SIRIUS Electronic Evidence Situation Report

2025

EU GLOBAL THREATS PROGRAMME

EUROPOL

EUROJUST

SIRIUS ELECTRONIC EVIDENCE SITUATION REPORT 2025

The Hague
July 2026

This publication was funded by the European Union. Its contents are the sole responsibility of the SIRIUS Project, co-implemented by Europol and Eurojust, and do not necessarily reflect the views of the European Union.

Funded by the European Union

EU GLOBAL THREATS PROGRAMME

EUROPOL EUROJUST

SIRIUS ELECTRONIC EVIDENCE SITUATION REPORT 2025

PDF Web | QL-01-26-021-EN-N | 978-92-9414-154-5| 3094-6786 | 10.2813/4169376

Luxembourg: Publications Office of the European Union, 2026

To cite this publication:

Europol & Eurojust, SIRIUS Electronic Evidence Situation Report 2025, Publications Office of the European Union, Luxembourg, 2026.

This report is jointly issued by the European Union Agency for Law Enforcement Cooperation (Europol) and the European Union Agency for Criminal Justice Cooperation (Eurojust) through the SIRIUS Project.

The SIRIUS Project has received funding from the European Commission's Service for Foreign Policy Instruments under Contribution Agreement NDICI THREATS FPI/2024/OPSYS CT NR 700002618.

This publication and more information on Europol are available on the internet via www.europol.europa.eu.

Your feedback matters

By scanning the embedded QR code or clicking on the following link you can share your feedback regarding this report. Your input will help us further improve our products.

https://ec.europa.eu/eusurvey/runner/2025_SIRIUS_REPORT_FEEDBACK

INDEX

FOREWORD

Jürgen Ebner
ACTING EXECUTIVE DIRECTOR, EUROPOL

The SIRIUS project facilitates cross-border access to electronic evidence since 2018 and manages one of the largest communities of experts and practitioners on Europol's Platform for Experts.

Europol and Eurojust – together as co-implementing partners – have established a widely recognised centre of excellence in the European Union. A true success-story that demonstrates inter-agency collaboration integrating key stakeholders for the investigation and prosecution of crimes.

In light of this, it is with great pleasure that I can introduce the 2025 edition of the SIRIUS Electronic Evidence Situation Report. A report that provides data-rich and unique insights for policy-makers, authorities and service providers about trends and challenges in cross-border access to electronic evidence. It offers tailored recommendations to relevant stakeholder groups and confirms its role as a trusted source of information for evidence-based decision-making by law enforcement, judicial authorities and service providers.

With the upcoming implementation of new electronic evidence legislation in the EU in August 2026, the assessment of public-private partnerships between authorities and service providers remains a crucial part to enhance the access to electronic evidence in criminal investigations. This contributes to our fight against a wide range of crimes with an electronic evidence component and contributes actively towards making the EU a safer digital space.

I would like to thank the SIRIUS project for its continued commitment to facilitate cross-border access to electronic evidence and ensure Europol's commitment to support its partners within and beyond the European Union in this field.

Michael Schmid
PRESIDENT, EUROJUST

Access to electronic evidence is and will remain the main challenge for prosecutors and investigators in the years to come. Since its inception in 2018, the SIRIUS project has rapidly become a key point of reference for cooperation with electronic communications service providers, supporting judicial practitioners and law enforcement professionals in obtaining electronic evidence.

This has also been recognised in the EU Roadmap for effective and lawful access to data for law enforcement, adopted in June 2025, which calls on Eurojust to further strengthen cooperation with service providers through SIRIUS as serious and organised crime continues to shift further into the digital sphere.

Judicial cooperation instruments remain essential to enabling cross-border access to electronic evidence. Within the European Union, access to electronic evidence through judicial cooperation is primarily ensured through the European Investigation Order (EIO) and, in specific cases, Mutual Legal Assistance (MLA) procedures. Both frameworks, however, were not originally designed to accommodate the specific characteristics of electronic evidence. The volatility of digital data, combined with divergent national procedural requirements and varying response times, continues to pose significant operational challenges.

Against this background, our community looks much forward to the introduction of the EU Electronic Evidence package and the Second Additional Protocol to the Budapest Convention on Cybercrime in August 2026. It will be crucial for prosecutors and judges to fully leverage the opportunities these instruments will provide.

And while we count on the cooperation of all partners involved, Eurojust and the SIRIUS project too remain fully committed to supporting the implementation of the new workflows and practices we expect, ensuring that cybercrime and cyber-enabled crime do not go unpunished in our physical world.

QUOTES FROM THE COMMISSIONERS

Magnus Brunner
COMMISSIONER, DG HOME

In today's digital age, criminals operate across borders, and so must the responses of law enforcement. Timely access to electronic evidence is therefore critical for effective investigations. Yet, with rapidly evolving technology and new legal frameworks on the horizon, law enforcement must be equipped with the knowledge and skills to keep pace. The SIRIUS Project contributes to both with this report. It is a key source of information for authorities on the status of cross-border access to electronic evidence in the European Union and selected third countries. Rising data request volumes analysed by the report, underline the necessity to retain and expand effective public-private cooperation through SIRIUS. Insights gathered by the project feed directly into their training activities – a resource highly valued by practitioners across EU Member States and beyond. Through this, the SIRIUS project has become indispensable for many authorities and service providers to fight crime in the digital sphere and remains an effective tool to tackle upcoming challenges in requesting cross-border electronic evidence.

Michael McGrath

COMMISSIONER FOR DEMOCRACY, JUSTICE, THE RULE OF LAW AND CONSUMER PROTECTION, DG JUST

In today's digital age, effective justice depends on timely and reliable access to electronic evidence across borders. This report highlights both the progress made and the challenges that remain in an evolving legal landscape. As the European Union moves towards implementing its Electronic Evidence framework, we are committed to equipping law enforcement and judicial authorities with faster, clearer, and more harmonised tools—while upholding fundamental rights and the rule of law. Strengthening cooperation with global partners and investing in capacity-building will be essential to ensure that justice systems can keep pace with technological change and continue to protect our citizens. The SIRIUS Project has proven to be an important vehicle to connect judicial authorities, law enforcement and service providers. With their expertise in coordinating complex cross-border investigation involving electronic evidence, Eurojust and Europol are ensuring that authorities and service providers have the right tools and knowledge at hand to overcome the legal challenges associated with the digital landscape that criminals operate in.

EXECUTIVE SUMMARY

For competent authorities worldwide, the effective investigation and prosecution of crime increasingly depend on timely access to digital data and the ability to rely on electronic evidence. As legislation governing the digital sphere continues to evolve, this report examines the increasingly complex – and in many respects divergent – legal landscape surrounding cross-border access to electronic evidence. No fundamental shift in the legal and operational landscape occurred in 2024. However, significant legislative and operational developments are forthcoming and are expected to substantially reshape the framework for cross-border access in the near future.

This report provides insights and guidance to practitioners in the field of cross-border access to electronic evidence. It covers the period of the year 2024 and is based on direct exchange with the main stakeholders in the field – law enforcement agencies, judicial authorities and service providers – and includes aggregated summary statistics of the transparency reporting from service providers. Building on this data, the report provides insights into the characteristics and trends of data disclosure in the EU and other jurisdictions.

From the perspective of EU law enforcement, direct requests remain the key type of request to access cross-border data from service providers. In 2024, most of these were channelled through online portals, but email remains another method regularly used. Aside from direct requests, other procedures are less popular and the Mutual Legal Assistance (MLA) process is largely considered too lengthy by the survey respondents.

In law enforcement requests, the three most relevant types of online services for investigations are social media, messaging apps and cryptocurrency exchanges, while the top three of the most important data types are connection logs, telephone numbers and IP addresses used at registration. To reach higher success rates under direct requests, Single Point of Contact (SPoC) units proved to be beneficial. If SPoCs are established in a jurisdiction or agency, law enforcement officers widely reported being satisfied with their work.

Finally, familiarity with the EU Electronic Evidence legislative package remains low among law enforcement professionals: 8% of respondents are very familiar with the package, while 40% indicated that they are not at all familiar. These findings underline the need for increased training that reflects the constantly evolving nature of cross-border access to electronic evidence.

From the perspective of judicial authorities, MLA and other formal judicial cooperation channels remain the primary means of obtaining electronic data from service providers located abroad. However, both EU and non-EU authorities consistently report that these mechanisms are often too slow and procedurally complex, risking delayed investigations and, in some cases, the loss of critical electronic evidence.

In response to these operational constraints, some authorities, particularly within the EU, have increasingly relied on direct voluntary cooperation with foreign service providers as a complementary, faster channel, especially for non-content data.

The forthcoming application of the EU Electronic Evidence legislative package, together with the entry into force and subsequent implementation of the Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Second Additional Protocol to the Budapest Convention), is expected to significantly strengthen the toolbox available to judicial authorities. These instruments aim to provide more robust, harmonised and streamlined mechanisms for cross-border data access, addressing many of the procedural challenges identified by judicial authorities.

Nevertheless, challenges remain, particularly in relation to data retention, which fall outside the scope of these new instruments. Authorities in both EU and non-EU countries highlight that short or absent retention periods continue to result in the unavailability of requested data, with direct consequences for criminal investigations and proceedings.

The findings further underline the importance of continuous capacity building on both existing and forthcoming data acquisition modalities. This is crucial for enabling 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. Without adequate preparedness and coordinated implementation, the full potential of the new cross-border mechanisms may not be realised.

From the perspective of service providers, there are three key aspects to consider. First, the request volume has increased significantly year over year. To illustrate, the 2024 volume is about 3.5 times higher than the base-year 2018, totalling 303 289 requests in this sample. The increased demand by authorities for access to company data for criminal investigations tests the ability of law enforcement response teams at service providers to handle the increased volume, update processes and adapt tools to their provider policies and applicable legal frameworks.

Second, the success rates of data requests to service providers have reached its highest level since the start of the report series. Currently, 76% of requests from authorities to access cross-border data from service providers for criminal investigations were successful. This underlines the continuous improvement of the cooperation between authorities and service providers and the quality of the request mechanism in general.

Third, emergency requests are on the rise. The report saw a jump of 32% from the last reporting period, reaching 28 608 emergency requests in the sample. This results in increased strains on the resources of law enforcement response teams at service providers as emergencies often must be dealt with immediately and require specialised teams to handle.

To conclude, service providers are also facing transformational challenges due to the EU Electronic Evidence legislative package and the need to comply through adequate processes and IT systems.

OVERVIEW ON RECOMMENDATIONS

This report concludes with a detailed set of recommendations to stakeholders in order to further improve existing processes. Please find an overview below.

For law enforcement agencies

- Increase training to request cross-border access to data from service providers;
- Assess the potential of introducing or expanding the SPoC approach in your jurisdiction and/or agency;
- Prepare for the effective application of new legal frameworks on cross-border access to electronic evidence.

For judicial authorities

- Strengthen capacity and practical expertise on available legal instruments for cross-border access to electronic evidence;
- Prepare for the effective application of new legal frameworks on cross-border access to electronic evidence;
- Enhance cross-border cooperation, mutual trust and knowledge sharing.

For service providers

- Assess the final readiness for the go-live of the decentralised IT system of the EU Electronic Evidence legislative package from a service provider perspective;
- Engage with the SIRIUS community and share your company policy updates with the SIRIUS team.

KEY FINDINGS

PERSPECTIVE OF LAW ENFORCEMENT IN THE EU

Fintech firms are now among the top five most relevant types of services for investigations – social media, messaging apps, cryptocurrency exchanges and VPN providers remain in the top positions for 2024.

Connection logs, telephone numbers and IP addresses used at registration are the top three most requested data types in 2024.

61% of law enforcement prefer to submit direct requests to service providers via an online portal – 21% via e-mail and 15% through SPoCs.

58% of law enforcement have received at least some training on cross-border access to electronic evidence – a slight decrease compared to last year.

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

'[It will be faster] because of the obligation to respond within 10 days and within 8 hours in cases of emergency, and the obligation to appoint a legal representative in the EU.'

But:

'Mandatory changes to an existing system will require legal changes as well as serious changes in the operational logic. Both take time and require constant updating and educational reviews.'

PERSPECTIVE OF JUDICIAL AUTHORITIES IN THE EU

Judicial cooperation channels remain the primary and most reliable means for judicial authorities to legally obtain electronic evidence across borders.

Lengthy judicial assistance procedures and the absence of a data retention framework continue to be the primary challenges.

A significant portion of judicial authorities in both EU and non-EU countries lack sufficient familiarity with cross-border data acquisition methods and forthcoming legal instruments.

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

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

'The EU e-Evidence Package will be transformative for Ireland, the EU and service providers alike, by providing legal certainty and addressing the territorial challenges that can arise when gathering electronic evidence in cross-border criminal investigations, due to the global reach of major service providers and increasingly borderless nature of modern communications services.

