providers offering their services in the EU. Predictably, the new legislation will change the international panorama for access to electronic evidence across borders, as many service providers

could introduce changes to their processes, affecting the current practice of accepting direct requests under voluntary cooperation, for example.

The new rules will have profound implications for the electronic evidence retrieval process. One year after the adoption of the legislative package (as of June 2024, when the survey with law enforcement was conducted for the purposes of this report), only 4% of law enforcement officers reported being very knowledgeable about the legislative package (a 3% decrease compared to last year's results). Conversely, the majority of officers surveyed (54%) had heard of the existence of the new rules yet without knowing the details.



Among the officers who indicated having heard about the EU Electronic Evidence legislative package, or those that are very familiar with it, only about one third are positive about the effect it may have (29%, resulting in a slight increase compared to last year's results). These officers believe it will certainly be faster to obtain electronic evidence from service providers. However, 17% of the officers surveyed also believe that there will be additional challenges to the process, whereas half of the respondents (50%) are still unsure about the effects the new legislation will have on their work.



Among officers who reported that it will certainly be **faster to obtain electronic evidence** from service providers, the following comments were submitted:

> "*I think the EU Electronic evidence legislative package will make the process of obtaining electronic evidence **more efficient, predictable, and legally secure**, which is crucial for law enforcement agencies to be able to combat crime in a more effective way."*
>
> *"The processes for obtaining data from abroad are far too cumbersome. **Every change in the right direction brings a considerable advantage** for investigations."*
>
> *"The new rules will bring **standardisation of communications and engagement with service providers**, will be easy to use and guarantee judiciary support."*
>
> *"The new rules will make it **easier and faster** for law enforcement agencies **to access electronic evidence** from service providers offering services in the EU, regardless of the location of the data."*

Among officers who reported that the new policy will introduce **new challenges to the process**, the following comments were submitted:

> "*The **criteria for the use** of new instruments are **reportedly very strict**. Service providers will not disclose data voluntarily anymore after they have to start answering to the electronic evidence orders, so there is **no route to obtain information in the criminal cases to which the Electronic Evidence legislative package is not applicable**. One problem is the detection and prevention incidents where no criminal pre-trial investigation is yet existing."*
>
> *"We have a big problem in Finland with the Electronic Evidence legislative package because orders have to be signed by a prosecutor. We have **no process** in Finland **to involve prosecutors with police requests** because we do not need the prosecutor to sign our requests normally. Police has all the investigative*

*powers and prosecutors are not tied to it in any way. This **introduces a new workload for prosecutors who are not prepared for the process**."*

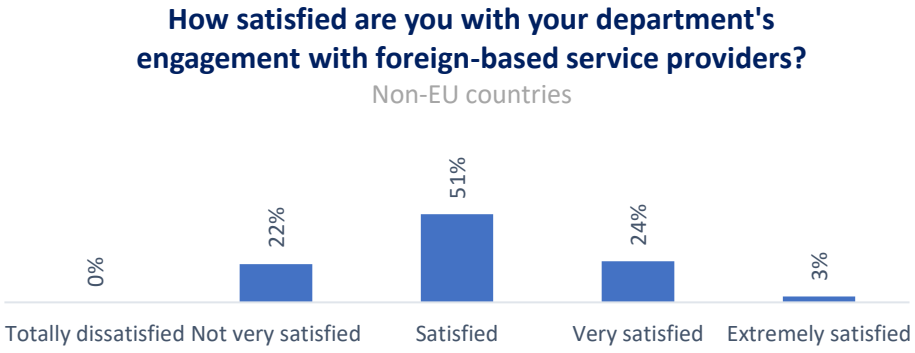
*"As far as we are aware, only judicial requests will be possible in the future. This leads to **considerable problems in purely police-related cases**, as **no public prosecutor's office is involved in these**. This can lead to information deficits*."

As the practical application of the new rules is still to come, EU law enforcement officers have yet to experience any direct effect. Consequently, the responses collected largely replicate what was reported in the previous edition of this report.

Electronic evidence for law enforcement in non-EU countries

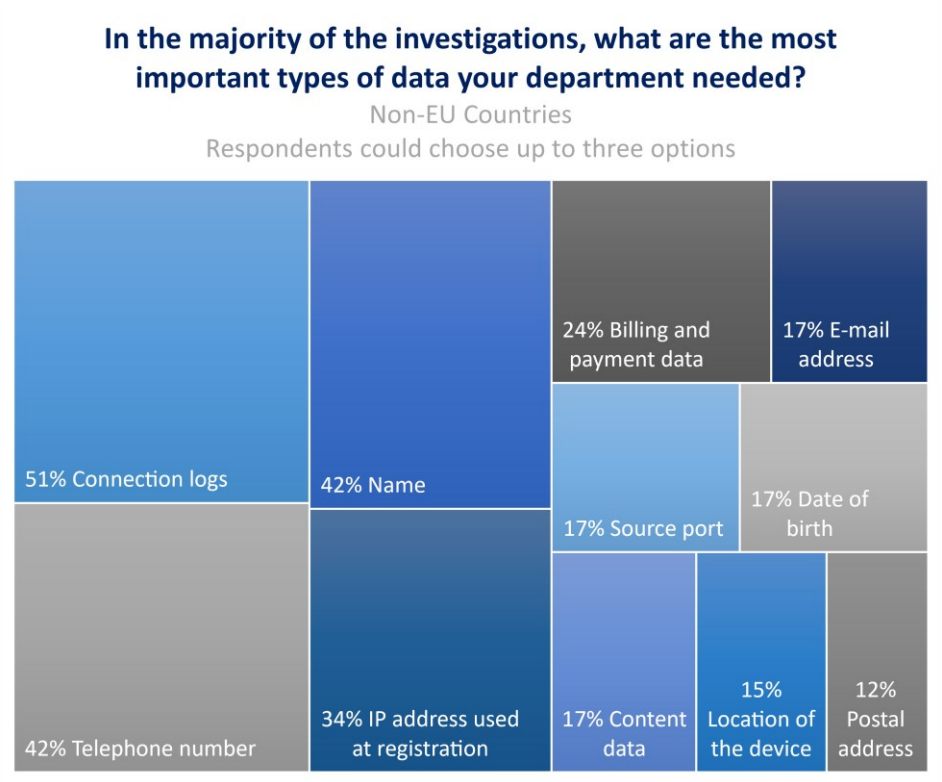
Law enforcement authorities from countries outside of the EU, with which Europol has operational or working agreements, were invited to reply to the same survey used to collect feedback from EU officers. A total of 60 responses were received from Albania, Bosnia and Herzegovina, Canada, Colombia, Iceland, Japan, Montenegro, Norway, Republic of North Macedonia, Serbia, Switzerland, Ukraine, and the United States of America.

In 2023, 78% of officers from non-EU countries reported being satisfied or more than satisfied with their department's engagement with service providers, compared to 71% in the EU.



Direct requests for disclosure of data under voluntary cooperation are the most important types of requests for respondents from non-EU countries; 53%, compared to 59% in the EU.

The most important types of data needed in criminal investigations are very similar for both EU and non-EU countries. Outside of the EU, connection logs (date, time and IP address of connection to an online service), names, phone numbers, and the IP address used at the moment of first registration to the service appear as the most important datasets for criminal investigations. It is worth noting that 17% of respondents have indicated that content data is one of the most important types of data in criminal investigations in non-EU countries (which is slightly higher than the result in the case of EU countries, 14%).



The three main issues encountered by non-EU law enforcement officers when submitting requests to foreign-based service providers in 2023 were almost the same as in the EU. The main issue is that the MLA process takes too long, followed by the

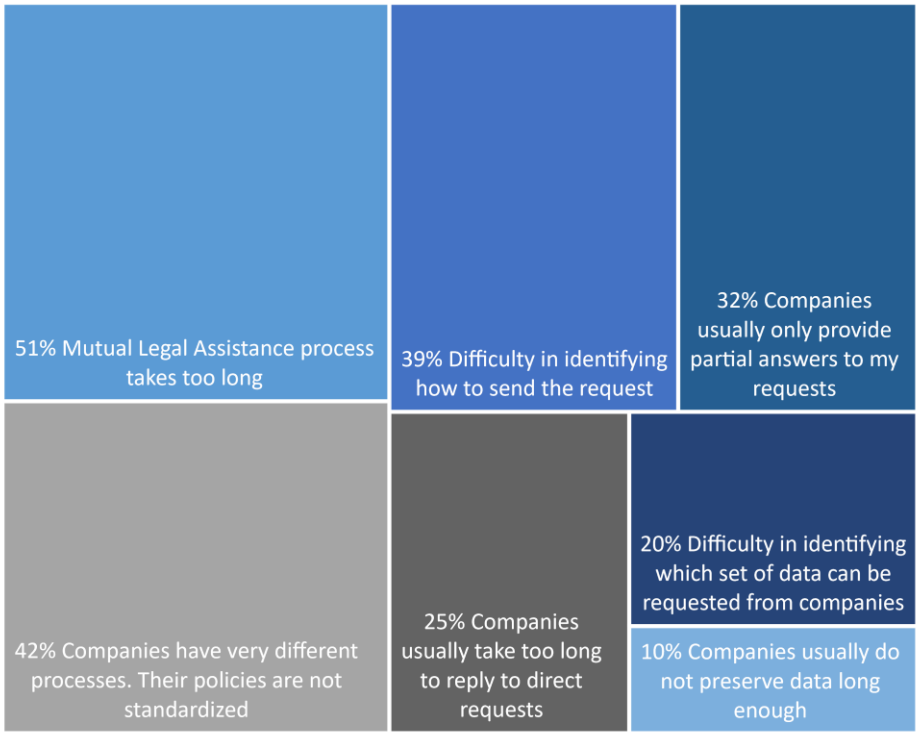
fact that service providers' policies are not standardised. The third issue mentioned the most by officers is the difficulty in identifying how to send their requests.

The similarity in the main issues encountered by law enforcement inside and outside the EU confirms the global nature of the challenges faced by competent authorities in the electronic evidence field. The results confirm that the existing MLA framework is unfit for the current reality of criminal investigations from a law enforcement perspective, and that the policies of service providers for responding to requests are still cumbersome.

What are the main issues your department encountered in requests to foreign-based service providers?

Non-EU Countries

Respondents could choose up to three options

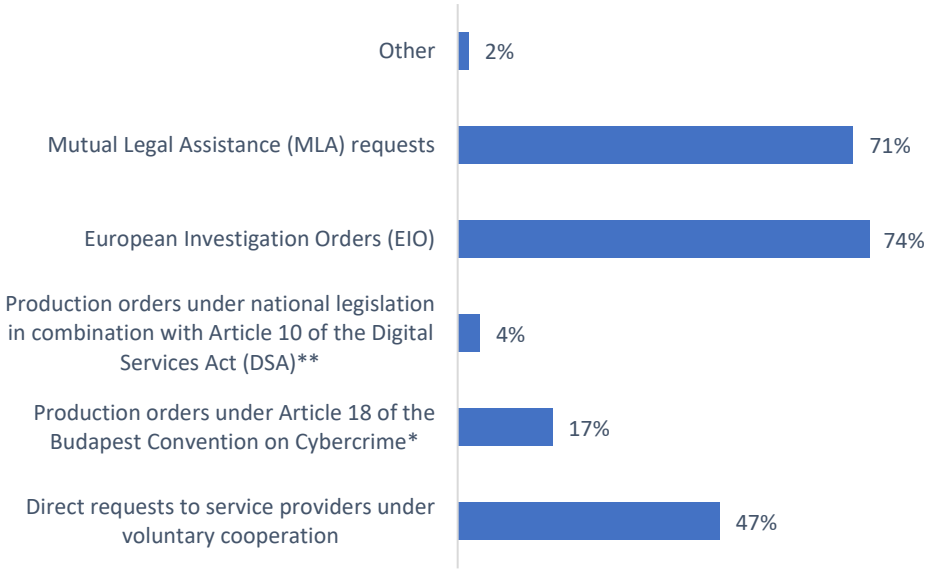


PERSPECTIVE OF JUDICIAL AUTHORITIES

Acquisition of electronic evidence across borders and challenges encountered

Among the various tools available for obtaining electronic data from service providers based abroad, traditional methods of cross-border cooperation in criminal matters — namely, MLA requests and the EIO — were the most preferred by EU judicial authorities surveyed in their criminal investigations in 2023. Specifically, 74% of the surveyed EU judicial authorities primarily used the EIO for acquiring data from service providers located abroad, followed closely by MLA requests, which were primarily used by 71% of the respondents. Direct requests to service providers under voluntary cooperation ranked as the third modality, primarily used by 47% of the respondents. Other tools, including production orders under national law in combination with Article 10 of the DSA or pursuant to Article 18 of the Budapest Convention, were indicated as preferred methods by a significantly lower number of surveyed authorities.

Which of the following modalities have you primarily used for acquiring data from service providers located abroad during your criminal investigations in 2023?