Arising from the number of large service providers who are expected to designate their addressees in Ireland, and the considerable volume of e-Evidence orders expected to be received by them, the e-Evidence package will have significant implications for both the technology sector and criminal justice system in Ireland.

This presents both challenges and opportunities for the Irish state, which it is embracing.

The establishment of a 'Criminal Justice International Cooperation Office' (CJICO) will provide a single point of contact for cross-border judicial cooperation on e-Evidence, a central hub for the necessary skills and expertise, and a streamlined regulatory framework for service providers. […].' (Ireland)

PERSPECTIVE OF SERVICE PROVIDERS

The 2024 request volume is about 3.5 times the volume of the base-year 2018, totalling 303 289 requests in this sample.

The success rate of EU requests in 2024 was at 76% in this sample – the best result since the first edition of this report.

Google and Meta receive the most requests – together they make up 82% (249 867) of the total volume in this sample.

The volume of emergency disclosure requests issued by EU competent authorities jumped by 32% compared to 2023, with 28 608 requests in the 2024 sample.

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

'The EU Electronic Evidence legislative package will bring legal certainty.'

But:

'There are huge implementation risks, particularly due to the unknown number of requests to be expected.'

INTRODUCTION

About the SIRIUS Project

"*The SIRIUS project has become the most important source of information to support law enforcement practitioners and judicial authorities in the EU and beyond in accessing electronic evidence stored by online service providers […].*"[1]

The SIRIUS project is an established centre of excellence in the field of cross-border access to electronic evidence in the EU and third countries. Implemented by Europol and Eurojust, the project assists over 7 800 law enforcement officers and around 500 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 and proceedings.

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, and delivering restricted online and in-person 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 Budapest Convention and 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 globally. There are three project phases:

- First phase from 2018 – 2021
- Second phase from 2021 – 2024
- Third phase from 2025 – 2027

Through the annual *SIRIUS 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. This edition of the report concludes the activities of the second phase of the SIRIUS project that ended in 2024.

Context

Several legislative changes have shaped cross-border access to electronic evidence in recent years, but the 2025 SIRIUS Electronic Evidence Situation report is predominantly impacted by the EU Electronic Evidence legislative package and the planned go-live of the decentralised IT system in August 2026. This (partial) transition from a voluntary request system to a system based on mandatory orders, creates several challenges for different types of stakeholders.

For law enforcement authorities, this transition comes with a significant reorganisation of processes to obtain data from service providers, as well as the potential involvement of the judiciary, depending on how national law enforcement authorities are designated as data requestors.

For judicial authorities, the transition results in a key role for authorities in the process to request data from service providers and the necessity to design new processes for cooperation between law enforcement and judicial authorities to accommodate the legislative changes.

For service providers, a mandatory response system with clear response times and legal certainty, requires adjustment, compared to the voluntary mechanism. However, there is uncertainty about the volume of requests that will be made via the new IT system and whether this large-scale transformation can be delivered according to the implementation plan and across all EU Member States at its start in August 2026.

In these transformative times, the 2025 SIRIUS Electronic Evidence Situation Report provides trend analyses and background information on the basis of qualitative and quantitative evidence gathered. It supports both authorities and service providers in the implementation of and preparation for this new legal instrument and future ones.

Methodology

The methodology used for this report is similar to previous editions. The SIRIUS Project utilises 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 a total of 227 responses between August and November 2025. Percentages reported are rounded for readability and therefore totals may exceed 100%.

There were 197 responses from EU Member State authorities. The survey was also open to law enforcement authorities from non-EU Member States which have operational or working agreements with Europol. There were 30 responses received from Albania, Australia, Bosnia and Herzegovina, Canada, Iceland, Moldova, Montenegro, Norway, Switzerland, Ukraine, the United Kingdom and the United States of America. The results related 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 Perspective of Law Enforcement chapter.

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, such as the SPoC network meeting in Warsaw in June 2025.

Surveys with judicial authorities

Eurojust collected feedback from judicial authorities across all EU Member States and 13 countries outside the EU, namely Bosnia and Herzegovina, Canada, Iceland, Kosovo, Lebanon, Mexico, Moldova, Montenegro, Palestine, Serbia, Switzerland, the United Kingdom and the United States of America.

The survey was administered between July and October 2025. It was disseminated through the SIRIUS Platform and circulated via Eurojust National Desks and Liaison Prosecutors, as well as through the European Judicial Cybercrime Network (EJCN) and the European Judicial Network (EJN) Contact Points. The survey was also shared within the framework of the EuroMed Justice Project and the Western Balkans Criminal Justice Project.

In total, 63 in-depth responses were received, reflecting the situation in 27 EU Member States, while 22 responses were submitted by judicial authorities from non-EU countries. This information constitutes the basis for the analysis and recommendations set out in this report.

The findings presented in this report are based on voluntary responses received through the survey and reflect the experience and perceptions of the participating judicial authorities. While the responses provide valuable practical insight into cross-border

access to electronic evidence, they may not fully capture all national practices or legislative nuances in each jurisdiction. The results should therefore be interpreted as indicative of operational trends and challenges rather than as an exhaustive assessment of national legal frameworks or practices.

Interviews with service providers

Between September and November 2025, Europol and Eurojust collected inputs from representatives of 12 service providers and one industry association, namely: Airbnb, Google, Meta, Microsoft, PayPal, Riot Games, Roblox, Snap, TikTok, OVH Cloud, Uber, Yahoo and EuroISPA.[2] 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:

- the 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;
- the impact of the upcoming E-evidence legislative package on SPoC approach and voluntary cross-border disclosure of data.

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

To ensure a continuous and comparable analysis of the transparency reports across the years since the first SIRIUS Electronic Evidence Situation Report in 2018, the service provider reports of Airbnb, Google, LinkedIn, Meta, Reddit, Snap, TikTok and Yahoo were selected as a sample for the 2025 SIRIUS report and cover the year 2024.

PERSPECTIVE OF LAW ENFORCEMENT

Examples of real cases

Europol asked 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 types of crime.[3]

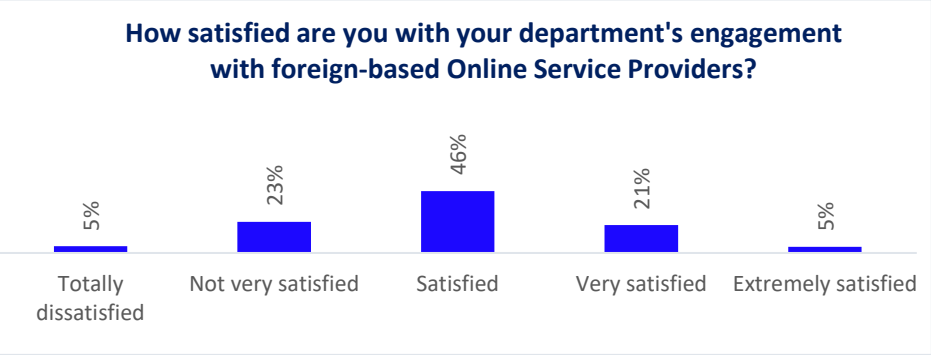
> ***'In some cases involving life-threatening situations, we were able to quickly access the [SIRIUS] guidelines and make a direct request to the respective ISP*** *without having to spend time searching for contact details, which was very important in these cases as time was of the essence.'*
>
> *'There are multiple cases where* ***information gained from online service providers has been vital****. Especially in cyber-enabled crimes, virtual currencies are quite common. We also deal a lot with social media platforms in CSAM cases. In these cases, co-operation with online service providers works best. […]'*
>
> ***'When investigating call centre cases, requests are made to [providers and] very often exceptionally good answers are received****, which results in the conviction of many individuals for committing organized crimes.'*
>
> *'I have* ***solved a big case, related to cybercrime, in which I have sent many direct requests*** *in order to obtain electronic evidence.'*
>
> ***'Different direct requests to crypto-asset service providers helped us gather very beneficial information and evidence in financial investigations that would be otherwise not possible to obtain at all.*** *SIRIUS tools and guidelines helped us with analysis, sorting, evaluating and visualisation of the data, so we could be more efficient in the realm of time and finance.'*
>
> *'[Through data provided by a request made to a service provider]* ***in a crypto-currency case, we were able to identify the sender as well as the recipient of the transaction*** *which helped to bring the investigation forward.'*

*'In some cases, **we were able to obtain server images and basic subscriber data through Direct Requests in countries outside the EU** that contained very important data for the investigations […]. The MLAT process is generally too slow, it would be useless in the case. […]'*

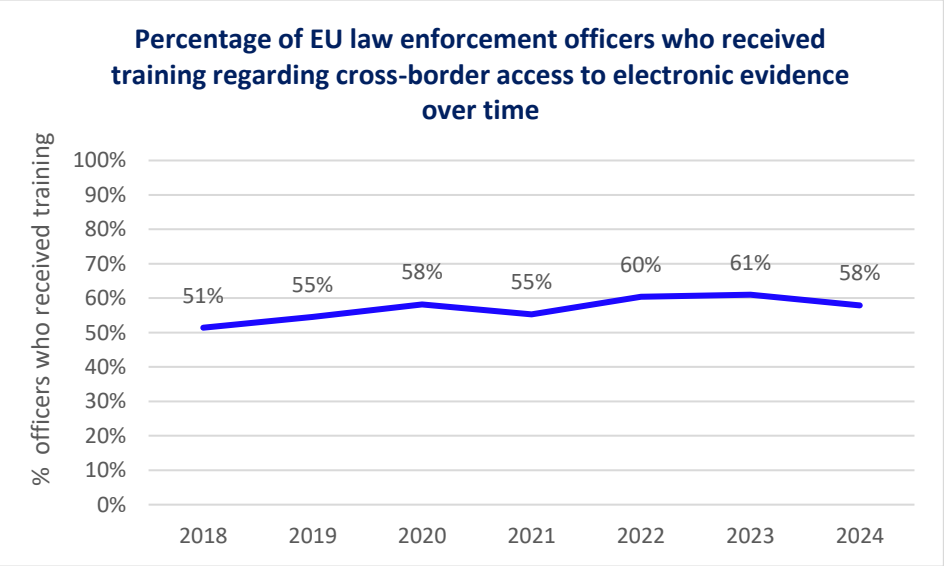
Engagement of EU law enforcement with foreign-based service providers

Engaging with foreign-based service providers can pose a threefold challenge for law enforcement: adherence to domestic legislation, international legislation and agreements, and that of the service provider's jurisdiction. When cooperation is volunatry, the different service provider requirements and company policies add an additional layer of complexity to this.

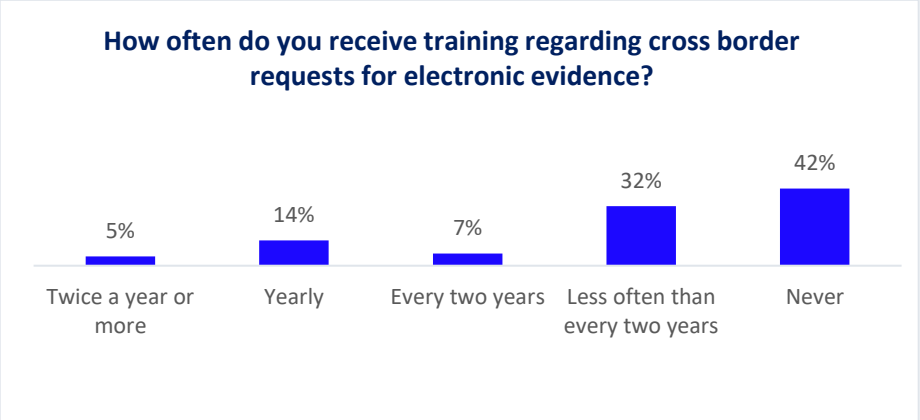
Despite this landscape in which law enforcement currently operates and the persisting challenges,[4] 72% of EU law enforcement officers reported being satisfied, very satisfied or extremely satisfied with their department's engagement with foreign-based service providers in 2024. These latest figures confirm the consistently high levels of 70% or more since 2021.[5]



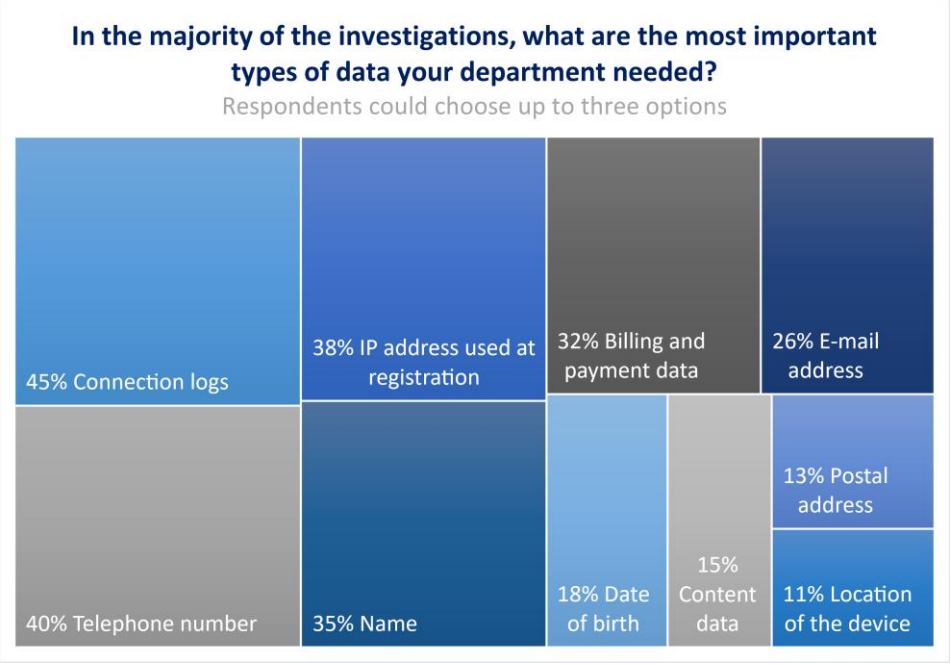
The challenging landscape of cross-border requests for electronic evidence demands regular training to educate and update officers on the latest developments in the field. In 2024, the majority of EU law enforcement officers (58%) reported having received at least some training regarding cross-border access to electronic evidence. This year's result shows a slight decrease compared to what was reported for 2023, falling back to 2020-levels.



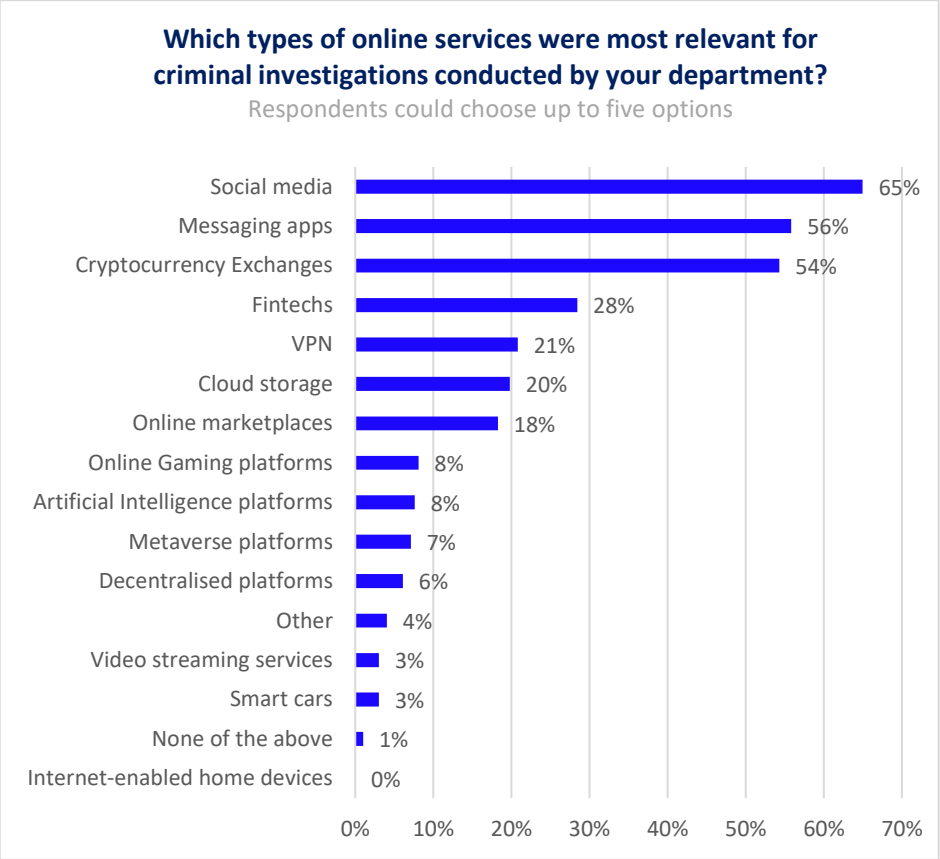
Overall, training remains the norm rather than an exception, but 32% of the respondents indicated that they have received training less often than every two years and 42% have never received training to request cross-border access to electronic evidence.



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 2024, 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), telephone number and the IP address used when first registering to the service. With connection logs and IP address at registration remaining top-ranked datasets, 40% of respondents added that telephone numbers were also among the most important types of data requested (up from 28% in 2023).



Providers of many different types of services can be deemed relevant by law enforcement for their investigations. In 2024, the five most important types of service providers were: social media platforms, messaging apps, cryptocurrency exchanges, fintechs (e.g. online payment and broker services except cryptocurrency) and Virtual Private Network (VPN) providers. The result largely reflects the last few years, with fintech firms pushing cloud storage providers out of the top five in 2024.



In contrast to the last two years, AI platforms received substantial votes from survey respondents for the first time, with 8% in 2024 (cf. 0% in 2023; 2% in 2022). With AI platforms being in use by perpetrators, the relevance of non-content data, e.g. subscriber or traffic data, and content data from these platforms becomes increasingly relevant in investigations.

On the other side, AI-related innovations also continue to be one of the driving factors to impact the work of law enforcement. Survey respondents argue that advancements in AI are transforming law enforcement by reshaping how electronic evidence is handled and that these technologies present both challenges and opportunities The increasing volume and complexity of electronic evidence that make evidence identification, gathering and analysis more difficult are particularly challenging, as is the emergence of new crime phenomena in virtual environments. On the other hand, AI can aid investigators by processing large datasets and facilitating communication among authorities. Some survey respondents stress the need for law enforcement to advance their tools and for training and international cooperation to adapt to these evolving technologies.

Subsequently, this section presents a selection of statements providing first-hand accounts from the field related to AI:

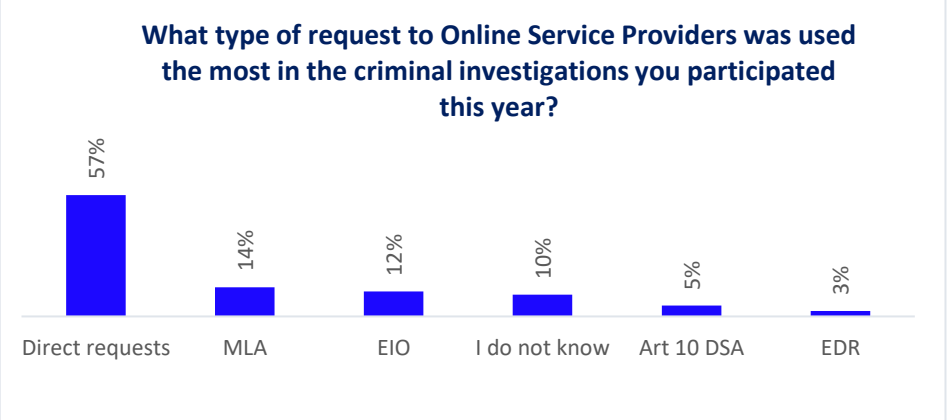
> *'**It will be a challenge but also an opportunity to aid the investigator**, it can easily process enormous data, trace, and filter suspects and also facilitate the communication of the European authorities.'*
>
> *'**Transformations in technology are reshaping every layer of law enforcement work with electronic evidence.** These technologies influence how evidence is generated, discovered, interpreted, and presented in court.'*
>
> *'These transformations will certainly affect the work in the area of electronic evidence. **The more complex devices are used, the more evidence will be requested to investigate.**'*
>
> *'**The evidence identification, gathering, preservation processing and analysis will be more difficult.**'*
>
> *'AI is speeding up and improving our efficiency. Image classification technologies are essential for my field of work. However, **I believe it's important to use AI exclusively offline or on internal networks to prevent sensitive data from being disclosed."***
>
> *'**Artificial intelligence will make it difficult to prove, especially in the field of AI-generated data, programs, videos, images and audio, as it will have to be checked for real or non-real content.** In addition, the forensic analysis of AIs and their results during AI interventions will be a challenge. Virtual Reality and Augmented Reality could create new unknown crime phenomena.'*
>
> *'**Advancements in AI, VR, AR, and other emerging technologies are transforming the way law enforcement handles electronic evidence.** These innovations present both challenges and opportunities – not only in OSINT but across digital forensics, investigative workflows, and real-time crime analysis. For LEAs and the tech companies supporting them, staying ahead requires continuous adaptation to these rapidly evolving tools.'*
>
> *'**Technological transformations such as AI, VR and AR are exponentially increasing both the volume and complexity of electronic evidence.** I expect this trend to intensify, with a growing diversity of crimes, new virtual environments and more sophisticated concealment methods, making detection, preservation and attribution increasingly challenging**. Law enforcement will need advanced tools, training and international cooperation to keep pace.**'*

Submission of cross-border requests

Direct requests for voluntary cooperation to service providers for the 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 (57%) reported that direct requests were the most used type of requests to service providers in 2024.

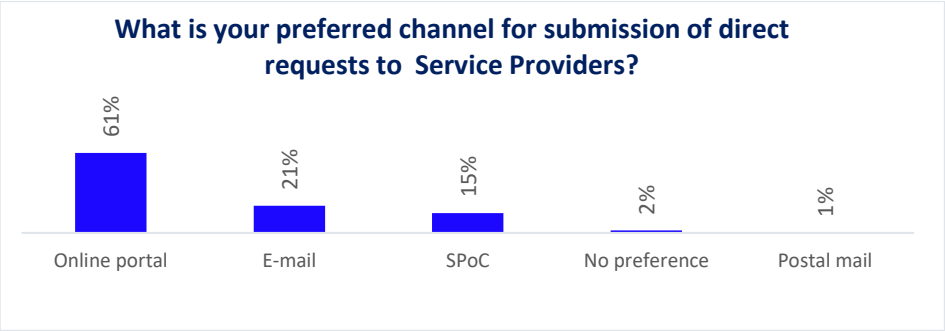
When direct requests are not possible, MLA or European Investigation Orders (EIOs) are often necessary to obtain data to continue the investigation. It is important to note that

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 types of requests might be used within one unique case – when, for example, authorities complement a direct request via judicial cooperation channels. There are service providers that do not cooperate with foreign authorities on a voluntary basis, or that are unable to do so in accordance with domestic regulations. Emergency Disclosure Requests (EDR) – direct requests for voluntary cooperation in emergency circumstances, usually those involving an imminent threat to life – accounted for 3% of the criminal investigations in 2024 according to the survey respondents.

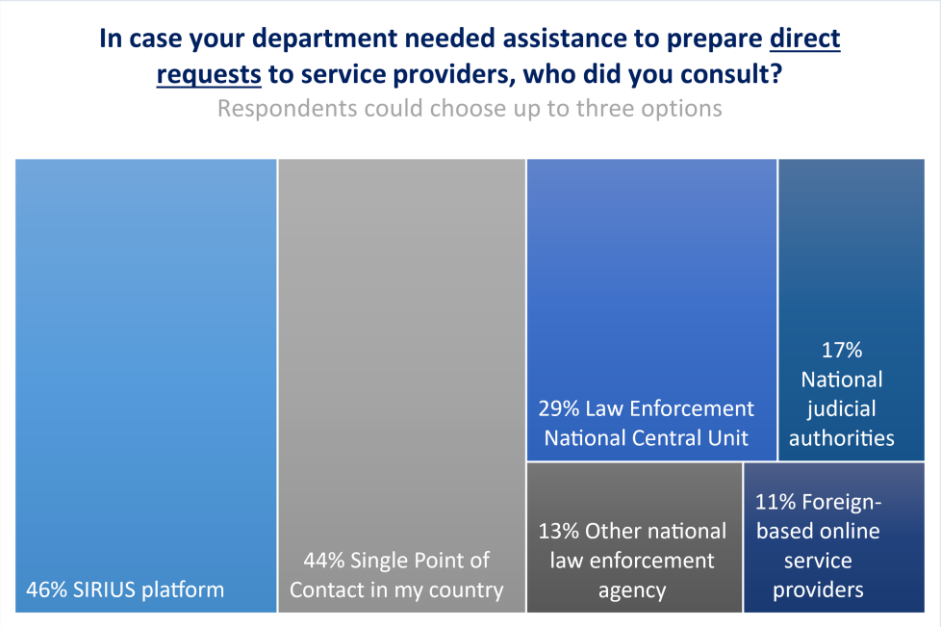


The DSA has been fully applicable since February 2024 and rules for designated Very Large Online Platforms and Very Large Online Search Engines (VLOPs and VLOSEs, respectively)[6] since 2023[7]. Under the DSA, EU law enforcement can submit orders requesting service providers to provide information pursuant to Article 10 of the DSA, in combination with a legal basis under EU or national law, to VLOPs and VLOSEs. In 2023 and 2024, the number of respondents that indicated they had used Art. 10 of the DSA as basis for requests remains at 5%.