Extraterritorial powers: Production orders and requests with extraterritorial effects

In the modern digital landscape, with globally active service providers and data increasingly residing in cloud-based infrastructures, authorities can no longer easily establish the physical location of electronic evidence. Extraterritorial powers — domestic orders or requests with extraterritorial effects — are indispensable tools in a world where data can be stored and managed across multiple jurisdictions. These powers ensure that legal processes are not hampered by the geographical dispersal of electronic evidence. They allow competent authorities to request data from service providers regardless of the location of the data and, to some extent, regardless of the service provider's place of establishment, thus overcoming the limitations imposed by traditional notions of territoriality. While typically seeking limited sets of data (i.e. subscriber data or domain name registration information), these powers are vital for the effective investigation and prosecution of crimes in a digital context, enabling authorities to take the first steps and further their investigations.

As regards the availability of such extraterritorial powers, pending the application of the EU Electronic Evidence legislative package, EU judicial authorities were asked whether their national legal framework provides a legal basis for the issuance of:

- Production orders for data towards service providers located abroad, in possession or control of the sought information, following the model of Article 18(1)(b) of the Budapest Convention;
- Production orders for data towards service providers located abroad, in possession or control of the sought information, following the model of Article 7 of the Second Additional Protocol; and/or
- Requests for domain name registration information to service providers located abroad, in possession or control of such information, following the model of Article 6 of the Second Additional Protocol.

In this regard, EU judicial authorities from 21 out of the 25 EU Member States surveyed indicated that their national legislation provides a legal basis for the issuance of production orders following the model of Article 18 of the Budapest Convention. Furthermore, while the Second Additional Protocol has yet to enter into force, survey results indicate that 11 out of the 25 EU Member States surveyed already provide a legal basis for the issuance of production orders following the model of Article 7 of the Second Additional Protocol and 15 out of the 25 already provide a legal basis for the issuance of requests for domain name registration following the model of Article 6 of the Second Additional Protocol. At the same time, EU judicial authorities from three of the EU Member States surveyed indicated that their national legal framework does not provide a legal basis for the issuance of any type of orders or requests addressed to service providers located abroad, not even following the model of Article 18(1)(b) of the Budapest Convention (despite two of those three EU Member States being a Party to the Convention).

Some of the respondents shared additional explanations and/or direct references to their national legislation, as further set out in Table 1.

TABLE 1 – EU MEMBER STATES' LEGISLATION PROVIDING A LEGAL BASIS FOR THE ISSUANCE OF ORDERS OR REQUEST FOR DATA FROM SERVICE PROVIDERS LOCATED ABROAD	
Austria	*§ 135 StPO (Code of Criminal Procedure) – Seizure of Letters, Disclosure of Subscriber and Access Data, Disclosure of Data from a Communication, Localization of a Technical Device, Data Retention for Specific Reasons, and Surveillance of Communications* [18] *(1) Seizure of letters is permissible if it is necessary for the investigation of an intentionally committed crime that is punishable by more than one year of imprisonment.* *(1a) Disclosure of subscriber data and disclosure of access data are permissible if they appear necessary for the investigation of a concrete suspicion of a crime.* *(2) Disclosure of data from a communication is permissible:* *if and as long as there is an urgent suspicion that a person affected by the disclosure has abducted another person or otherwise taken control of them, and the disclosure is limited to data of such a communication that is presumed to have been sent, received, or transmitted by the accused at the time of the deprivation of liberty,* *if it is expected that this will aid the investigation of an intentionally committed crime that is punishable by more than six months of imprisonment and the owner of the technical device that was or will be the origin or target of a transmission of communications explicitly consents to the disclosure, or* *if it is expected that this will aid the investigation of an intentionally committed crime that is punishable by more than one year of imprisonment, and there are specific facts that suggest that this will help to identify data of the accused.* *if there are specific facts that suggest that this will help to determine the whereabouts of a fugitive or absent accused who is urgently suspected of an intentionally committed criminal act punishable by more than one year of imprisonment.* *(2a) Localization of a technical device is permissible in the cases of paragraph 2, items 1, 3, and 4 exclusively for the determination of the data mentioned in § 134, item 2a.* *(2b) Data retention for specific reasons is permissible if, based on an initial suspicion (§ 1 para. 3), it appears necessary to secure an order under paragraph 1a, second case, or under paragraph 2, items 2 to 4.* *(3) Surveillance of communications is permissible:* *in the cases of paragraph 2, item 1,* *in the cases of paragraph 2, item 2, provided that the owner of the technical device that was or will be the origin or target of a transmission of communications consents to the surveillance,* *if it appears necessary for the investigation of an intentionally committed crime that is punishable by more than one year of imprisonment, or if the investigation or prevention of crimes committed or planned within the framework of a criminal or terrorist organization (§§ 278 to 278b StGB) would otherwise be significantly hampered, and* *a. the owner of the technical device that was or will be the origin or target of a transmission of communications is urgently suspected of an intentionally*

	committed crime that is punishable by more than one year of imprisonment, or a crime under §§ 278 to 278b StGB, or *b. there are specific facts that suggest that a person urgently suspected of the crime (lit. a) will use the technical device or establish a connection with it;* *in the cases of paragraph 2, item 4.*
Belgium	*Article 46bis of the Code of Criminal Procedure (CCP), as interpreted by the Court of Cassation, allows a prosecutor or investigating judge to order a service provider to produce user information if said service provider offers its services directly to customers present on Belgian territory without a need for any physical or legal representation of the service provider on Belgian soil.*
Bulgaria	*Article 159a of the Bulgarian Criminal Procedure Code* *(1) Upon request by a court as part of court proceedings or based on motivated order by a judge of the respective court of first instance, issued by request of the supervising prosecutor of pre-trial proceedings the enterprises, providing public electronic communication networks and/or services shall make available the data, generated in the course of performance of their activities, which may be required for:* *1. tracing and identification of the source of the communication link;* *2. identification of the direction of the communication link;* *3. identification of the date, hour and duration of the communication link;* *4. identification of the type of the communication link;* *5. to identify the terminal equipment of the user or what purports to be a terminal equipment of the user;* *6. establishment of an identification code of the cells used.* *(2) The data under Paragraph 1 shall be collected where required for investigation of serious premeditated crimes.* *(3) The request of the supervising prosecutor under Paragraph 1 shall be substantiated and must certainly contain:* *1. information concerning the crime, for the investigation of which data concerning the traffic is required;* *2. description of the circumstances, on which the request is based;* *3. data regarding the individuals, for whom data concerning the traffic is required;* *4. a reasonable period of time to cover the information summary;* *5. the investigating authority, to which the data must be provided.* *(4) The court shall indicate in the order under Paragraph 1:* *1. data, which must be reflected in the information summary;* *2. a reasonable period of time to cover the information summary;* *3. the investigating authority, to which the data must be provided.* *(5) The time period, for which provision of the data under Paragraph 1 may be requested and authorised, shall not exceed 6 months.* *(6) If the information summary contains data, which is not related to the circumstances under the case and does not contribute to their clarification, upon motivated written request of the supervising prosecutor the judge, who*

	issued the authorisation, shall order the destruction of that material. The destruction shall be performed under procedure, approved by the Chief Prosecutor. Within 7 days of receipt of such order the enterprises under Paragraph 1 and the supervising prosecutor shall submit to the judge who issued it the protocols of destruction of the data.
The Netherlands	*Article 18 of the [Budapest] Convention is the basis for sending production orders for a customer's personal information. In the Netherlands, a police officer may send a production order for this type of data. The same possibilities apply to a police officer when he wants information from an ISP abroad. However, this is subject to the restriction that the production orders that we want to send abroad must have a basis in a treaty or customary international law. Article 18 of the Convention is considered as that legal basis in a treaty. Thus, this applies only to information as named in Article 18 [i.e. subscriber information].*
Slovenia	*Article 149č of the Criminal Procedure Act* *(1) If there are grounds for the suspicion that a criminal offence prosecutable ex officio has been committed or is being prepared for which the perpetrator is prosecutable ex officio and if, for the purpose of detecting, preventing or proving this criminal offence or detecting the perpetrator, it is necessary to obtain the subscriber data on the owner or the user of a particular communication medium or information service, or on the existence and content of its contractual relationship with the IT operator or information service provider regarding the performance of communication activities or information services, the court, state prosecutor or the police may request in writing that the IT operator or information service provider transmit such information even without the consent of the data subject. The written request must include the legal instruction referred to in paragraph two of this Article and an indication of the competent court. In the written request, the state prosecutor or the police must specify in detail the categories of requested subscriber data.* *(2) The IT operator or information service provider may, for substantiated reasons and at its own expense, submit the requested information together with a copy of the written request to the competent court instead of to the police or the state prosecutor. Upon receipt, the court shall verify the legality of the categories of information stated in the request. If the request also contains information other than subscriber data referred to in paragraph one of this Article or information that may not be transmitted pursuant to paragraph four of this Article, the received information shall be destroyed; otherwise, it shall be forwarded to the state prosecutor or the police. In the event of destruction, the investigating judge shall make an official note thereof which shall be sent to the IT operator or information service provider, the head of the competent district state prosecutor's office or the state prosecutor, the ministry responsible for supervising police work and the police.* *(3) The IT operator or information service provider may not disclose to its user, subscriber or third parties that it has or will transmit certain information in accordance with this Article. Such information may not be disclosed for 24 months after the end of the month in which the data were transmitted. In the event that the IT operator or information service provider receives a court order within this period that refers to the information obtained upon the request referred to in this Article, the period of the prohibited disclosure of that request shall be extended until the expiry of the time limit that might be set in the order received. By an order, the investigating judge or court may set a different time limit, extend it by a maximum of 12 months, but not more than twice, shorten the time limit or remove the prohibition on disclosure.*

	(4) Under this Article, it shall not be possible to request or obtain traffic data related to any identifiable communication, or data that must be obtained by processing data that can only be obtained pursuant to Articles 149b and 149c of this Act. Under this Article, it shall also not be possible to request or obtain data relating to the content of communication.
Slovakia	*Strictly within the meaning of Article 32(b) of the Budapest Convention on Cybercrime and within the meaning of the TC-Y Guidance Note on this issue.*
Sweden	*It was previously allowed only in Article 32(b) cases. But a new ruling from the Supreme Court issued on 30 March 2023 allows law enforcement to access data regardless where it is stored. As long as it can be done through authentication (i.e. login with username and password) the data can be obtained and used in court.*

As noted above, while awaiting implementation of new legal instruments such as the Second Additional Protocol and the Electronic Evidence Regulation, Article 10 of the DSA already establishes common rules for data disclosure orders directed at intermediary service providers in the EU.

It is important to note that Article 10 does not grant new powers to competent national authorities. Instead, it requires that data disclosure orders be based on already existing EU or national laws (such as, e.g., provisions implementing Article 18 of the Budapest Convention into national legislation). In addition to minimum requirements for orders, Article 10 also regulates language requirements, user notification, confidentiality, transmission of orders, and service providers' obligations.

Regarding the application of Article 10, the survey results indicate that only 4% of the EU judicial authorities surveyed have ever used this provision of the DSA, in combination with another EU or national law, to obtain data from service providers located abroad. Several factors could explain this outcome. Firstly, there may be a lack of awareness among competent authorities about the existence and applicability of Article 10. Secondly, as noted above, authorities appear to prefer other established methods for data acquisition, such as judicial cooperation, with which they are more familiar and in which they may have greater trust. Additionally, the novelty of the DSA might mean that procedures and best practices are still being developed. These factors highlight the importance of ongoing education and support to facilitate the effective use of Article 10, indicating a need for more comprehensive training and dissemination of information about the DSA's provisions.

Judicial cooperation

As highlighted by the survey's findings set out above, judicial cooperation instruments are essential tools for facilitating cross-border access to electronic evidence. Based on bilateral or multilateral treaties, these instruments enable competent authorities in one country to legally request and obtain electronic evidence stored by service providers based in another jurisdiction. To acquire data through judicial cooperation channels, EU Member States must issue an EIO for EU countries, excluding Denmark

and Ireland. For Denmark, Ireland, and any country outside the EU, an MLA process must be followed.

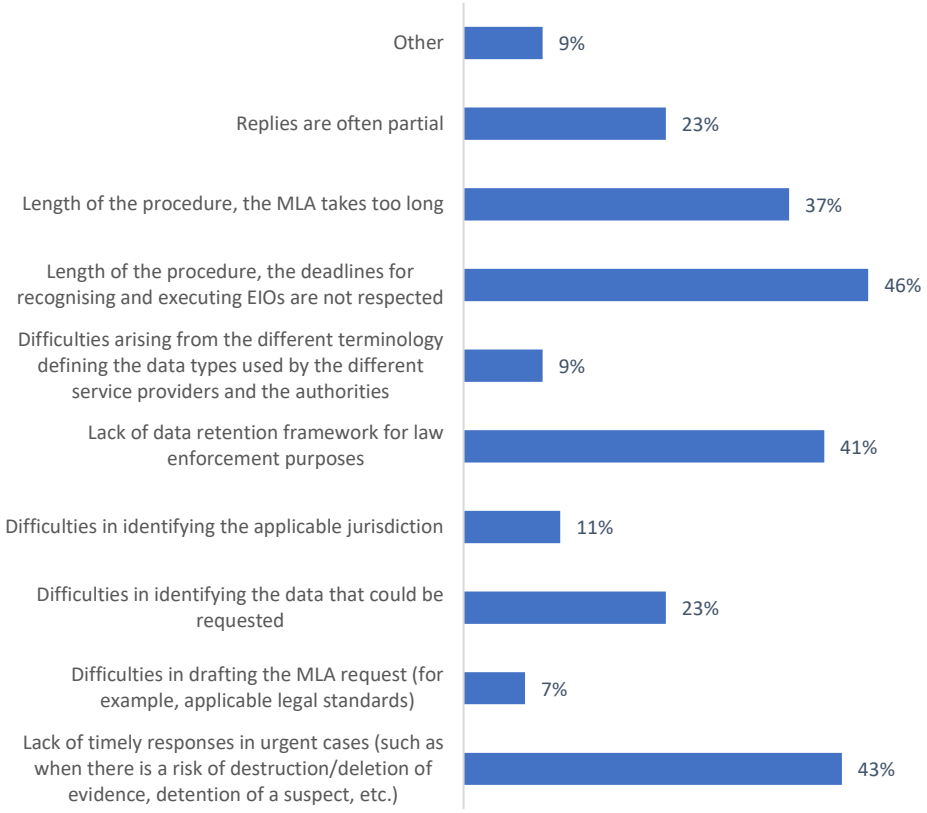
Although EIOs and MLA requests are the preferred methods among EU judicial authorities for obtaining electronic data, they present certain challenges. Neither process was specifically designed for electronic evidence, and the volatile nature of digital data further complicates matters. The effectiveness and efficiency of these instruments are crucial for the success of criminal investigations and prosecutions. While awaiting the application of additional legal tools, EU judicial authorities identified the main challenges they faced in obtaining electronic data through judicial channels in 2023, both within the EU and from countries outside the EU.

Challenges related to the EIO/MLA process towards EU Member States

Regarding the EIO/MLA process towards other EU Member States, the most pressing challenge highlighted by respondents was the lengthy procedure. Specifically, 46% of respondents noted that deadlines for recognising and executing EIOs are not always respected, and 37% mentioned that the MLA process takes too long. While the findings of previous reports primarily highlighted delays associated with the MLA process, there has been a noticeable shift in concern towards the challenges related to the execution of EIOs, which are increasingly seen as more significant. These delays are critical as they impact the timely securing of electronic evidence. Additionally, 43% of respondents cited the lack of timely responses in urgent cases, and 41% pointed to the absence of a data retention framework for law enforcement purposes. These were ranked among the three most prevalent problems encountered in their investigations in 2023. Other issues reported with a lower prevalence concern:

- Difficulties in identifying the data that could be requested: 23%
- Replies received are often partial: 23%
- Difficulties in identifying the applicable jurisdiction: 11%
- Difficulties arising from the different terminology used by the different service providers and the authorities defining the data types: 9%
- Difficulties in drafting the MLA request (for example, applicable legal standards): 7%
- Other: 9%

What have been, in your experience in 2023, the three main problems with the EIO/MLA process towards EU Member States?



Additional information regarding the issues related to obtaining electronic evidence via judicial cooperation channels from other EU Member States was provided by two of the respondents:

- Obtaining a preservation reference number from SPs located in Ireland/fulfilling the data location requirements for the Irish Central Authority for Mutual Assistance. (Austria)
- A combination of the applicable jurisdiction and legal possibilities in requested countries, such as identifying the (true) location of data. Once it is clear that the data is being held within the borders of the requested EU Member State, the possibilities of local law enforcement to obtain the requested information might be limited. (Netherlands)

Challenges related to the MLA process towards countries outside the EU

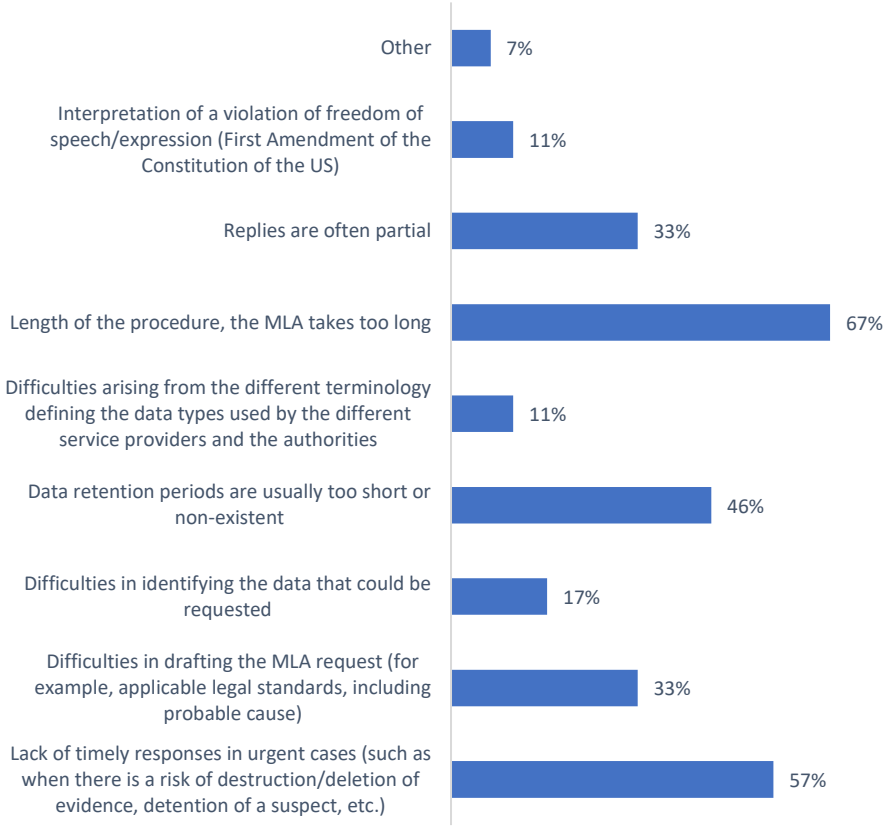
Regarding judicial cooperation for obtaining electronic evidence from countries outside the EU, the length of the procedure remains the most challenging issue encountered in criminal investigations in 2023. This issue, consistent with findings from previous years, was highlighted by 67% of respondents. Additionally, the lack of

timely responses in urgent cases (57%) and the short or non-existent data retention periods (46%) were identified as other major problems. These same issues have been emphasised by representatives of the EU judiciary in previous editions of this report, proving them to be recurring and long-standing challenges for EU authorities.

Other challenges reported with a lower prevalence are:

- Difficulties in drafting the MLA request: 33%
- Replies received are often partial: 33%
- Difficulties in identifying the data that could be requested: 17%
- Difficulties arising from the different terminology used by the different service providers and the authorities: 11%
- Interpretation of a violation of freedom of speech/expression (First Amendment of the Constitution of the US): 11%
- Other: 7%

What have been, in your experience in 2023, the three main problems with the MLA process towards third states (i.e. non-EU Member States)?



Further information regarding the problems related to the MLA process towards countries outside the EU was reported by two of the respondents:

- Certification/Statements are not provided with the evidence; legislative obligations in the requested country to inform the data subject. (Ireland)

- The possibilities of law-enforcement might be limited or the threshold for obtaining the requested data/information might be quite higher compared to the requesting country. (Netherlands)

Looking ahead: Navigating solutions and addressing challenges

Comparing this year's survey results with information from previous editions of this report reveals a consistent pattern among the surveyed EU judicial practitioners. While judicial assistance constitutes the main modality for legally obtaining electronic evidence across borders, the predominant issues highlighted in recent years concern:

- The length of the process (both within and outside the EU);

- The lack of a data retention regime for law enforcement purposes; and

- The lack of timely responses in urgent cases (such as when there is a risk of destruction/deletion of evidence, detention of a suspect, etc).

The evolving legislative landscape concerning access to electronic evidence aims to address and resolve some of these long-standing challenges faced by EU judicial authorities. The upcoming EU Electronic Evidence legislative package and the Second Additional Protocol are expected to enhance the efficiency of obtaining electronic evidence, addressing the inefficiencies of the current judicial cooperation process and delays in urgent cases.

The European Production Orders and European Preservation Orders introduced by the EU Electronic Evidence Regulation promise to provide a more streamlined and expedited procedure compared to the existing EIO and MLA processes. Clear deadlines for service providers to respond to these orders are anticipated to significantly improve the timeliness of obtaining electronic evidence, including in urgent cases. Additionally, the EU Electronic Evidence Directive mandates that service providers offering services in the EU have an establishment or representative within the EU, regardless of their location. This requirement is expected to facilitate the appropriate direction of European Production Orders and European Preservation Orders to service providers, thereby expediting the process and reducing jurisdictional complexities that often delay MLA and EIO processes.

While the EU Electronic Evidence legislative package will primarily benefit EU Member States, the Second Additional Protocol will provide a new global framework, assisting authorities in engaging with service providers outside the EU's jurisdiction. Key provisions – particularly Articles 6 and 7, which establish a legal basis for authorities to obtain domain name registration information and subscriber data from entities providing domain name registrations services and service providers based in any other Party to the Protocol – may become crucial for investigations requiring data from entities and service providers not covered by the novel EU legislation. In addition, among other provisions, the Second Additional Protocol also aims to enhance

cooperation between competent authorities themselves when obtaining electronic evidence in emergency circumstances, as outlined in Article 9 (Expedited disclosure of stored computer data in an emergency) and Article 10 (Emergency mutual assistance).

Unlike the EU Electronic Evidence Regulation, the Second Additional Protocol lacks specific deadlines for inter-authority cooperation and enforcement mechanisms for cooperation with service providers. Nevertheless, these legal developments are set to enhance the toolbox available to competent authorities, as well as simplify and expedite access to electronic evidence, providing much-needed solutions to some of the most pressing challenges faced by judicial authorities.

However, these novel legal frameworks will not address one of the key challenges identified by EU judicial authorities – the absence of a data retention framework for law enforcement purposes.

Data retention

Data retention involves service providers storing data for a specific period, as long as necessary to deliver services and for legitimate business purposes such as invoicing, fraud prevention, and enhancing user safety and security. Service providers may also retain data to comply with legal obligations like tax and audit regulations.

Service providers can also be legally required to retain data for law enforcement purposes, enabling access by authorities for criminal investigations and proceedings. Since the invalidation of the Data Retention Directive [(19)] by the Court of Justice of the European Union (CJEU or Court) in 2014, data retention is governed by national laws within the framework of Article 15(1) of the E-Privacy Directive [(20)], as interpreted by the CJEU in light of relevant provisions of the EU Charter of Fundamental Rights (Charter) and the Treaty on the EU. The CJEU has developed consistent jurisprudence, establishing conditions for lawful data retention and access under EU law [(21)].

In 2024, the CJEU issued two judgments which are of relevance for the topic of data retention and/or access to retained data.

In Case C-178/22 – *Procura della Repubblica presso il Tribunale di Bolzano*, the Court provided key rulings regarding access to traffic and location data retained by providers of electronic communications services, consisting of details of incoming and outgoing communications as well as location data, which can enable precise conclusions to be drawn as to the individuals' private lives. The main findings of the Court are as follows:

- Conditions for access: Access to traffic and location data, which may allow precise conclusions to be drawn concerning the private life of a user, retained by a provider of electronic communications services, can only be granted in connection with individuals suspected of being implicated in a serious offence;
- Definition of 'serious offences': It is up to the EU Member States to define what constitutes 'serious offences. However, they must not distort this concept (and, by extension, the concept of 'serious crime'), by including offences that are clearly not serious in the context of their societal conditions;

- Prior review requirement: To ensure the concept of 'serious crime' is not misinterpreted, any access to retained data that could significantly interfere with fundamental rights must be subject to prior review by a court or an independent administrative body. This reviewing body must have the authority to refuse or restrict access if the fundamental rights interference is deemed serious and the offence does not qualify as a serious crime given the societal conditions. This ensures a fair balance between the needs of the investigation and the fundamental rights to privacy and protection of personal data.

In Case C-470/21 – *La Quadrature du Net and Others*, the Court provided key rulings regarding the retention of and access to personal data for combating online counterfeiting, especially concerning IP addresses and civil identity data. The main findings of the Court are as follows:

- General retention of IP addresses: The CJEU ruled that EU Member States can impose obligations on internet access providers to retain IP addresses in a general and indiscriminate manner for combating criminal offences, provided that such retention does not allow precise conclusions to be drawn about individuals' private lives. This can be achieved by ensuring a strict separation of IP addresses from other categories of personal data (such as civil identity data and traffic and location data). Moreover, the data can be retained only for a period not exceeding what is strictly necessary.

- Access to civil identity data: The Court found that EU law does not preclude national legislation authorising competent public authorities to access civil identity data associated with retained IP addresses. This access must serve the sole purpose of identifying individuals suspected of committing criminal offences and must be regulated to prevent drawing precise conclusions about their private lives. Officials accessing this data must be prohibited from disclosing the content of the files consulted (except for the sole purpose of referring the matter to the public prosecution service) or using the data for purposes other than identification.