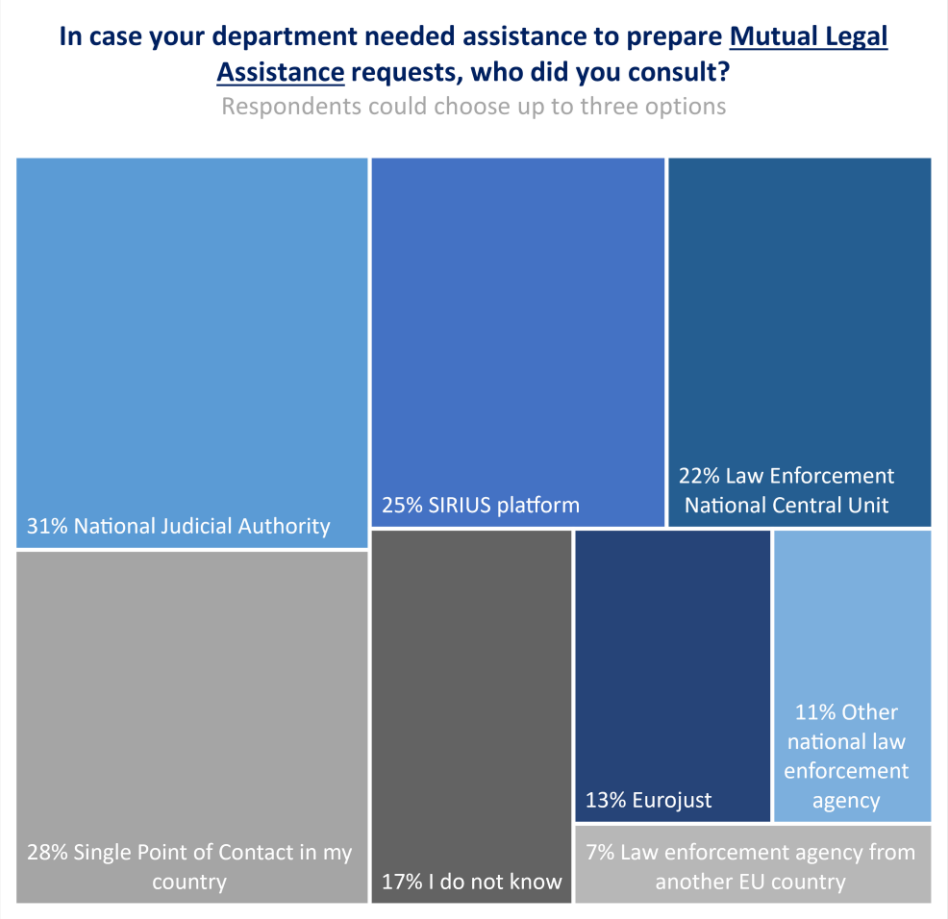
Because direct requests are considered voluntary cooperation, service providers may set up their own rules and requirements for competent authorities to adhere to. The channel for submitting requests is one such requirement that varies among service providers. Some providers choose to create dedicated online law enforcement portals to submit their requests. Other providers do not have their own online law enforcement portal, but accept requests via third-party online portals offered by specialised companies. The benefits of using online portals include a better status overview on the request progress, secure downloads of responses and streamlined communication between competent authorities and representatives of service providers. In 2024, the majority of officers surveyed (61%) prefer submitting their requests via online portals, rather than via e-mail (21%) or through a SPoC (15%). While the use of online portals decreased by 5% compared to 2023, falling back to levels of previous years (60% in 2021; 59% in 2022), the use of SPoCs increased by 3% according to the survey respondents. The results are presented overleaf.



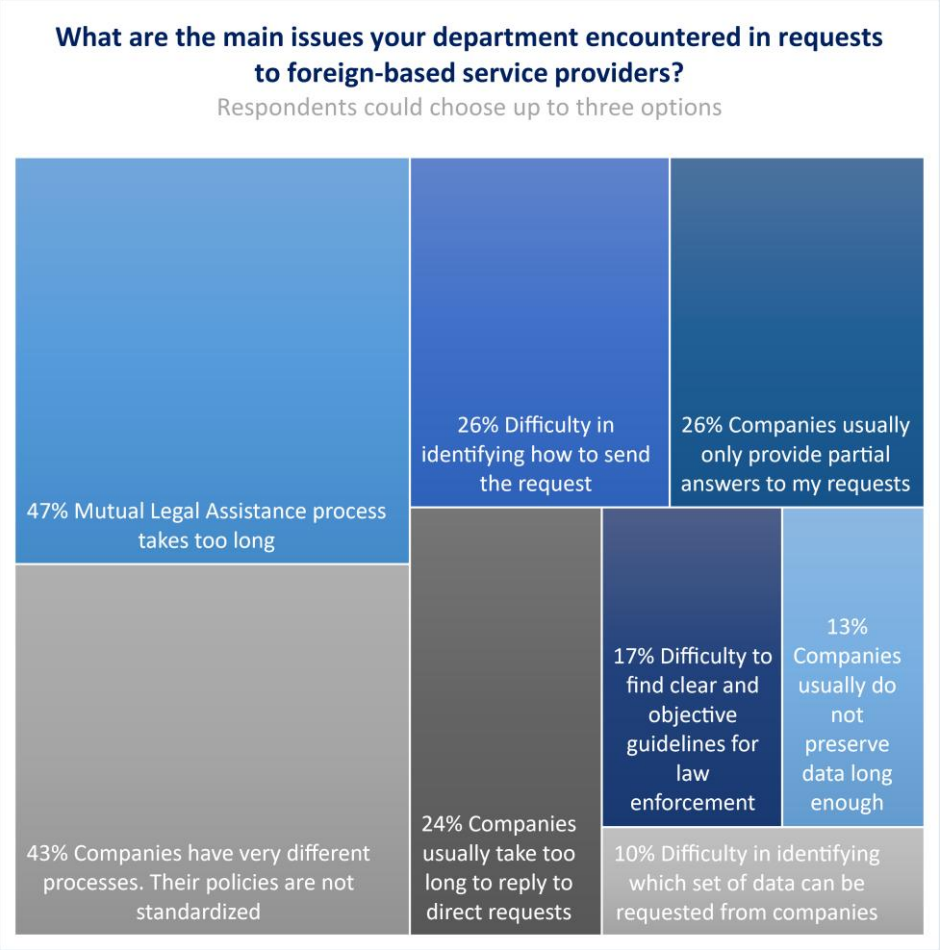
The 2024 survey presents a clear message on who to consult in case cross-border access to electronic evidence is required: specialised centres of excellence are the first choice for law enforcement seeking assistance. Overall, the SIRIUS Platform remains the first ranked source of information in 2024 for law enforcement officers who need assistance to prepare direct requests (46%) and support from the EU level. Together with SPoCs (44%) and the law enforcement national central units (29%), who may be the hosts of SPoCs and support on a national level, complementing the assistance available to law enforcement.



When it comes to assistance relating to MLA, national judicial authorities have surpassed SPoCs as the first point of contact for assistance in 2024 (31% and 28%, respectively).



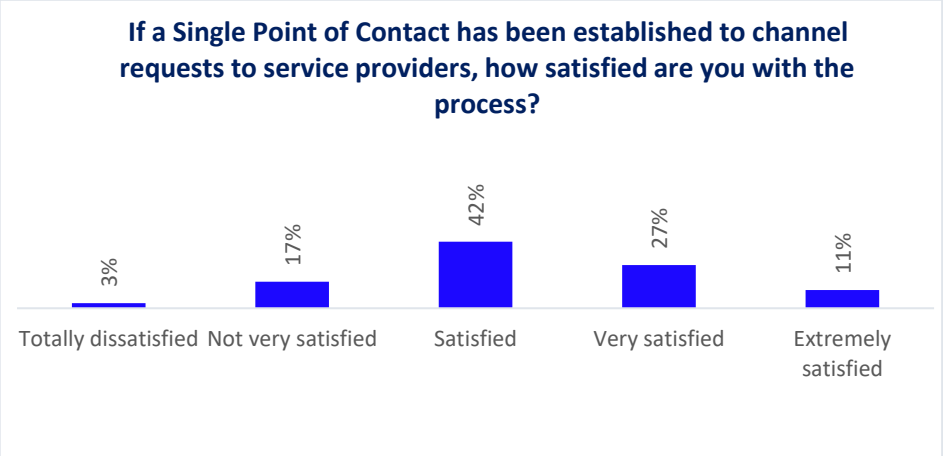
Asked about the main issues encountered in requests to foreign-based service providers, the top issues remain relatively similar recent years: lengthy MLA process; different company policies and not standardised processes; partial answers to requests; difficulties identifying how to send a request; and long response times.



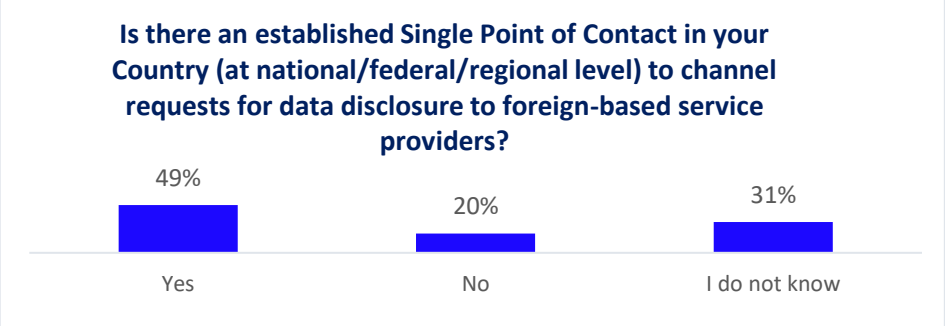
Other issues that were mentioned by less than 10% of officers included:

- Requests are usually only accepted in English, not in my own language;
- Information is only available in English, not in my own language;
- Companies change processes and response formats too often;
- Lack of technological resources to analyse responses from service providers;
- Companies' guidelines are too complicated or too long;
- Companies' responses are not easy to analyse and understand.

The overall importance of SPoCs for law enforcement is still unrivalled, and this is demonstrated by high satisfaction levels reported in the survey, with 80% of the officers' reporting being satisfied or more than satisfied with their SPoCs.



Setting up a SPoC can reduce or eliminate some of the issues listed above and help to centralise and streamline the request process, generally improving request success rates and quality. However, with these benefits in mind, it is surprising that more than half of the survey respondents were either unsure or answered that there is no SPoC in their country.

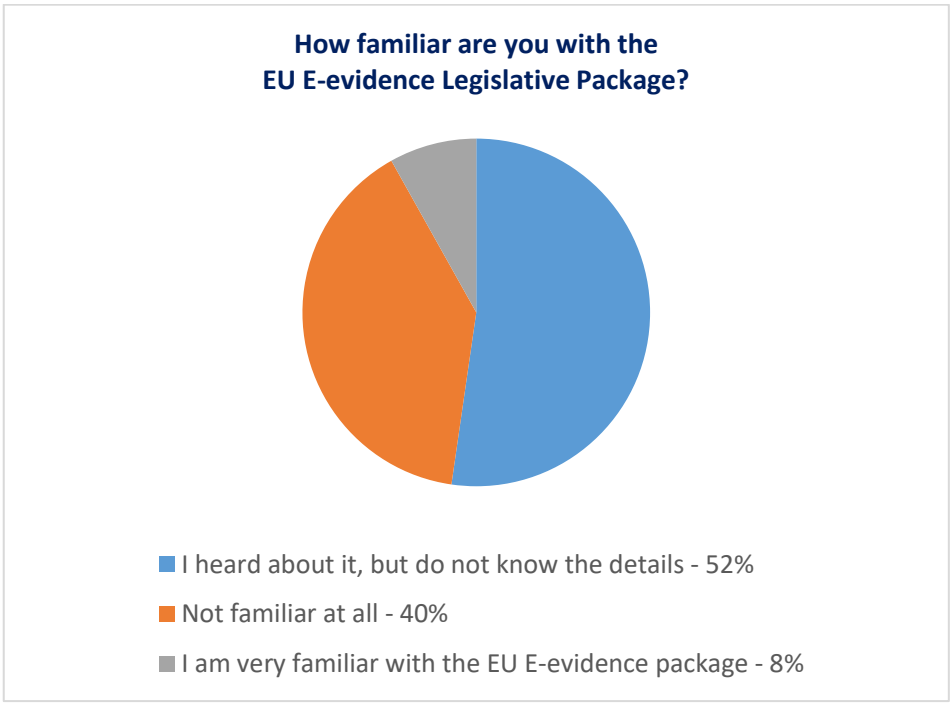


Via direct engagement with EU law enforcement authorities, SIRIUS identified 36 law enforcement agencies acting as SPoCs in 22 Member States: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic[8], Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Slovenia, Spain and Sweden. Additionally, another six law enforcement agencies and one judiciary authority in four non-EU countries have SPoCs established as well: Iceland, Georgia, Norway and the United Kingdom, resulting in a total of 43 SPoCs identified in 26 jurisdictions (22 EU MSs / 4 Non-EU).