- Conditions for access: The Court emphasised that prior review by a court or an independent administrative body is not required when accessing civil identity data solely for identification purposes, as this does not constitute a serious interference with fundamental rights. However, if the national procedure allows linking data in a way that could draw precise conclusions about an individual's private life, such access must be subject to prior judicial or independent administrative review.

- Retention and access safeguards: The data retention and access system must be subject to regular reviews by a body independent from the public authority using the data processing system. This review is intended to ensure the system's integrity, effectiveness, and reliability in detecting potential offending conduct.

Despite the CJEU's clear guidelines on data retention for law enforcement purposes and regarding access to such data, the lack or limited scope of such frameworks in the EU Member States remains a significant challenge for EU judicial authorities when seeking data from other jurisdictions.

As noted above, recent legal developments will enhance the tools available to authorities for cross-border data requests. However, effective access to electronic data by competent authorities depends on its availability. Thus, there remains a pressing need for EU-wide legislative measures to harmonise data retention specifically for this purpose. This matter is well-illustrated by a quote from the Estonian State Prosecutor-General, Andres Parmas:

> Large international corporations collect the same data on a daily basis that law enforcement agencies are increasingly being restricted from collecting and accessing. In the case of private companies, it is often unclear who collects, uses, and shares various personal data, on what basis, and for what purpose. However, when the state seeks to use this same data to protect victims of crime and to address injustices done to them, various counter-arguments arise.

Implications of cost reimbursement

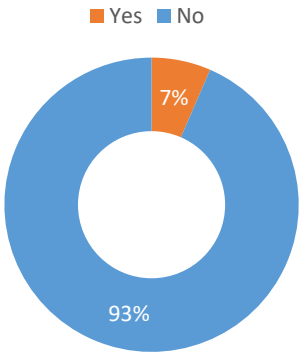
In addition to posing certain challenges for authorities in accessing such data, the increasing demand for electronic data in criminal investigations and proceedings also imposes additional financial burdens for service providers and/or national authorities seeking access to such data. Furthermore, the fragmented legal framework, which includes EU Member States' national legislation and international and EU legislation governing cross-border access to electronic evidence, along with service providers' internal policies, can complicate determining responsibilities for cost reimbursement. Competent authorities strive to fulfil their investigative duties without unduly burdening their budgets.

In some jurisdictions (e.g. Austria, Belgium, Czechia, Germany), the national legal framework provides for the reimbursement of costs incurred by service providers in responding to request from authorities. In other jurisdictions, such provisions may not exist (e.g. Finland, Greece, Italy, Slovenia) or the national legal framework may even require service providers to comply with requests at their own expense (e.g. Estonia, Hungary, Poland). This legal fragmentation could make determining who bears the costs of accessing electronic evidence a critical consideration for requesting authorities when choosing the legal framework for their requests. For instance, the EU Electronic Evidence Regulation includes provisions on cost reimbursement for service providers, linking it to whether such reimbursement is allowed under the national law of the issuing authority in each specific case. In contrast, the Second Additional Protocol does not include any provisions on cost reimbursement.

At present, the reimbursement of costs associated with complying with requests from authorities does not significantly impact access to electronic evidence. Service providers generally refrain from seeking compensation for providing information. The results of the survey confirm that only 7% of the respondents encountered a situation where a service provider requested reimbursement for costs associated with

responding to requests for data. The vast majority of the respondents (93%) indicated they had never received such a claim for compensation, underscoring the limited impact of service providers' expenses on the data retrieval process.

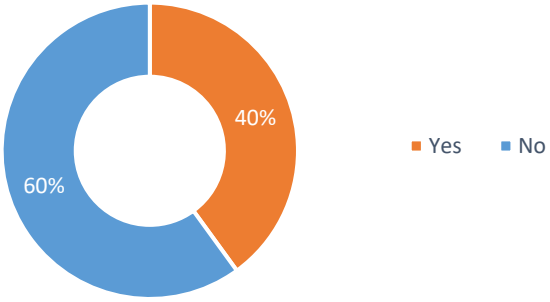
In relation to your requests for data from service providers located abroad in 2023, have you ever encountered a situation where the service provider requested reimbursement of the associated costs?



However, this situation may change with the application of the Electronic Evidence Regulation, which imposes strict time limits for compliance—10 days for standard requests and 8 hours for emergencies. Meeting these timelines may require additional resources, including dedicated personnel and technological investments, thereby increasing costs for service providers. The Regulation stipulates that service providers can seek reimbursement for the costs incurred in complying with European Production Orders and European Preservation Orders, provided such reimbursement is permissible under the national laws of the issuing state. The diverse legal frameworks across EU Member States may complicate the reimbursement process, contributing to financial uncertainty for service providers as they navigate different national laws to determine eligibility for cost reimbursement.

The feedback received from judicial authorities indicates that the majority of the EU Member States surveyed (15 out of 25) do not currently have national rules in place for cost reimbursement. In the context of the application of the Electronic Evidence Regulation, this means that service providers will not be able to claim reimbursement for costs incurred while complying with European Preservation and Production Orders issued by the majority of EU Member States.

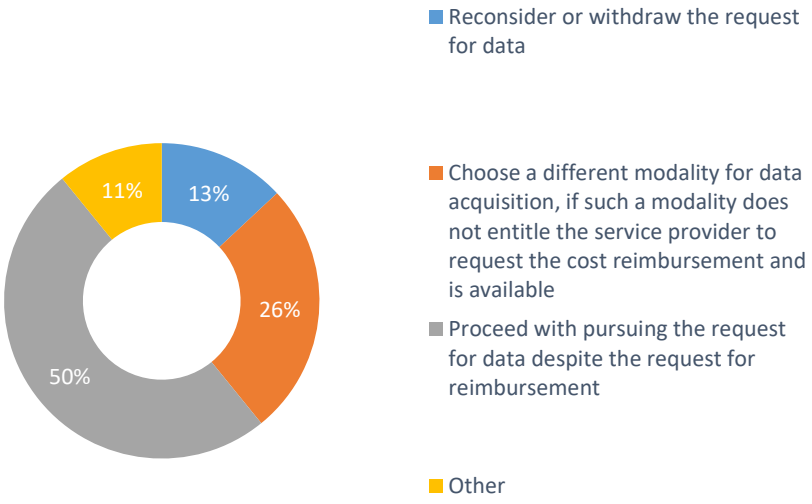
Does your country have a cost reimbursement system for private entities in place, in case they provide data upon official request?



Furthermore, the potential for "legal venue shopping" by requesting authorities seeking to minimise costs may further complicate the landscape. Authorities may opt to issue requests under legal frameworks that impose fewer financial obligations on them, potentially resulting in inconsistent application of the law and unequal financial burdens on service providers.

According to the results of the survey, should service providers seek reimbursement for costs incurred in data production, 26% of respondents would prefer data acquisition methods that do not allow service providers to seek cost reimbursement. Additionally, 11% of the respondents indicated they would reconsider or withdraw their data requests, especially if the associated costs were deemed too high with no alternative options available.

If, during the process of making a request for data from a service provider located abroad, the service provider would ask for the reimbursement of the costs incurred for the production of data, what would be your response?

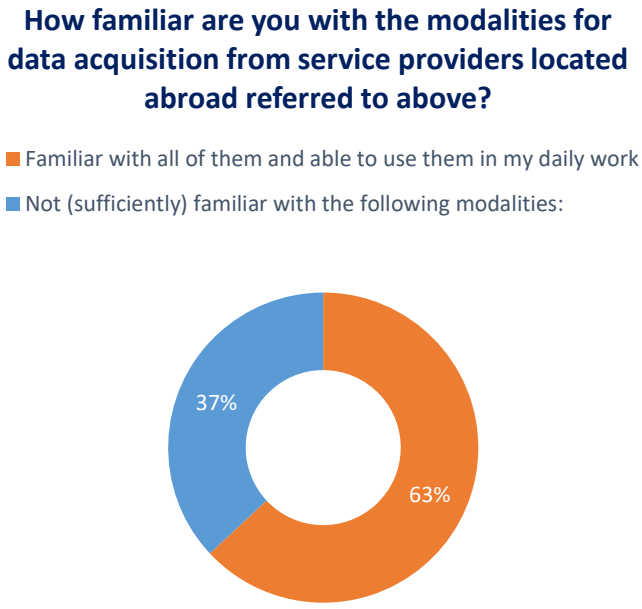


The need for expanding knowledge and capacity

As technological advancements and digital transformations continue to shape criminal activities, judicial authorities must remain adept in navigating the complexities of electronic evidence. This includes understanding the various legal frameworks and the available legal instruments for cross-border access to electronic evidence, including MLA, EIO, production orders under Article 18 of the Budapest Convention, direct requests to service providers under voluntary cooperation, as well as preparing for future legislative developments in this field.

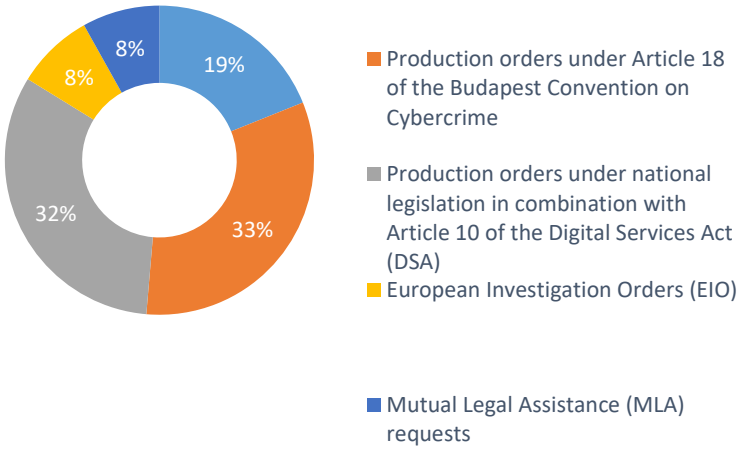
In this regard, EU judicial authorities were surveyed on their familiarity with the existing modalities for acquiring data from service providers located abroad. The results suggest that a significant portion of EU judicial authorities may not be well-versed in the specific provisions of the current legal instruments, potentially hindering their effective application. Specifically, 37% of the respondents reported that they are either not familiar or not sufficiently familiar with the following cross-border data acquisition modalities:

- MLA requests (8% of the respondents);
- EIO (8% of the respondents);
- Direct requests to service providers under voluntary cooperation (19% of the respondents);
- Production orders under Article 18 of the Budapest Convention on Cybercrime (32% of the respondents);
- Production orders under national legislation in combination with Article 10 of the DSA (33% of the respondents).



Examining the matter more closely, 33% of respondents identified production orders under Article 18 of the Budapest Convention and 32% pointed to production orders under national legislation combined with a newly available Article 10 of the DSA as requiring increased knowledge and capability among EU judicial authorities. This ties in with the results from the question on the modalities predominantly used by authorities in their investigations in 2023, indicating that these two methods for obtaining data are less frequently employed by competent authorities for acquiring data from service providers located abroad compared to judicial assistance and direct requests under voluntary cooperation. Insufficient familiarity with these methods may lead authorities to underutilise them effectively. Conversely, the lack of utilization due to unfamiliarity can perpetuate a cycle of inadequate knowledge among judicial authorities, where potentially valuable tools are overlooked. Therefore, enhancing familiarity and capability with these modalities is essential to broaden the toolkit available for accessing electronic evidence across borders.

Not (sufficiently) familiar with the following modalities:

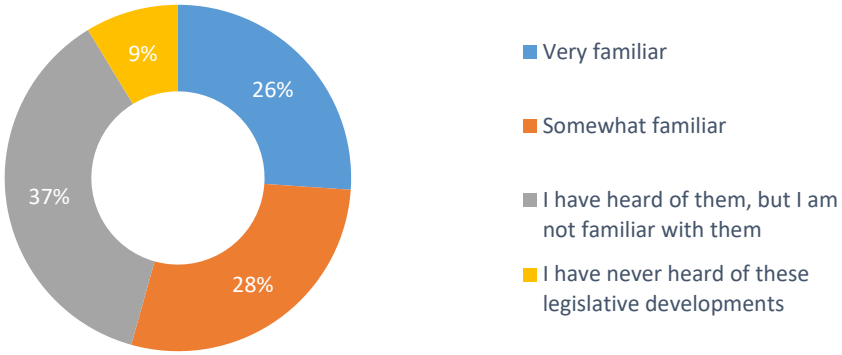


Looking ahead, as legislative changes reshape the landscape of cross-border access to electronic evidence, it is crucial to prepare judicial authorities for new instruments that enhance efficiency in this area. The new legal instruments will provide important additional tools to access electronic evidence across borders more efficiently. However, effective navigation of these frameworks will depend on equipping judicial authorities with essential knowledge and skills.

Assessing the awareness of EU judicial authorities regarding the evolving legal landscape of cross-border access to electronic evidence, respondents were asked about their familiarity with the recent legislative developments. The results of the survey indicate that the majority of respondents (37%) have heard of the EU Electronic Evidence legislative package and the Second Additional Protocol, but are not familiar with them. Another 28% indicated having some knowledge of these new pieces of legislation. On a more positive note, 26% of respondents reported being very familiar

with these novel pieces of legislation, while only 4% indicated never having heard of these legislative developments.