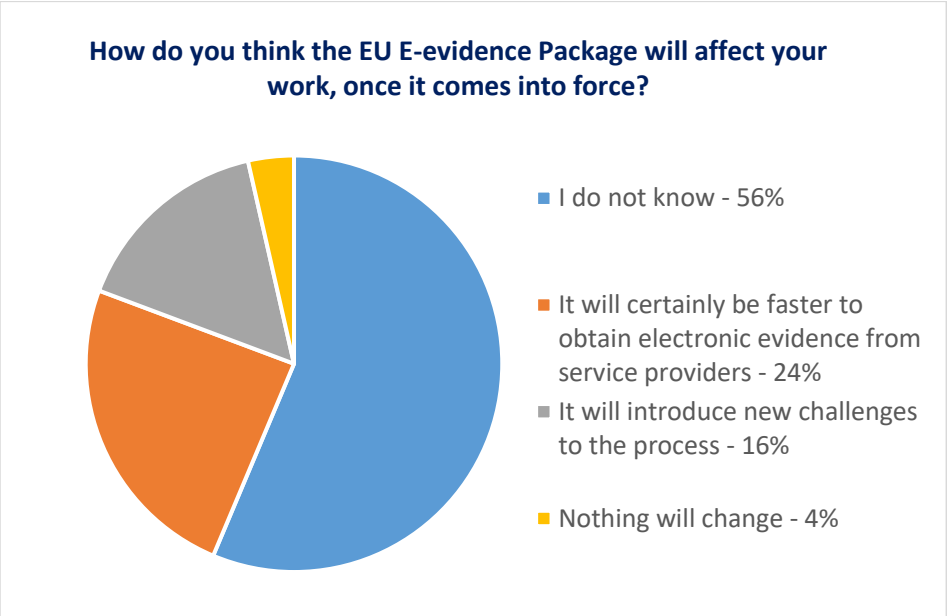
EU Electronic Evidence legislative package

The EU Electronic Evidence legislative package will introduce new instruments for authorities to request data preservation and data disclosure from foreign-based service providers offering their services in the EU. The legislation will offer a new system based on cross-border mandatory orders with short deadlines, resulting in profound changes to the electronic evidence gathering process.

The date of entering into application of the EU Electronic Evidence Regulation and implementation of the EU decentralised IT system for requests is nearing (18 August 2026). However, the 2025 survey for law enforcement revealed that knowledge about and familiarity with the new legislative framework still remain low. Respondents reported not being familiar in 40% and not knowing the details in 52% of all answers. 8% of survey respondents reported that they were very familiar with the new legislation, which is a 4% increase compared to the last reporting period. Overall, the numbers are low given the potential impact the Regulation will have on the process of acquisition of electronic evidence. In addition, the lack of knowledge dissemination and training poses a risk that can jeopardise investigations.



Among the officers who indicated that they had heard about the EU Electronic Evidence legislative package, or those that are very familiar with it, only about one quarter are positive about the effect it may have (24%). These officers believe it will be faster to obtain electronic evidence from service providers. On the other hand, 16% of the officers surveyed believe that there will be additional challenges to the process. Only 4% responded that nothing will change. The remaining 56% of respondents are unsure about the effects the new legislation will have on their work. This is an increase of 6% since last year. The results are presented overleaf.



Faster response times are a key potential improvement underlined by law enforcement survey respondents. Among officers who reported that it will certainly be **faster to obtain electronic evidence** from service providers, the following comments have been selected:

> *'[It will be faster] because of the obligation to respond within 10 days and within 8 hours in cases of emergency, and the obligation to appoint a legal representative in the EU.'*
>
> *'I hope that there will be a uniform guideline across all Member States.'*
>
> *'It is important to create a common platform and uniform procedures for requests.'*
>
> *'Response is mandatory, deadlines are shorter.'*
>
> *'It will be easier to obtain e-evidence from foreign service providers.'*
>
> *'There are prescribed time frames within the legislation which will aid the process. In Ireland, however, we may find a significant increase in workload in assisting other [EU] Member States.'*

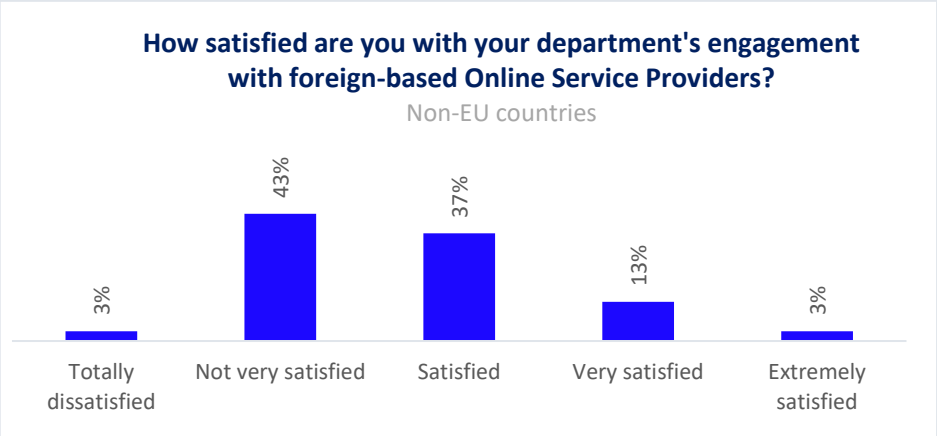
Among officers who reported that the new policy will introduce **new challenges to the process**, the following comments have been selected:

> *'To be effective, a (semi) automated request tool is needed on a [Law Enforcement] level. If not, the efficiency will lack and [Judidical Authorities] will be submerged by paperwork / mailwork.'*
>
> *'The e-evidence regulation is a great tool, however Denmark is not part of it, hence we fear that the implementation of the regulation will mean that voluntary disclosure, which we rely heavily on, will not be prioritised by the OSPs.'*

As the practical application of the new rules is still to come into effect in August 2026, EU law enforcement officers have yet to experience any direct effect. Consequently, the responses collected largely mirror what was reported in the previous edition of this report.

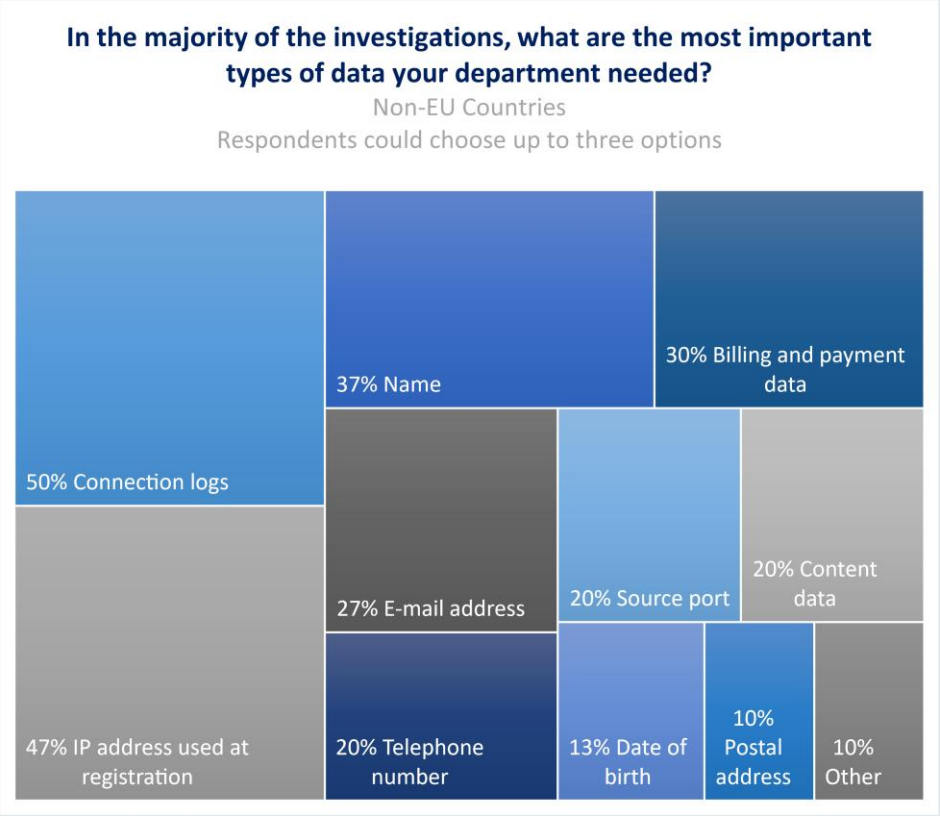
Electronic evidence for law enforcement in non-EU countries

Law enforcement authorities from countries outside of the EU, with which Europol has operational or working agreements, were invited to respond to the same survey used to collect feedback from EU officers. A total of 30 responses were received from Albania, Australia, Bosnia and Herzegovina, Canada, Iceland, Moldova, Montenegro, Norway, Switzerland, Ukraine, the United Kingdom and the United States of America. In 2024, 53% of officers from non-EU countries reported being satisfied or more than satisfied with their department's engagement with service providers, compared to 72% in the EU. Satisfaction reported by non-EU respondents dropped from 78% to 53%. There may be several reasons for this. First, methodological aspects may have skewed the responses, as the number of non-EU survey participants has changed compared to the previous year and the survey is not designed to restrict which entities may participate so as to allow as broad a response base as possible. Second, there may have been significant changes in the authorities' request process and response policies from service providers. To determine the actual cause, further research is necessary.



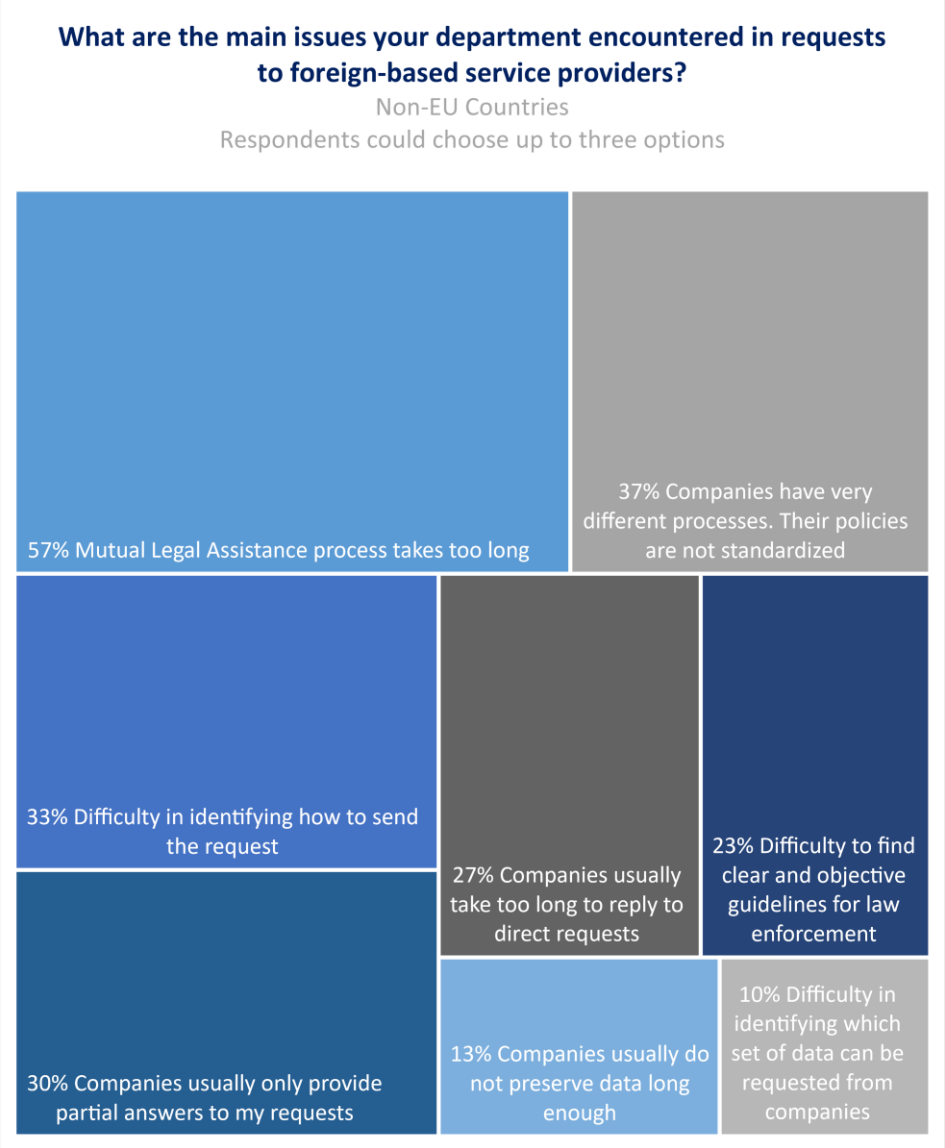
Direct requests for disclosure of data under voluntary cooperation are the most important types of requests for respondents from non-EU countries. At 57% this is a similar proportion of the responses than in the EU.