How familiar are you with the EU Electronic Evidence legislative package and the Second Additional protocol to the Budapest Convention on Cybercrime?



Additionally, some respondents provided further insights regarding legislative changes and their expected impact on their daily work:

- The trainings on the new instruments for collecting e-evidence would be the most useful. (Bulgaria)
- The new EU [Electronic Evidence] Regulation is known to the experts of the public prosecutor's office in the Netherlands. Preparations are being made to approach ISP's directly on that basis and also to request production of the content available at those ISP's (if that is possible). But the Regulation is not widely known yet. Even the SPoC has yet to prepare in order to require data from the major ISPs on that basis. Right now, there is still a lot of ambiguity as to what is the difference in scope between the DSA and the [Electronic Evidence] Regulation. More education about the differences and possibilities between those two instruments is much appreciated. (Netherlands)
- Both the EU Electronic Evidence package and the Second Additional Protocol require domestic measures of implementation: that is, they cannot merely apply automatically when entering in force. EU MSs need support in this process and the SIRIUS project could do it. (Portugal)

The results of the survey and the insights from EU judicial authorities underscore the urgent need to enhance knowledge and capacity among EU judicial authorities as legal frameworks evolve to address challenges in obtaining electronic evidence. Effective navigation of cross-border access requires thorough understanding of existing tools and readiness to leverage new legal instruments under forthcoming legislative

changes. Ensuring judicial authorities are well-informed and prepared is crucial for facilitating efficient and effective access to electronic evidence across borders.

Building on its established role as a pivotal resource for authorities from the EU Member States, the SIRIUS Project will play a crucial role in supporting them as they prepare for and implement the new EU Electronic Evidence legislative package and the Second Additional Protocol. By focusing on knowledge and capacity building activities, SIRIUS will enhance awareness and understanding among judicial and law enforcement entities regarding these new legal instruments. This will include the development of practical tools and guidelines tailored to the implementation of the EU Electronic Evidence Regulation, as well as awareness raising about the Second Additional Protocol.

The European Judicial Network approach - Transmission of Electronic Evidence via the e-EDES Platform

The Role of e-EDES in the New Framework

Based on e-CODEX, the Commission initiated the development of the e-Evidence Digital Exchange System (e-EDES) in 2016 to support digital exchanges of EIOs, MLA forms and Interception of Telecommunication Notifications (ITNs). Launched in a pilot mode in May 2022, 11 Member States (AT, BE, DE, ES, FR, HU, LU, LV, PT, PL, SI) and 191 national judicial authorities have joined the digital exchange. The platform is scheduled to be fully operational for transmitting EIOs, MLA requests and ITNs between all Member States by 2028. Additionally, it is anticipated that it will be used for transmitting European Production or Preservation Order Certificates (EPOC and EPOC-PR) from 18 August 2026.

When fully operational, e-EDES will be the mandated platform for transmitting electronic evidence within the EU. However, the EJN Contact Points have already taken into consideration potential practical issues with this inflexible approach:

- **Technical or Other Barriers**: Situations may arise where using e-EDES is impossible. How will practitioners send electronic evidence, especially in urgent cases
- **Legal and Technical Constraints**: Challenges in sending evidence via e-EDES could exist
- **Training Needs**: Ensuring all practitioners are trained, particularly in larger countries, could be problematic before e-EDES is launched.

A more flexible approach to e-EDES usage, including exceptions, is considered necessary to address those circumstances. The platform's potential should also be fully utilised. For instance, integrating a videoconference application into e-EDES could resolve compatibility issues. Broadening the scope of legal instruments transmitted via e-EDES would enhance coordination between executing authorities, ensuring awareness of related requests within the same investigation. Additionally, the platform should enable user-friendly extraction of statistical data.

In particular, EJN legal experts have identified several concerns and key issues regarding the transmission of electronic evidence through the e-EDES platform [22]:

Enhancing Flexibility and Usability

Flexible Use and Exceptions: While e-EDES is set to become the standard for electronic evidence transmission, it is crucial to build in flexibility to accommodate various practical scenarios. Exceptions should be permitted when technical failures or other significant issues prevent the use of e-EDES. This flexibility ensures that evidence can still be transmitted promptly, maintaining the integrity of investigations.

Training and Implementation: Comprehensive training programs are essential for the successful implementation of e-EDES. These programs should be tailored to the needs of different Member States, taking into account their particular national structures, size and the volume of cases they handle. Training should not only cover the technical use of the platform but also the legal implications and procedural requirements. This ensures that all practitioners, regardless of their prior experience with digital platforms, can effectively use e-EDES.

Leveraging e-EDES for Videoconferencing

One of the significant benefits of e-EDES is its potential to support videoconferencing, which is becoming increasingly important for cross-border judicial cooperation. Currently, the lack of compatibility between different videoconferencing systems is a major hurdle. By integrating a standardised videoconferencing application within e-EDES, practitioners across the EU could seamlessly conduct remote hearings, witness testimonies and other judicial proceedings. This integration would enhance efficiency and reduce the logistical challenges associated with physical appearances.

Expanding e-EDES Functionality

Broader Legal Instrument Scope: Expanding the range of legal instruments that can be transmitted via e-EDES would improve coordination and streamline processes. Including more instruments would allow for better management of related cases and reduce the risk of uncoordinated actions by different authorities within the same Member State. This holistic approach would support more efficient and cohesive judicial cooperation.

Statistical Data Extraction: Efficient extraction and analysis of statistical data from e-EDES could significantly enhance the operational insights for judicial authorities. By making this feature user-friendly, authorities can easily monitor trends, identify bottlenecks and assess the effectiveness of cross-border cooperation. This data-driven approach would facilitate continuous improvement of the judicial processes.

Advanced Integration with EJN Resources

The current architecture of e-EDES involves redirecting users to the EJN Atlas on the EJN website to identify competent authorities. To streamline this process, a more advanced integration is recommended. Direct access to the EJN Atlas from within e-EDES would eliminate the need for multiple web pages, making the system more user-

friendly. Additionally, integrating links to resources such as the Fiches Belges and EJN Contact Points related to the receiving authority would provide valuable context and support to practitioners.

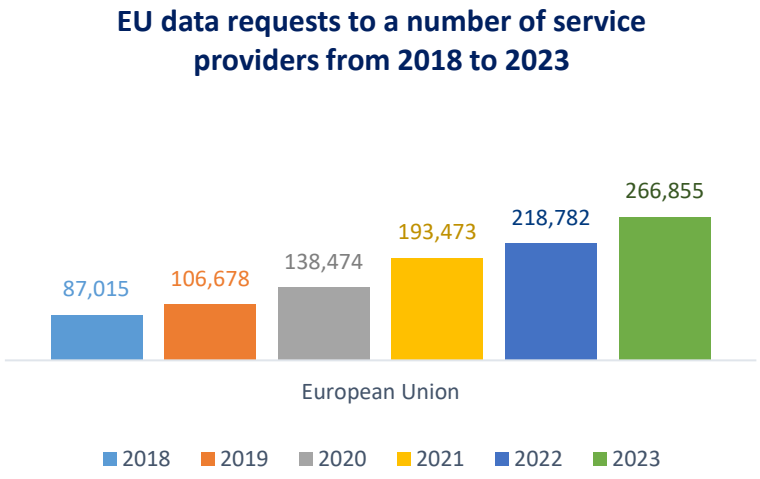
Conclusion

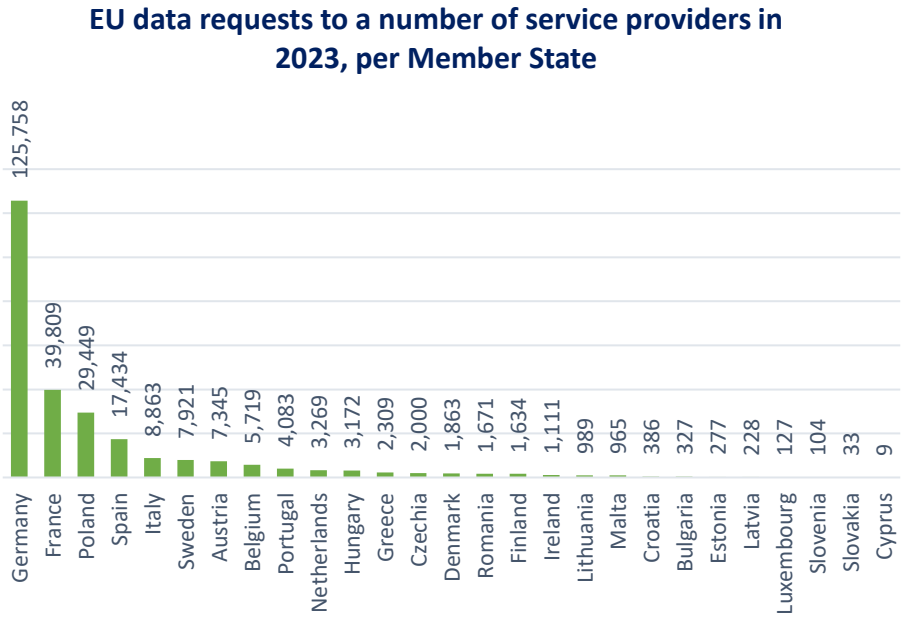
The e-EDES platform represents a significant step forward in harmonising the transmission of electronic evidence across the European Union. By addressing the current fragmented legal framework and providing a standardised approach, e-EDES has the potential to enhance efficiency and cooperation in judicial processes. However, to fully realise and harness this potential, it is essential to build in flexibility, provide comprehensive training, integrate videoconferencing capabilities, expand the scope of legal instruments, and strengthen connections with existing EJN resources. These enhancements will ensure that e-EDES not only meets the current needs of judicial authorities but also adapts to future challenges and technological advancements.

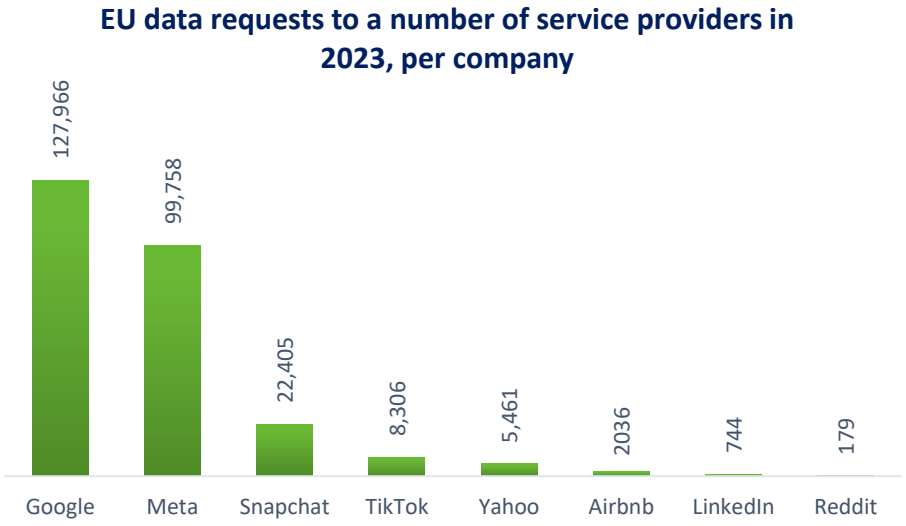
PERSPECTIVE OF SERVICE PROVIDERS

Volume of data requests per country and per service provider

The volume of data disclosure requests submitted by EU competent authorities to eight service providers increased by 22% from 2022 to 2023. Last year, 266,855 requests were submitted to Airbnb, Google, LinkedIn, Meta, Reddit, Snapchat, TikTok and Yahoo. This is the result of the analysis of transparency reports published by the service providers themselves [23]. In 2023, Germany submitted the highest amount of request in the EU (125,758), followed by France (39,809). Combined, they account for more than 60% of requests submitted in 2023 to the eight providers considered. Among the service providers analysed, Google was the one that received most of the requests, followed by Meta.