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 20% of respondents have indicated that content data is one of the most important types of data in criminal investigations in non-EU countries. Respondents have increasingly selected this category in their responses in recent years).



The three main issues encountered by non-EU law enforcement officers when submitting requests to foreign-based service providers in 2024 were almost the same as in the EU and remained stable over the years surveyed. The main issue is that the MLA process takes too long, followed by the fact that service providers' policies are not standardised. The third most frequently mentioned issue by officers is the difficulty in identifying how to send their requests.

The similarity of 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 service providers' policies for responding to requests are still cumbersome.



PERSPECTIVE OF JUDICIAL AUTHORITIES

Cross-border access to electronic evidence by EU judicial authorities: modalities for obtaining data from foreign service providers

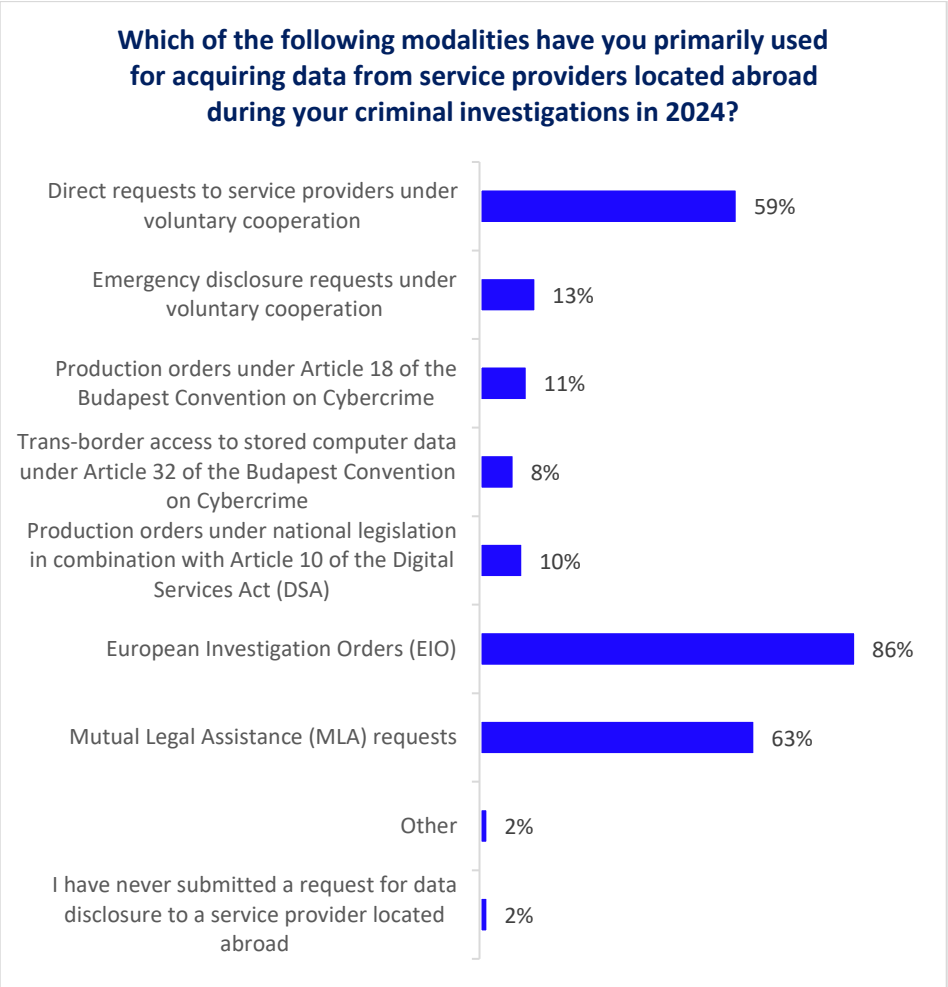
In 2024, the modalities used by EU judicial authorities to obtain electronic evidence from service providers located in different jurisdictions largely mirrored those reported in the previous year.

Significant advancements are expected in the legal landscape governing access to cross-border electronic evidence with the introduction of the EU Electronic Evidence legislative package, the Second Additional Protocol to the Budapest Convention on Cybercrime and the United Nations Convention against Cybercrime. Designed to be more efficient, these instruments are set to substantially enhance the toolkit available to EU judicial authorities by providing more streamlined and enforceable mechanisms for obtaining electronic evidence across borders. However, while these developments are anticipated in the near future, the legal landscape for cross-border access to electronic evidence in 2024 remained largely unchanged compared to previous years. It is therefore unsurprising that traditional methods of international cooperation in criminal matters – namely the European Investigation Order (EIO) and MLA requests – continued to be the modalities most frequently used by the surveyed EU judicial authorities in their criminal investigations in 2024.

According to the survey, 86% of responding authorities primarily used the EIO when seeking data from foreign-based service providers. MLA requests followed as the next most frequently used tool, identified as the primary modality by 63% of respondents.

Direct requests to service providers under voluntary cooperation constituted the third most common approach, used by 59% of surveyed authorities. In contrast, other mechanisms – such as production orders under national law combined with orders under Article 10 of the Digital Services Act (DSA), production orders pursuant to Article 18 of the Budapest Convention, trans-border access to stored data with consent or where publicly available under Article 32 of the Budapest Convention, and emergency voluntary disclosure requests – were indicated by significantly fewer respondents. These tools therefore continued to play only an incremental role in 2024.

The 2024 findings are fully aligned with the trends observed the year before. In 2023, judicial authorities likewise opted for traditional cooperation mechanisms more frequently: 74% of respondents reported using MLA requests and 71% relied on the EIO as their primary modalities, followed by 47% who used voluntary direct requests to service providers. The near-identical rankings in 2023 and 2024 underscore the stability of existing practice, which is likely to change once more efficient legal tools provided by legislative and policy developments become applicable.

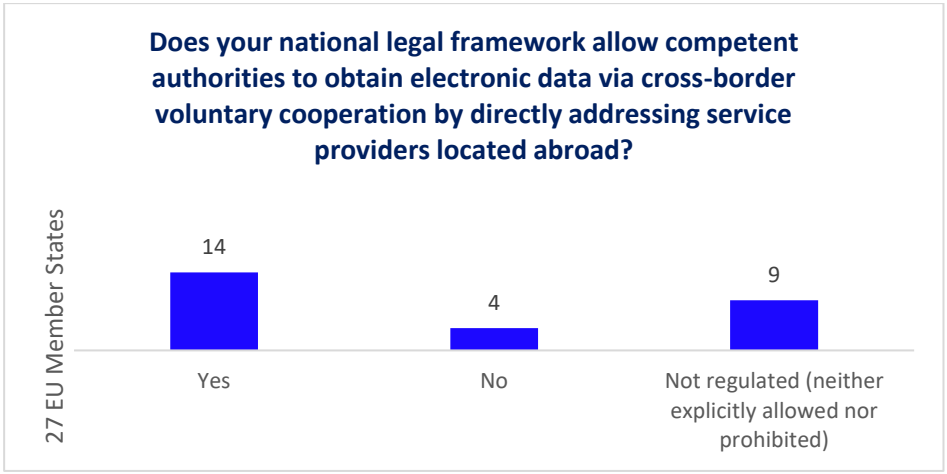


Direct voluntary cooperation with service providers

National legal framework

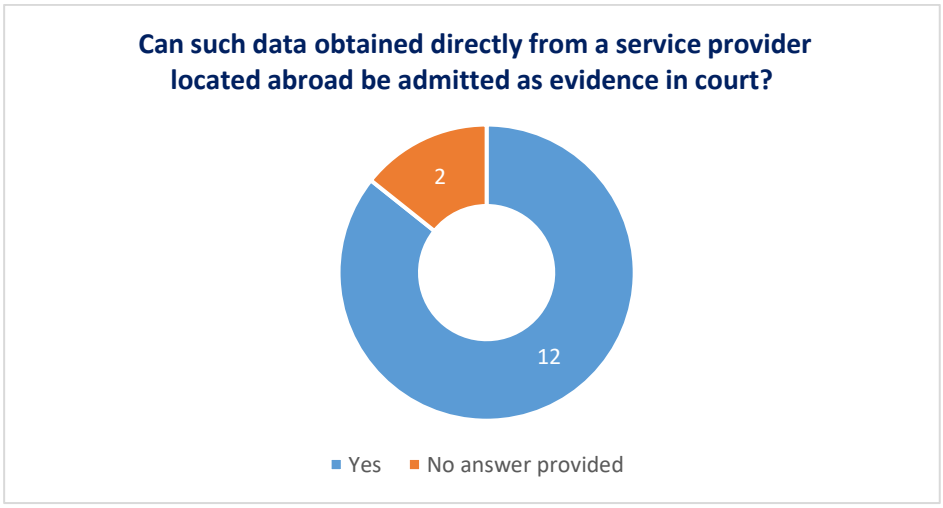
Direct requests for data refer to requests submitted by competent authorities directly to foreign-based service providers for the preservation and/or production of non-content data on the basis of voluntary cooperation. As these requests are not legally binding, their effectiveness depends on service providers' internal policies on cooperating with public authorities, and the relevant domestic legislation in both the requesting and the requested jurisdictions. In practice, this results in varying conditions and procedures governing the issuance and execution of such requests.

Survey results indicate that the national legislation of a considerable number of EU Member States (14 out of 27) permits the collection of electronic data through voluntary cooperation by directly contacting service providers located abroad. However, the findings also reveal that competent authorities' interpretation of the possibility to use this modality may differ due to the absence of explicit regulation. While only four Member States were identified as not allowing the use of direct voluntary cooperation for obtaining evidence, respondents from nine Member States reported that their national legal frameworks neither explicitly allow nor explicitly prohibit the collection of electronic evidence through voluntary cooperation channels.



The complexity of the direct voluntary cooperation mechanism is even more evident when considering whether electronic data collected directly from a service provider situated abroad through a direct request for voluntary cooperation can be admissible as evidence in court in accordance with the applicable national legal framework.

In this regard, the answers received reveal that in the vast majority of the EU Member States whose legal frameworks permit competent authorities to obtain electronic data via cross-border voluntary cooperation (12 out of 14), such data can be admitted as evidence in court.



Some of the respondents shared additional explanations and/or direct references to their national legislation:

France	*Evidence provided voluntarily is admissible as long as it is clear that cooperation is not mandatory.*
Germany	*In principle, contact to obtain the data is only permitted if direct contact with the service providers is permitted; for example within the EU or in the USA. In the case of third countries, an MLAT must be issued in order to request the release of the data.*
Hungary	*In Hungary, the XC Act of 2018 on Criminal Procedure, section 265/A, provides: if it is not prejudicial to the interests of the criminal proceedings, the prosecution and investigative authorities may also request information by inviting the requested body to provide it voluntarily, without any sanction being imposed.*

Luxembourg	*Service providers located abroad agree to respond to direct requests from Luxembourg law enforcement/judicial authorities as part of voluntary cooperation following requests submitted through the online request system addressed to law enforcement agencies. Only certain data, defined by the operators, are provided on a voluntary basis. To access data other than those defined, it is mandatory to go through MLA/EIO.*
The Netherlands	*Our national legal framework does not contain any specific rules regarding voluntary cooperation, whether domestic or international. Our direct requests to foreign service providers are based either on the national law of the country in which the provider is located or on mutual agreements between the Netherlands and that other country. We ask other countries to approach the relevant Dutch authorities before directly submitting requests to service providers based in the Netherlands.*
Sweden	*We do not have any laws in Swedish legislation prohibiting the admissibility of any kind of evidence and that includes electronic data as well. We have however legislation that prohibits prosecutors and the police force gathering information on voluntary cooperation if the country where the service provider is located does not allow that kind of direct contact.*

Challenges related to direct voluntary cooperation with service providers located in foreign jurisdictions