As reported above, 5% of EU law enforcement surveyed stated that requests pursuant to Article 10 of the DSA, in combination with a legal basis under EU or national law, were the most used instrument to directly engage with foreign service providers. It is worth prefacing that DSA-related data from service providers' transparency reports does not provide a complete picture of the year 2023 as, depending on the services considered, providers selected different reporting periods in line with their obligations under the DSA [(24)]. Nevertheless, the reports indicated that, from 25 April to 30 September 2023, a total of 13,042 orders pursuant to Article 10 of the DSA were submitted to the four services considered for the purposes of this report, namely

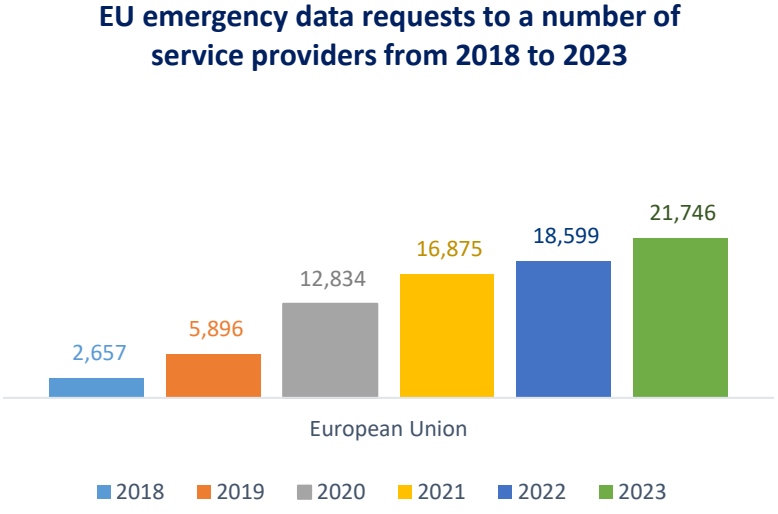
Facebook and Instagram [25], TikTok, Snapchat, and LinkedIn. Furthermore, during their respective reporting periods, Google indicated not having received any such order.

Although the systematic comparison between orders under Article 10 of the DSA and the total volumes of requests received from EU authorities seems at this stage improper, the qualitative feedback collected from the service providers interviewed in the preparation of this report offers some insights. The providers shared how different interpretations of Article 10 of the DSA generally affect the gathering of statistics. Some providers consider DSA obligations as additions to current practices or requirements applicable to voluntary cooperation and, consequently, will count orders under Article 10 of the DSA as part of their global transparency reports. Others, conversely, will produce separate reporting.

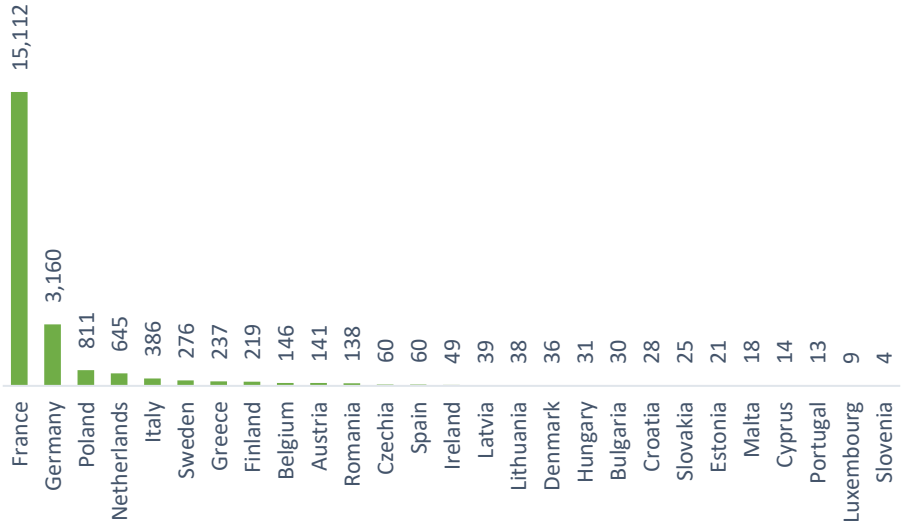
While some providers were able to estimate the volume of orders under Article 10 of the DSA as amounting to 15% of the total requests received in 2023, others were yet to experience any impact. Others, finally, expect any DSA-related volumes of orders to be minimal given that they already voluntarily comply with requests for data disclosure in a number of EU jurisdictions.

Volume of Emergency Disclosure Requests per country and per service provider

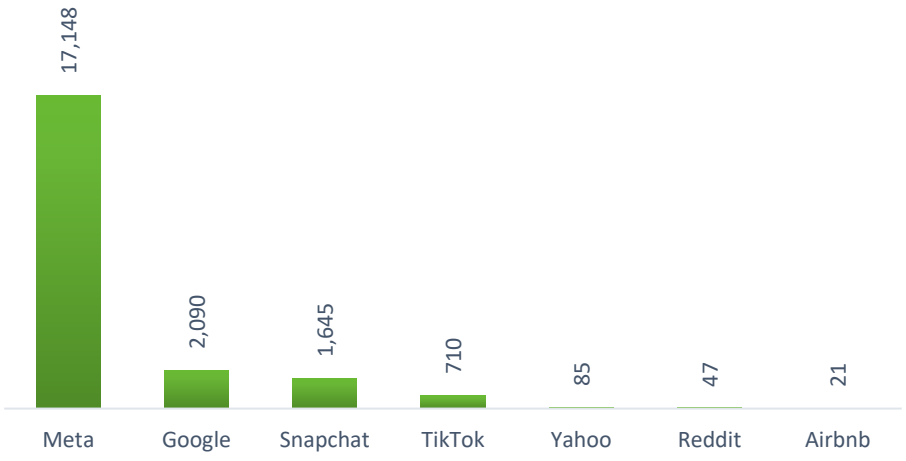
Emergency circumstances usually constitute situations where there is imminence of harm or serious physical injury to any person. Some service providers adopt a wider definition of emergencies to include imminent and serious threat to the security of a State, the security of critical infrastructure or installation or crimes involving minors. From 2022 to 2023, the volume of Emergency Disclosure Requests issued by EU competent authorities increased by 17%, to 21,746, considering data from eight service providers [26]. The majority of the requests were submitted by France (15,112) and the provider that received the highest amount was Meta.



EU emergency data requests to a number of service providers in 2023, per Member State



EU emergency data requests to a number of service providers in 2023, per company



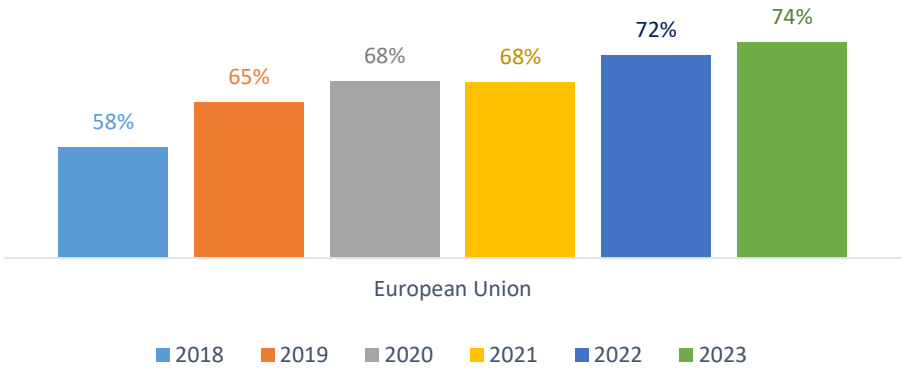
Success rate of EU cross-border requests for electronic evidence

The average success rate of data disclosure requests submitted by EU competent authorities increased by 2% from 2022 to 2023, a constant positive trend since the first edition of this report. The average EU success rate at 74% is the best result since the first edition of this report (created using data from 2018). 15 Member States have

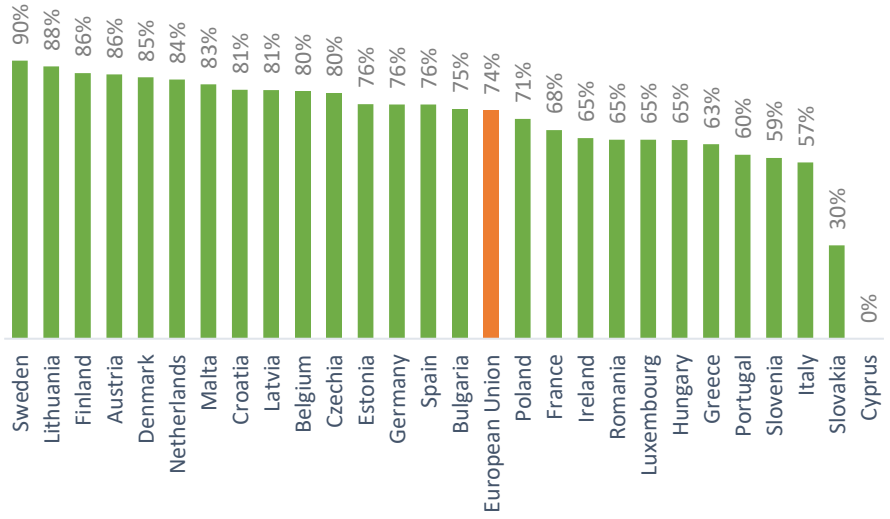
success rates higher than the average. Lithuania, Finland, Croatia, Belgium, Netherlands, Austria, Latvia, Malta, Czechia and Denmark all have success rates equal to or above 80%. Sweden records a 90% success rate. These results attest to the fact that EU competent authorities and service providers alike have more mature processes in place, and more experience in the field of cross-border access to electronic evidence.

Among the companies analysed, Google had the highest success rate (82%) and Yahoo the lowest (33%). Moreover, Member States where SPoCs for direct requests under voluntary cooperation have been established have success rates of 6% higher on average than those that do not have such units.

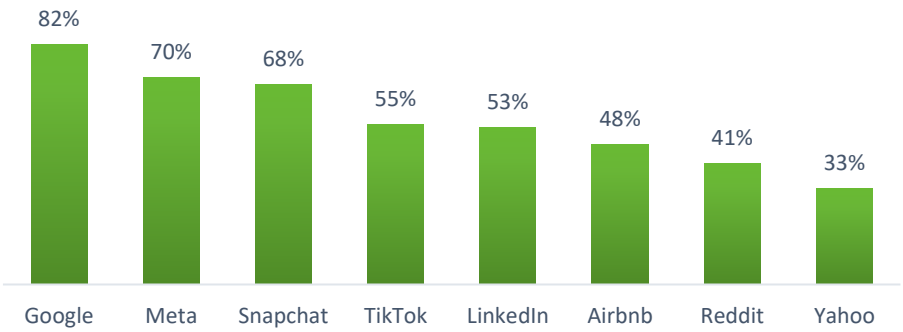
Average EU success rate of requests to a number of service providers from 2018 to 2023



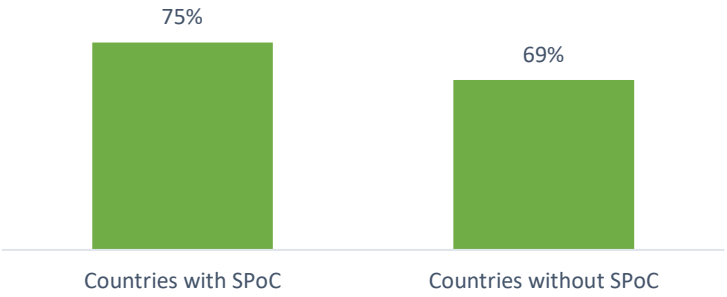
Success rate of EU data requests to a number of service providers in 2023, per Member State



Average EU success rate of requests to a number of service providers in 2023, per company



Average success rate of countries with or without an established SPoC for centralisation of requests in 2023



Reasons for refusal or delay in processing direct requests for voluntary cooperation issued by EU authorities

The quantitative feedback concerning the success rate of EU cross-border requests for electronic evidence is relevant. At the same time, understanding the main reasons for any refusal or delay in handling direct requests provides a qualitative dimension to the overall analysis. Although any such list is influenced by circumstantial factors – such as the different policies adopted by different service providers for voluntary cooperation, in 2023, service providers indicated there were no significant changes to what reported in previous years.

The following list of reasons for refusal or delay in processing direct requests for voluntary cooperation issued by EU authorities is not ranked by order of importance.

- Overly broad requests

Requests that fail to identify a targeted number of accounts in connection with an investigation or that cover an excessive amount of data on the specified users are often considered, in providers' eyes, too broad. In these situations, authorities need to narrow down the request by specifying the service concerned – out of the many services offered by one entity – by defining a specific and narrow timeframe of relevance for the information sought, and/or by listing the exact datasets that are being requested.

- Lack of context and information regarding the crime under investigation

Service providers decide whether or not, and to which degree, they will respond to a direct request for voluntary cooperation based on the information included in the requests. Equally, that information is necessary to assess the necessity and proportionality of direct requests under voluntary cooperation and to give them the right prioritisation. Requests that are drafted in a vague manner, that do not provide a reasonable ground for suspicion linking the investigation and the data sought from the service provider addressed or that, more generally, lack context, are likely to be rejected or delayed until more information is provided by the authorities.

Providing detailed background information becomes even more essential when authorities are submitting requests that may have extraterritorial effects, e.g. when the user targeted is outside the investigating jurisdiction, or when dealing with particularly sensitive cases, e.g. terrorism or child-related crimes.

Some providers that were interviewed reported how the unclear description of the case or the poor drafting of requests affect around 45% of the direct requests received, triggering straight rejections or delays in processing.

- Procedural issues and non-fulfilment of legal requirements

Requests for disclosure of data are often delayed or rejected due to procedural issues. Depending on the provider and the applicable policies considered, these may involve missing dates, lack of signature by the requesting officer or of official letterheads. Further delays or rejections may be caused by the fact that a wrong or no legal basis is mentioned, that the required legal process is not attached or because requests are addressed to the provider's wrong legal entity.

Additionally, since the entry into force of the DSA, some providers started applying the minimum requirements for orders set out in Article 10 of the DSA to assess the validity of the direct requests received. In those instances, providers reported how the quality of requests received diminished – and rate of rejection/delay increased, as authorities appeared not to be aware of the additional DSA-related requirements.

- Lack of reply from authorities when service providers ask for additional information

In case of wrong or incomplete requests – which according to the service providers interviewed may amount to 70% of the cases, providers may reach out to the competent authority via the same channel used for the submission of the request in

order to address the outstanding issues. In this regard, providers reported how oftentimes authorities are not responsive and requests are not followed up.

From a reverse perspective, authorities may interpret such outreach efforts as service providers being uncooperative and therefore choose to pursue different investigative approaches. Such a lack of response from authorities frequently leads to delays in responding to requests.

- Misunderstanding on the services provided or the datasets available

Data disclosure requests are rejected when the data requested is not collected by the service provider, or is only collected with end-to-end encryption. Large service providers which offer numerous products and services may be more affected by this issue, as there may be more misunderstandings in relation to the data they collect from users. Additionally, some providers reported how officers misattribute services and providers, submitting requests for a service accessible via a specific platform but owned by another provider.

It is notable how many of these issues could be avoided by increasing awareness among stakeholders, ensuring capacity building activities, as well as increasing opportunities for direct engagement between service providers and competent authorities.

Existing challenges: the perspective of service providers

From a broad perspective, service providers encounter significant challenges in their day-to-day work of cooperating with EU authorities. Figures show how the volume of requests continues to rise steadily, while the legislative and policy landscape evolves just as rapidly. Additionally, 2023 has also been characterised by significant layoffs affecting the private sector, including among the service providers that SIRIUS engages with [27].

During the interviews conducted for the purpose of collecting data for this report, the specific challenges mentioned by representatives of the industry remain similar to last year's ones.

- Dealing with increasing volumes of requests and their authentication

As the volume of requests increases, service providers must routinely consider their workload. The scale of the phenomenon is worsened by the fragmentation existing at EU Member States' level, especially when a SPoC approach is not in place and providers may receive requests from different officers – the so-called "one-time requesters". The need to contact one-time requesters to clarify policies and requirements is one of the biggest challenges for many service providers, as many officers have little or no formal training in electronic evidence matters.

To minimise the impact of one-time requesters, some providers, especially those operating at global level and that receive requests via proprietary online portals, establish a maximum number of portal accounts assigned per country or authority.

Such policy guarantees that only officers whose primary task is submitting direct requests to providers have the technical possibility to do so. Additional mechanisms that entail automatic account deactivation for inactivity are further being introduced.

Increased volumes of incoming requests have a direct effect on their authentication too. Equally challenging is the verification of identities of competent authorities submitting requests, especially as some providers reported receiving fraudulent requests from what appeared to be legitimate sources.

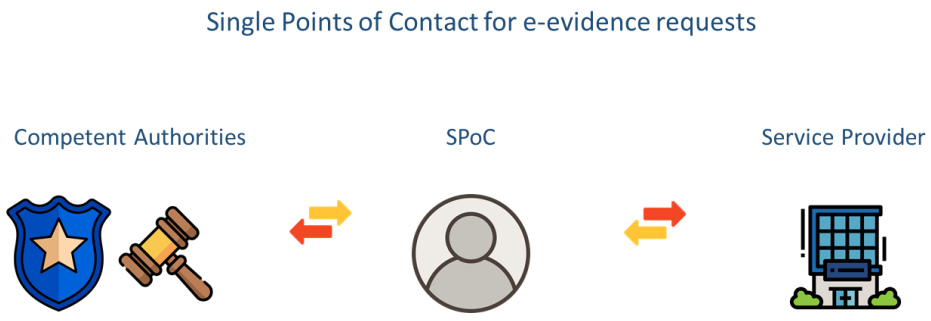
- Monitoring changes to domestic legislations and implementing new international rules

Service providers, especially those operating across several countries and world regions, must keep track of evolving domestic legislations and maintain a thorough understanding of applicable regulations. Due to the high degree of fragmentation, they oftentimes need to account for regional differences within the same country. The effort required in such circumstances and the overall impact on processes was reported as a challenge by some service providers.

In relation to changing legislations, providers also referred to circumstances in which authorities were unaware of new pieces of international legislation and their impact on direct requests and voluntary cooperation. As mentioned above, the DSA is a fitting example, whereby providers started applying DSA-related requirements without authorities fully understanding the resulting effects.

The experience of service providers with Single Points of Contact

As noted above, SPoCs are designated persons or units within the competent authorities of a respective country that streamline and channel cross-border data disclosure requests under voluntary cooperation to one or more foreign-based service providers in a centralised manner.



As in previous years, all service providers that have cooperated with SPoCs in 2023 report positive and efficient engagement. In addition to what reported in previous editions of this report, in 2023 service providers highlighted the following aspects:

- SPoCs significantly increase the quality of data disclosure requests and therefore lead to a higher success rate. A provider offered a quantitative

estimate of such benefits mentioning how, when SPoCs are part of the process, the compliance rate is 14% higher, the time to process requests is 15% lower, and the likelihood of errors is reduced by 13%.

- The SPoC model is scalable and service providers encourage all EU Member States to adopt it. By doing so, EU Member States without SPoCs can learn from the experience of their peers and favour better internal promotion. Providers adapt to national SPoC structures, yet they favour nation-wide SPoCs. Some providers even support the idea of SPoCs covering the entire EU jurisdiction.

- SPoCs are fundamental for awareness raising and training activities. This is particularly important in the context of evolving legislation, where SPoCs can be critical in internalising new requirements – such as those stemming from the DSA, and in implementing new pieces of legislation – such as the EU Electronic Evidence legislative package.

Many service providers advocate for the capacity of existing SPoCs in EU Member States to be expanded even further. This would ensure the continuous improvement of existing processes and prepare for an increasing volume of requests for electronic evidence. Service providers also strongly encourage law enforcement agencies that still do not have SPoCs in place to establish such units.

EU Electronic Evidence legislative package

The EU Electronic Evidence legislative package will introduce, as of August 2026, significant changes for the industry as well. As such, those service providers interviewed have started preparing for what these changes might entail. Some providers feel comfortable with the new rules, are ready to implement them, and do not expect the Electronic Evidence legislative package to significantly alter their operating procedures. Others have started adapting their processes to the new rules, whereas a smaller group is waiting for full clarity before taking any action.

In addition to the positive changes the new rules will bring – such as increased legal certainty and a more standardised approach, above all, providers interviewed shared a list of concerns, expectations, and potential future challenges.

- Providers agree on the need for a large multi-stakeholder effort in order to prepare for the implementation of the EU Electronic Evidence legislative package in a smooth, efficient and homogeneous manner. They expect such effort to be led and promoted by the EU Commission, especially when it comes to offering guidance on and clarification of fundamental notions – such as the exact scope of the new rules and the definition of key legal concepts, such as what constitutes a “service provider”.

- The anticipated increase in the volume of orders that providers will have to handle also emerged as an element of concern. Notably for those service providers that currently only cooperate voluntarily with a limited number of EU Member States but have to predict new volumes at EU level. Reliable

forecasts of how volumes will change is a precondition for planning and allocating appropriate financial and human resources.

- The decentralised IT system for secure digital communication and data exchange between competent authorities and service providers remains a topic of high concern. Service providers regard the readiness and availability of this technical solution as the element that will determine the success or failure of the entire legislative initiative. Moreover, some providers are concerned about the compatibility of the decentralised IT system with their internal systems as they regard interoperability and smooth data flow as their priority. Based on the information currently available to them, some providers doubt that the decentralised IT system will adapt to the size of data transfers, especially when involving disclosure of content data. Finally, ensuring the confidentiality and security of data remains fundamental.

- Given the unanimously positive experience in cooperating with SPoCs, providers expect this centralised approach to remain relevant when the new rules will become effective. Continued and enhanced engagement with SPoCs – from both an operational and a strategic point of view, can guarantee a better outcome in the future of electronic evidence exchange.

- Providers reported that their decision on whether forms of voluntary cooperation will be maintained after August 2026 largely depends on the correct interpretation and application of the new rules.

Service providers call upon EU legislators to provide clear guidance and set up outreach and cooperation programmes to prepare all stakeholders involved. The ultimate desire for a smooth and effective application of the new rules is accompanied by the need to act well in advance of August 2026. The recent experience with the implementation of DSA serves as a benchmark.

Some service providers reported that the misalignment between the industry and EU competent authorities regarding the application of new DSA rules had a significant negative impact on providers' operations. The perceived lack of guidance from EU legislators left service providers free to interpret and apply the DSA in an uncoordinated manner opening therefore the door to fragmentation and further complications in the entire process. Unable to play by the same rules, service providers had to also face the unpreparedness of EU competent authorities in this regard.

Service providers interviewed are therefore keen to learn from past experiences and avoid similar issues with the new EU legislation on electronic evidence.

Against this background, service providers attach to the SIRIUS Project a role of primary importance, especially during the implementation period leading up to August 2026. Some providers shared further insights concerning the SIRIUS Project:

- With its comprehensive overview of EU competent authorities and service providers, SIRIUS is a reliable interlocutor. The EU Commission should leverage this to gain a clear picture of stakeholders' needs and expectation.

- The work of SIRIUS has led to tangible improvements in the quality of today's requests for data disclosure. The project will therefore remain a relevant actor in the future of electronic evidence as well.

- The SIRIUS Project could issue recommendations or a collection of best practices for companies to help them comply with the legislation. It could also continue offering specific guidelines as an effective means for competent authorities to gain initial guidance on obtaining electronic data from specific providers.

- The SIRIUS SPoC network will also become particularly relevant once the new legislation comes into play, helping resolve any issues or clarifications needed to quickly respond to a cross-border data disclosure request.

Similar to the past edition of this report, service providers were asked whether they will continue to accept direct requests under voluntary cooperation, once the new EU Electronic Evidence Regulation will come into force. Responses on this matter remain varied, with providers' intention ranging from discontinuing any future voluntary cooperation to maintaining it as a more effective process considering the high volume of criminal investigations that require electronic data disclosure.

RECOMMENDATIONS

In light of the findings of the 2024 edition of the SIRIUS Electronic Evidence Situation Report – the persistence of challenges that EU law enforcement and judicial authorities face while the legislative framework is evolving, an overarching recommendation for all stakeholders is to follow closely the activities of the SIRIUS Project. SIRIUS products and services, designed to advance authorities' knowledge and operations in the current panorama of cross-border investigation and prosecution of crime involving evidence in electronic format, will also prove useful as the new rules stemming from the EU Electronic evidence legislative package are being defined.

A more targeted list of recommendations for different stakeholder groups follows.

For EU law enforcement agencies

Prepare for and adapt to the EU Electronic Evidence legislative package

As the EU Electronic Evidence legislative package takes shape, one year on, this report shows how knowledge of the concrete aspects of the new legislation and its implications from the side of law enforcement authorities remains low. At the same time, the impact that the new legislation will have on them is significant.

Law enforcement agencies should therefore make sure they participate in the current discussions between policy makers, at international and national level, to ensure that the definition and operationalisation of the new rules is adapted to the officers' concrete needs and existing investigative practices. Specifically, law enforcement should seek a closer collaboration and stronger level of engagement with SPoCs – where applicable, national judicial authorities, relevant service providers, and authorities of other EU Member States for the establishment of relevant processes and procedures. To facilitate coordination and preparedness, active participation in future SIRIUS events is encouraged.

Preparation and adaptation to new roles and processes appears fundamental especially as service providers may change their policies with respect to voluntary cooperation, once the new rules will be in place. Adapting current internal processes to the new legislation will eventually generate more effective results if conducted in a coordinated manner.

SIRIUS' established role as a centre of excellence in the EU could assist in this process by facilitating information-sharing on a bilateral and multilateral level.

Broaden training efforts on cross-border access to electronic evidence covering the current framework and future developments

Although the legislative developments on cross-border access to electronic evidence are poised to fundamentally change the investigative panorama in this regard, this

report shows how the challenges faced by EU law enforcement authorities persist, roughly unchanged.

Therefore, ensuring that EU law enforcement officers are prepared to request and analyse electronic evidence in the current legal framework is crucial for today's criminal investigations. The recommendation made in previous editions of this report that training activities on cross-border access to electronic evidence be included in all training programmes of investigators and first responders remains highly relevant.

At the same time, EU investigators and law enforcement at large will be confronted with new rules, instruments, and potential future technological challenges. Ensuring therefore that EU Members States' training efforts for law enforcement authorities are broad enough to consider future developments is required in order for authorities to remain ahead of the curve.

Reinforce the SPoC approach and ensure active engagement with the SPoC Network

In line with previous editions, this report reiterates the strong support towards the creation and operationalisation of SPoCs in the EU. These actors are essential in increasing compliance rates of direct requests, as well as reducing the processing time and the chance of mistakes in requests. Equally, SPoCs appear essential both when the future rules of cross-border engagement for electronic evidence exchange will come into effect, as well as throughout the process of defining and implementing those rules.