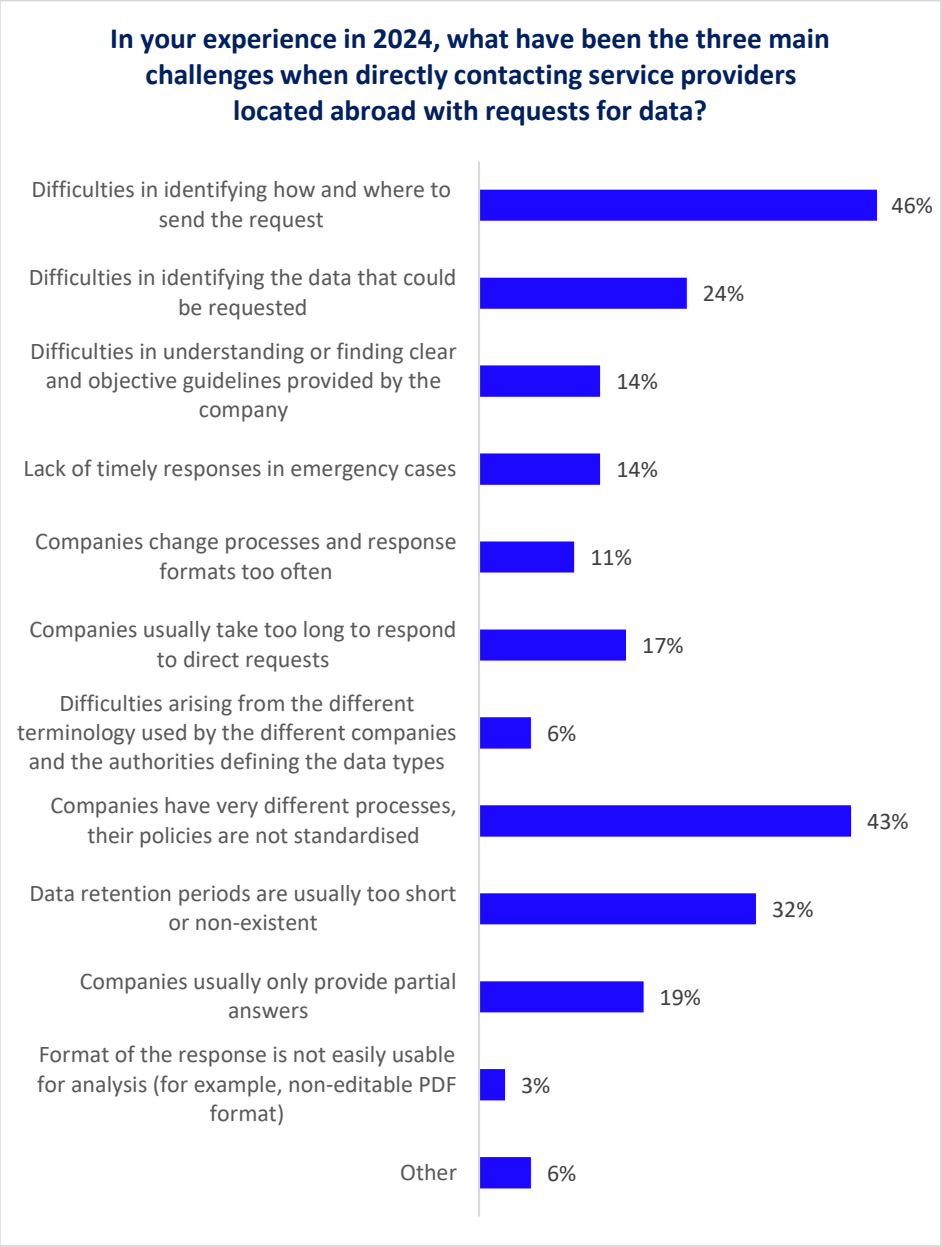
Even though the direct voluntary cooperation mechanism is often perceived as the fastest channel for competent authorities to obtain non-content data, it is also not immune to obstacles. In this regard, judicial authorities were asked to identify the three most challenging aspects faced when directly contacting service providers located abroad with requests for electronic data under voluntary cooperation.

The collected responses reveal that the predominant issue in 2024 for most respondents was the difficulty in identifying how and where to send the request (highlighted by 46% of respondents). Issues related to different processes and policies applied by service providers were identified as the second most prominent problem in investigations carried out in 2024 (43% of respondents). The third most prevalent challenge indicated by the EU judiciary concerned data retention related challenges (32% of respondents). Other issues identified are related to the difficulties in identifying the data that could be requested (24%).

Less commonly reported problems were as follows:

- Companies usually only provide partial answers: 19%
- Companies usually take too long to respond to direct requests: 17%
- Difficulties in understanding or finding clear and objective guidelines provided by companies: 14%
- Lack of timely responses in emergency cases: 14%
- Companies change processes and response formats too often: 11%
- Difficulties arising from the different terminology used by the different companies and the authorities defining the data types: 5%

- The format of the response is not easily usable for analysis (for example, non-editable PDF format): 3%
- Other: 4% (indicated by the respondents as related to costs of the requests; difficulties in identifying which countries allow their service providers to accept voluntary cooperation requests)



Compared to previous SIRIUS EU Digital Evidence Situation Reports[9], the most pressing challenges faced by judicial authorities when seeking data through voluntary cooperation mechanisms remain largely unchanged, reflecting a consistent pattern of recurring issues. These challenges refer to:

- Data retention related issues;
- Difficulty in identifying the applicable jurisdiction;
- Diversity in policies and processes in place among service providers.

The challenges identified stem largely from a fragmented legal framework, limited enforceability of voluntary cooperation mechanisms and legal uncertainty for both public authorities and service providers, including the risk of potential conflicts of law. A key solution lies in the implementation of the EU Electronic Evidence legislative package, which is expected to streamline cross-border judicial cooperation by introducing binding rules for the preservation and production of electronic evidence and shorter timeframes for their execution. In particular, the obligation for service providers falling under the scope of this new legal framework to designate an establishment or appoint a legal representative in the EU, together with clear and secure communication channels between authorities and providers through a dedicated decentralised IT system, should significantly improve the efficiency, clarity and enforceability of data requests. In parallel, there was an increased policy focus on data retention in 2024, alongside the launch of an EU-level impact assessment in 2025.

Extraterritorial powers: production orders and requests with extraterritorial effects

Extraterritorial powers – domestic orders or requests with effects beyond national borders – have become indispensable tools to ensure that legal processes are not obstructed by the geographical dispersal of data. These powers enable competent authorities to request data from service providers regardless of the location of the data, and in some cases, regardless of the service provider's place of establishment, thus overcoming traditional territorial limitations. While typically used to obtain limited data sets, such as subscriber information or domain name registration details, these powers are critical for initiating investigations and prosecuting crimes in the digital environment.

Budapest Convention on Cybercrime

As regards the availability of such extraterritorial powers in 2024, EU judicial authorities were asked whether their national legal framework provides a legal basis for the issuance of:

- Production orders for data from 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 from service providers located abroad, in possession or control of the sought information, following the model of Article 7 of the Second Additional Protocol of the Budapest Convention; 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 of the Budapest Convention.

In this regard, EU judicial authorities from 18 Member States 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 13 EU

Member States already provide a legal basis for the issuance of production orders following the model of Article 7 of the Second Additional Protocol and 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 nine Member States 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 all of those Member States being a Party to the Convention).

Some of the respondents shared additional explanations and/or direct references to their national legislation:

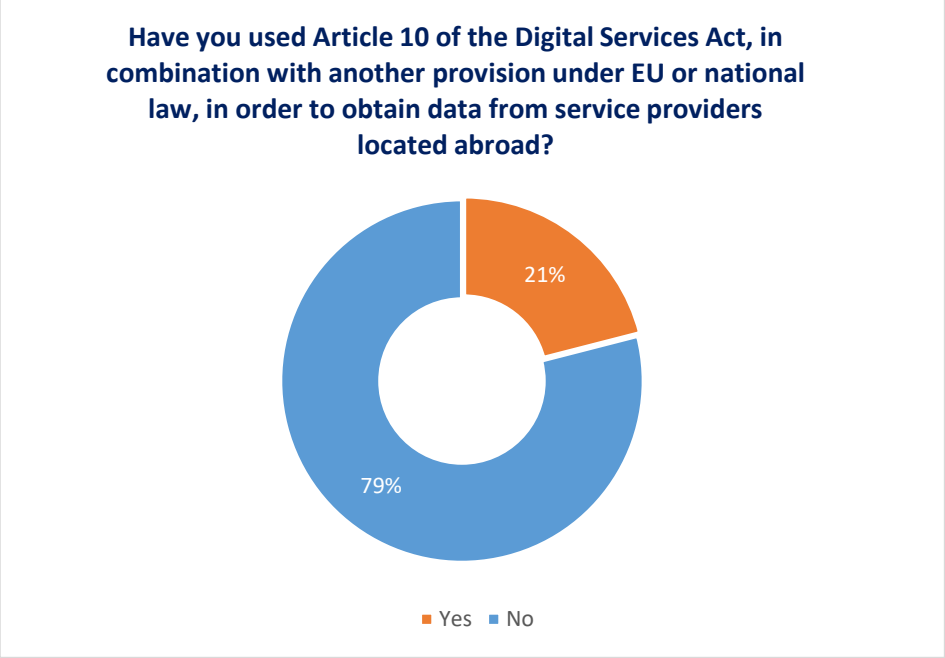
The Netherlands	*Our national legislation follows the model of Art. 18 of the Budapest Convention on Cybercrime. At the moment our national legislation has no provisions that allow us to directly send requests to service providers in other countries.*
Czech Republic	*Articles 78 and 79 of Code No. 141/1961 Coll., Criminal Procedure Code, concern orders for the surrender and seizure of items relevant to criminal proceedings, and the provisions of § 8 concern requests for publicly binding decrees. Such production orders are in the Article 88a of Criminal Procedure Code.*

Digital Services Act

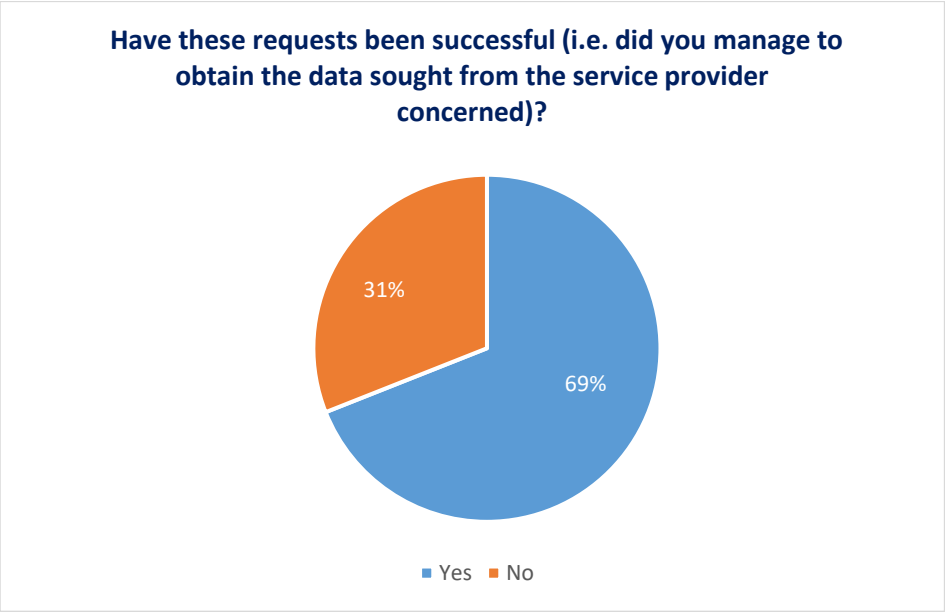
While awaiting implementation of new legal instruments such as the Second Additional Protocol and the Electronic Evidence Regulation, Article 10 of the DSA already establishes common rules for information sharing orders directed at intermediary service providers in the EU.

It is important to note that Article 10 does not grant new powers to competent national authorities. Instead, it requires providers to give information concerning orders for data disclosure which fulfil the criteria under Article 10 of the DSA and are issued under already existing EU or national laws (such as provisions implementing Article 18 of the Budapest Convention on Cybercrime into national legislation). In addition to minimum formal requirements for orders, Article 10 also regulates language requirements, user notification, confidentiality, transmission of orders, service providers' obligations and conditions to limit the scope of Article 10 of the DSA in the interest of the prevention, investigation, detection and prosecution of criminal offences or criminal procedural law in general.

Regarding the application of Article 10 of the DSA, the survey results show that 21% of the EU judicial authorities surveyed used this provision in 2024, in combination with another EU or national legal basis, to obtain data from service providers located abroad. This represents a significant increase compared to the previous year, when only 4% of respondents indicated that they had ever relied on Article 10. This marked growth can largely be attributed to increased awareness among competent authorities of the existence, scope and practical applicability of this provision.



In addition, the survey indicates a high success rate in obtaining the requested data when Article 10 was used in combination with another EU or national legal basis. This positive outcome appears to have contributed to greater confidence in and preference for this modality among competent authorities in 2024, reinforcing its perceived effectiveness as a tool for cross-border data acquisition.



These findings underline the importance of continued dissemination efforts, guidance and targeted training to support the effective and consistent use of the DSA's provisions by judicial authorities across the EU.