The recommendation to establish SPoCs in those law enforcement agencies where they do not yet exist remains highly relevant, both for the present as well as for the medium and long-term future. Law enforcement agencies working on the establishment of SPoCs are encouraged to contact the SIRIUS Team at Europol to join the SIRIUS SPoC Network as observers to learn from the experience of their peers.

Law enforcement authorities may contact the SIRIUS Team at Europol via e-mail at: sirius@europol.europa.eu

For EU judicial authorities

Enhance knowledge and build capacity on available legal instruments for cross-border access to electronic evidence

Continuous training on existing legal instruments and specific procedures for requesting the preservation and production of electronic evidence across borders is crucial to equip EU judicial practitioners with the necessary expertise to acquire electronic evidence effectively, using tailored solutions that meet the unique requirements of each case.

In this respect, EU judicial authorities are encouraged to use the support and resources provided by EU actors involved in the field of judicial cooperation, such as Eurojust, the EJN, the EJCN and the SIRIUS Project.

For further assistance and to access specialised resources, judicial authorities can contact the SIRIUS Project team at Eurojust via e-mail at sirius.eurojust@eurojust.europa.eu.

Prepare judicial authorities to effectively use new instruments under forthcoming EU Electronic Evidence legislative package, as well as other legislative changes concerning the cross-border acquisition of electronic evidence

Building knowledge and capacity is pivotal to empower judicial authorities with the skills and expertise needed to effectively utilise upcoming legal instruments, including the EU Electronic Evidence legislative package, which will bring groundbreaking changes in the process of cross-border gathering of electronic evidence.

To adequately prepare for these forthcoming legislative changes, EU judicial authorities are encouraged to engage with the resources, training sessions, and awareness-raising programs developed by the SIRIUS Project.

For further information, training opportunities, and support tailored to the implementation of new legal frameworks, judicial authorities can contact the SIRIUS Project team at Eurojust via email at sirius.eurojust@eurojust.europa.eu

Strengthen mutual trust and knowledge sharing among EU judicial practitioners on cross-border gathering of electronic evidence

Recognising the challenges faced in obtaining electronic evidence across diverse jurisdictions, enhancing mutual trust among EU judicial authorities is essential. Facilitating knowledge sharing and exchanging best practices on accessing electronic evidence across borders are critical steps.

In this regard, EU judicial authorities are encouraged to actively participate in the dedicated forum on the restricted SIRIUS platform. Engaging with fellow members of the judicial community and participating in events, trainings, and networking opportunities provided by the SIRIUS Project will foster collaboration and enhance expertise.

Judicial authorities can benefit from joining discussions and accessing resources on the SIRIUS platform to stay informed about best practices and developments in cross-border access to electronic evidence.

For service providers

Prepare for compliance with the EU Electronic Evidence legislative package and share early updates with EU Authorities

Given the obligations introduced by the EU Electronic Evidence legislative package, service providers should carefully consider the impact these may have on their existing processes and resources and how this may affect future cooperation with EU

competent authorities. For example, many service providers reported the need for additional human resources and technical solutions to allow them to comply with the deadlines for responses to European Production Orders set out in the Electronic Evidence Regulation.

Service providers falling under the scope of the EU Electronic Evidence legislative package should strive to properly inform EU competent authorities whether different policies are in place and in which cases or for which services voluntary cooperation mechanisms can still be relied on.

Similarly, as several service providers of interest for EU competent authorities will fall outside the scope of the EU Electronic Evidence legislative package, a clear definition and dissemination of their policies would help prevent significant misunderstandings, at the benefit of public and private stakeholders as well.

Engage closely with the SIRIUS Project and share policy updates with the SIRIUS Team

Service providers can make use of the SIRIUS Platform and events to disseminate their policies and relevant updates to EU law enforcement and judicial authorities. Similarly, smaller service providers can take advantage of the expertise of the SIRIUS Project in the field of cooperation with authorities to increase their understanding of the matter, structure their policies for responding to authorities' requests and ensure that they are prepared for upcoming legislative developments.

This appears even more relevant considering how international legislation evolves and rules stemming from the EU Electronic Evidence legislative package will not cover the entirety of service providers of interest for EU competent authorities.

Service providers may contact the Europol SIRIUS Team at: sirius@europol.europa.eu

For actors implementing the EU Electronic Evidence legislative package at the EU and Member State level

Engage with the broad community of EU competent authorities and service providers

The new rules on cross-border access to electronic evidence will revolutionise the working field of all EU competent authorities mandated with the prevention, investigation and prosecution of crime. However, based on the findings included in this report, EU authorities' knowledge about the future of electronic evidence appears limited.

To ensure that the new rules meet the needs of competent authorities and duly consider their requirements, their direct involvement during the implementation phase of technical solutions and workflows appear the best approach for subsequent buy-in.

Specifically, direct engagement with both the actors involved in the processes of cross-border disclosure of data in the currently and the forthcoming applicable legal framework appears necessary during the implementation phase, as well as when the new rules will become applicable. Their specialised knowledge and skills are to be exploited and leveraged.

As legislation will equally affect service providers, a broader outreach and engagement approach targeting a larger share of the industry would guarantee better and early alignment on how new channels and processes will concretely work.

Leverage SIRIUS' expertise via early involvement in implementation

As the centre of excellence in the field of cross-border access to electronic evidence in the EU, SIRIUS has developed significant experience and knowledge via its direct engagement with EU competent authorities as well as the main service providers active in the EU and worldwide.

SIRIUS' knowledge and expertise can thus be leveraged by those actors tasked with implementing the EU Electronic Evidence legislative package, with the objective of collecting experience from field investigators, SPoCs in the remit of voluntary cooperation with service providers, judicial practitioners, and representatives of the industry in a condensed and streamlined manner.

END NOTES

[1] Single Points of Contact (SPoCs) for cross-border data disclosure requests to foreign-based service providers under voluntary cooperation are defined as designated persons or units within the competent authorities of a respective country which streamline and channel cross-border data disclosure requests under voluntary cooperation to at least one or more foreign-based service providers in a centralised manner.

[2] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191/118) and Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191/181).

[3] The Electronic Evidence Regulation shall apply from 18 August 2026 while in the case of the Electronic Evidence Directive, EU Member States shall adopt the necessary measures to comply with it by 18 February 2026.

[4] Council of Europe, Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), accessible at https://www.coe.int/en/web/cybercrime/second-additional-protocol.

[5] European Commission, 2024, The Digital Services Act package, accessible at https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

[6] European Commission, The Digital Markets Act, accessible at https://digital-markets-act.ec.europa.eu/index_en.

[7] See AI Act (applicable as of August 2026, with some provisions being applicable as of February 2025 and August 2027, respectively). European Commission, 2024, AI Act, accessible at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. European Commission, The Digital Markets Act, accessible at https://digital-markets-act.ec.europa.eu/index_en.

[8] Europol, 2024, Internet Organised Crime Threat Assessment (IOCTA) 2024, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024#downloads.

[9] Europol, 2024, SIRIUS and An Garda Síochána advance collaboration in cross-border access to electronic evidence, accessible at https://www.europol.europa.eu/media-press/newsroom/news/sirius-and-garda-s%C3%ADoch%C3%A1na-advance-collaboration-in-cross-border-access-to-electronic-evidence.

[10] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden.

[11] The service providers were chosen based on their relevance for criminal investigations in the EU as indicated by competent authorities on previous occasions, as well as their availability to contribute to this report.

[12] Throughout this report, some responses were edited for additional clarity, or translated from different EU languages into English.

[13] See section on 'Submission of cross-border requests', p. 22.

[14] Europol and Eurojust, 2022, SIRIUS EU Digital Evidence Situation Report 2022, accessible at https://www.europol.europa.eu/publications-events/publications/sirius-eu-digital-evidence-situation-report-2022.

[15] The DSA categorises online platforms and search engines as "very large" based on the number of users they serve, specifically those reaching more than 45 million monthly active users in the EU.

[16] European Commission, 2023, Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines, accessible at https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.

[17] Austria: 4,973 (4,913 direct requests and 60 emergency disclosure requests); Croatia: 38 emergency disclosure requests; Denmark: 3,265 (2,059 direct requests, 32 emergency disclosure requests and 1,174 preservation requests); Norway: 545 direct requests; Spain: 18,676 (the sum of 105 direct requests of Policía Foral of Navarra, 13,417 direct requests of Guardia Civil and 5,154 direct requests of Policía Nacional); Sweden: 7,649 (7,433 direct requests and 216 preservation requests). Data shared by the SPoC in Belgium was not included in the final sum as Belgian statistics refer to the total number of accounts in relation to which data was requested rather than the total number of requests submitted. In this regard, in 2023, the SPoC in Belgium handled requests targeting a total of 11,801 accounts.

[18] This constitutes a courtesy translation.

[19] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105/54).

[20] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), (OJ L 201).

[21] A comprehensive review can be found consulting:

- Europol and Eurojust, 2022, SIRIUS EU Digital Evidence Situation Report 2022, accessible at https://www.europol.europa.eu/publications-events/publications/sirius-eu-digital-evidence-situation-report-2022.
- Europol and Eurojust, 2021, SIRIUS EU Digital Evidence Situation Report 2021, accessible at https://www.eurojust.europa.eu/publication/sirius-eu-digital-evidence-situation-report-2021.
- Europol and Eurojust, 2020, SIRIUS EU Digital Evidence Situation Report 2020, accessible at https://www.eurojust.europa.eu/publication/sirius-eu-digital-evidence-situation-report-2020.
- Eurojust, 2023, Cybercrime Judicial Monitor – Issue 8, accessible at https://www.eurojust.europa.eu/publication/cybercrime-judicial-monitor-issue-8.
- Eurojust, 2022, Cybercrime Judicial Monitor – Issue 7, accessible at https://www.eurojust.europa.eu/publication/cybercrime-judicial-monitor-issue-7.

[22] General Secretariat of the Council, 2024, 61st Plenary meeting of the European Judicial Network (EJN) (Madrid, Spain, 7-9 November 2023) - Conclusions of the workshops, accessible at https://www.consilium.europa.eu/en/documents-publications/public-register/public-register-search/?AllLanguagesSearch=false&OnlyPublicDocuments=false&DocumentNumber=8712%2F24&DocumentLanguage=EN.

[23]Apple, Microsoft and X (formerly known as Twitter) have been removed from the analysis in comparison with previous editions of this report, because their transparency reports for the full year of 2023 had not been published by 20 October 2024, when the draft of this document has been finalised.

[24] Facebook: from 25 April to 27 September 2023; Instagram: from 25 April to 27 September 2023; Google (inclusive of Google Search, Google Maps, Google Play, Google Shopping and YouTube): from 28 August to 10 September 2023; TikTok: from 1 September to 30 September 2023; Snapchat: from 1 July to 31 December 2023; LinkedIn: from 25 August to 30 September 2023.

[25] Facebook's and Instagram's DSA transparency reports provide the exact same volumes as figures relate to Meta services in general.

[26] LinkedIn does not report on the number of Emergency Disclosure Requests separately.

[27] Crunchbase news, 2024, The Crunchbase Tech Layoffs Tracker, accessible at https://news.crunchbase.com/startups/tech-layoffs/.

REFERENCES

All links were accessed in September and October 2024.

- Airbnb Law Enforcement Transparency Reports, accessible at https://news.airbnb.com/transparency/
- Google Global requests for user information, accessible at https://transparencyreport.google.com/user-data/overview
- LinkedIn Government Requests Report, accessible at https://about.linkedin.com/transparency/government-requests-report
- Meta Government Requests for User Data, accessible at https://transparency.fb.com/data/government-data-requests/
- Reddit Transparency Report, accessible at https://www.redditinc.com/policies/transparency?_ga=2.6477810.1955032930.1679335409-1865029628.1677515303
- Snap Transparency Report, accessible at https://www.snap.com/en-US/privacy/transparency
- TikTok Information Request Report, accessible at https://www.tiktok.com/transparency/en/information-requests-2022-2/
- Yahoo Government Data Requests, accessible at https://www.yahooinc.com/transparency/reports/government-data-requests/JUL-DEC-2023/index.html

ACRONYMS

AI	Artificial Intelligence
AR	Augmented Reality
CJEU	Court of Justice of the European Union
DSA	Digital Services Act
e-EDES	e-Evidence Digital Exchange System
EDR	Emergency Disclosure Request
EIO	European Investigation Order
EJCN	European Judicial Cybercrime Network
EJN	European Judicial Network
EPOC-PR	European Preservation Order Certificate
EU	European Union
GDPR	General Data Protection Regulation
IP	Internet Protocol
LEA	Law Enforcement Agency
MLA	Mutual Legal Assistance
OSINT	Open Source Intelligence
SP	Service provider
SPoC(s)	Single Point(s) of Contact
UK	United Kingdom of Great Britain and Northern Ireland
UN	United Nations
US	United States of America
VLOP	Very Large Online Platform
VLOSE	Very Large Online Search Engine
VPN	Virtual Private Network
VR	Virtual Reality