Judicial cooperation

As highlighted by the survey findings presented above, judicial cooperation instruments remain essential for enabling cross-border access to electronic evidence. Based on bilateral or multilateral legal frameworks, these instruments allow competent authorities in one jurisdiction to lawfully request and obtain electronic evidence held by service providers established in another country.

Within the EU, access to electronic evidence through judicial cooperation requires the issuance of an EIO when requesting data from another Member State, with the exception of Denmark and Ireland. Requests addressed to Denmark, Ireland or to third countries must follow MLA procedures. These mechanisms continue to represent the primary and preferred channels for EU judicial authorities to obtain electronic data across borders.

However, both EIOs and MLA requests were not originally designed to address the specificities of electronic evidence. The volatile nature of digital data, differing national procedural requirements and varying response times pose significant challenges to their effectiveness. As a result, delays and practical obstacles can undermine the timely acquisition of evidence, with potential implications for criminal investigations and prosecutions.

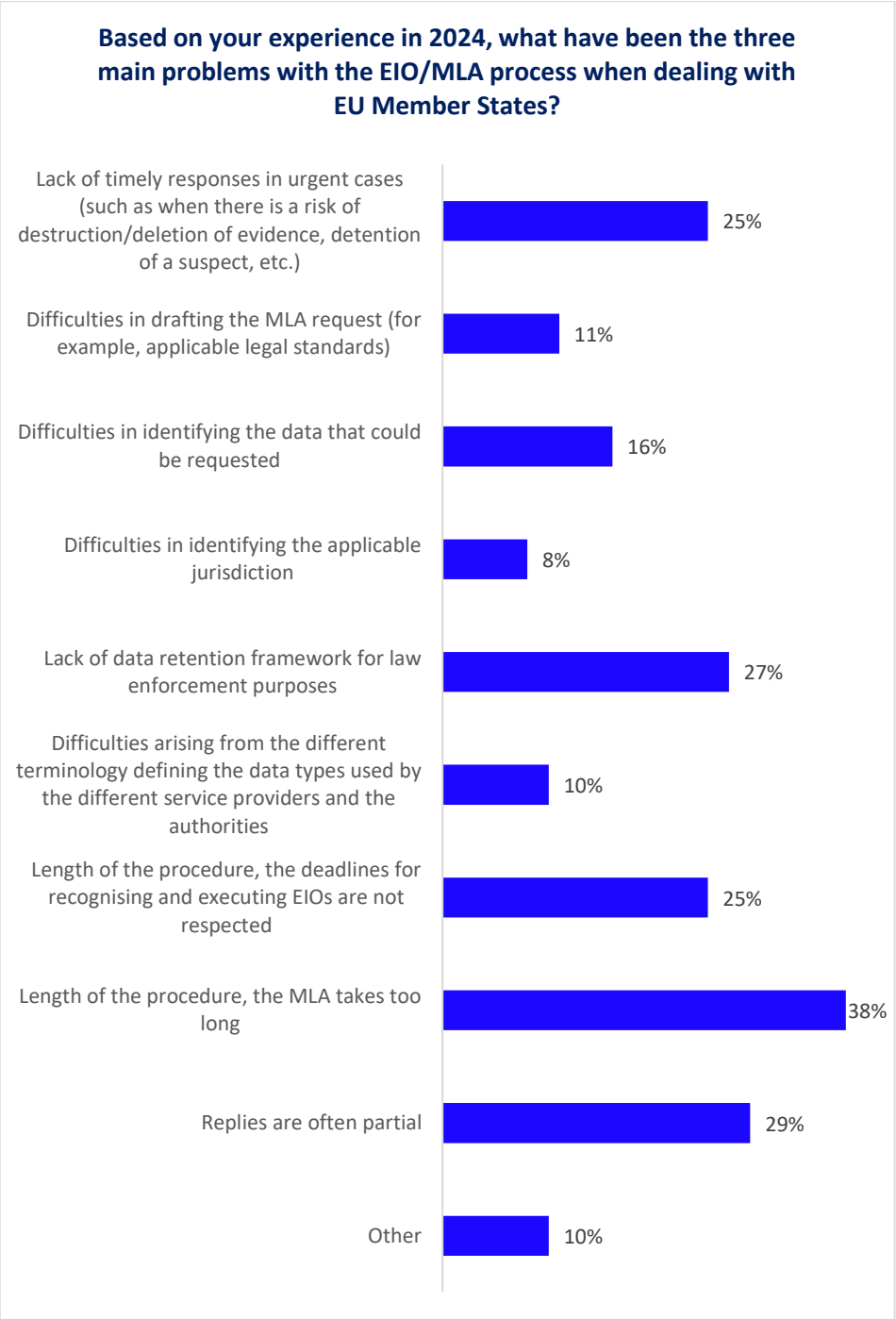
Against this background, and while awaiting the full application of additional legal instruments tailored to electronic evidence, EU judicial authorities were asked to identify the main challenges encountered in 2024 when obtaining electronic data through judicial cooperation channels, both within the EU and in relation to non-EU countries.

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, 38% of respondents identified the long duration of the MLA process as one of the main problems affecting the MLA process towards other EU Member States. Additionally, 29% of respondents pointed out that replies received are often partial, and 27% cited absence of a data retention framework for law enforcement purposes. These were ranked among the three most prevalent problems encountered in their investigations in 2024.

Other issues reported with a lower prevalence concern:

- Deadlines for recognising and executing EIOs are not always respected: 25%
- Lack of timely responses in urgent cases: 25%
- Difficulties in identifying the data that could be requested: 16%
- Difficulties in drafting the MLA request (for example, applicable legal standards): 11%
- Difficulties arising from the different terminology used by the different service providers and the authorities defining the data types: 10%
- Difficulties in identifying the applicable jurisdiction: 8%
- Other: 10%



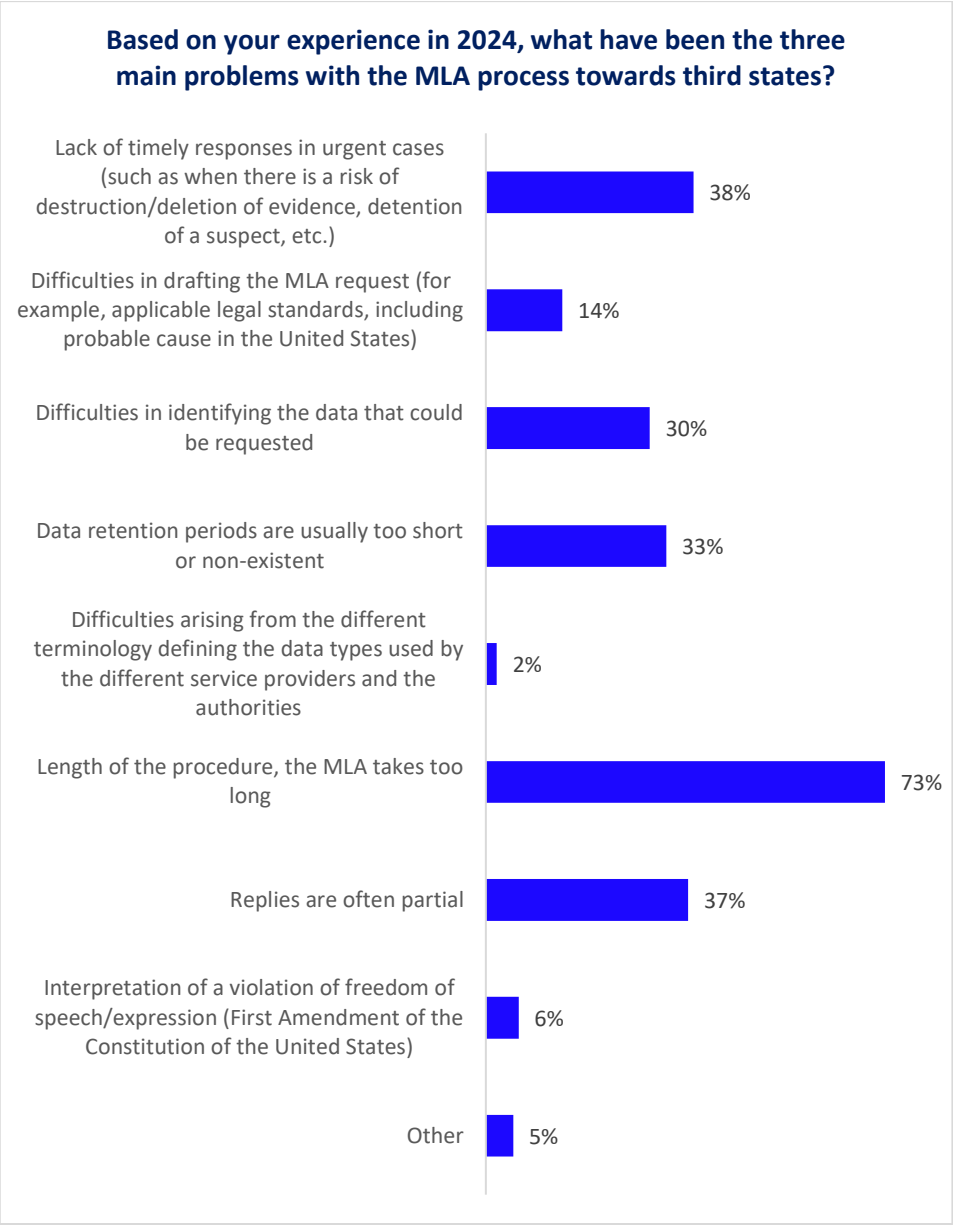
While the relative weight of the identified challenges varies, the results are broadly consistent with the findings of previous reports, which highlighted the length of procedures and data retention constraints as key obstacles. However, the 2024 results reveal a noticeable increase in concerns related to the quality of requests and the responses received. In particular, respondents reported a significant shift towards difficulties linked to receiving only partial data in response to requests, as well as challenges in properly drafting MLA requests, indicating growing practical and technical complexities in judicial cooperation processes.

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 continued to represent the most significant challenge in criminal investigations in 2024. This issue, which has been consistently identified in previous reports, was highlighted by 73% of respondents. In addition, the lack of timely responses in urgent cases (38%) and the frequent receipt of only partial replies (37%) were identified as among the main obstacles encountered by EU judicial authorities. Although short or non-existent data retention periods were ranked slightly lower by respondents (33%), they remain a substantial concern, as they directly affect the availability of electronic evidence. The persistence of these issues, repeatedly highlighted by representatives of the EU judiciary in successive editions of this report, confirms their long-standing nature in the context of judicial cooperation with non-EU countries.

Other challenges reported with a lower prevalence are as follows:

- Difficulties in identifying the data that could be requested: 30%
- Difficulties in drafting the MLA request: 14%
- Interpretation of a violation of freedom of speech/expression (First Amendment of the Constitution of the US): 6%
- Difficulties arising from the different terminology used by the different service providers and the authorities: 2%
- Other: 5%



Looking ahead: navigating solutions and addressing challenges

Looking ahead, the evolving EU and international legal frameworks on access to electronic evidence offer concrete opportunities to address a number of long-standing challenges faced by EU judicial authorities. In particular, the forthcoming EU Electronic Evidence Regulation and the Second Additional Protocol to the Budapest Convention are expected to significantly improve the efficiency, speed and legal certainty of cross-border access to electronic evidence, notably by reducing procedural delays and improving responses in urgent cases.

The introduction of European Production Orders and European Preservation Orders under the EU Electronic Evidence Regulation represents a decisive step towards more streamlined and time-bound procedures, offering a more effective alternative to traditional EIO and MLA mechanisms. Clear deadlines for service providers, combined

with the obligation for providers offering services in the EU to have an establishment or designated representative within the EU, are expected to simplify enforcement, reduce jurisdictional uncertainty and facilitate faster access to electronic evidence.

Beyond the EU framework, the Second Additional Protocol provides an important global cooperation tool, particularly for investigations involving service providers or entities located outside the EU. Its provisions on direct cooperation with service providers, as well as enhanced cooperation between competent authorities in emergency situations, expand the operational toolbox and help bridge gaps not covered by EU legislation. While the Protocol does not establish binding deadlines or strong enforcement mechanisms comparable to the EU framework, it nonetheless constitutes an important step towards more effective international cooperation.

Taken together, these developments mark an important step towards a more efficient and coherent framework for accessing electronic evidence in a cross-border context. While the EU Electronic Evidence legislative package and the Second Additional Protocol substantially strengthen the operational and legal toolbox available to competent authorities, their full impact will depend on effective implementation, awareness and practical use. At the same time, addressing the absence of a harmonised data retention framework remains essential.

In this context, it is particularly relevant that the European Commission is currently assessing the need for updated and harmonised EU rules on data retention. This offers a crucial opportunity to close a longstanding legislative gap and to ensure that future solutions not only provide faster and more reliable access to electronic evidence, but also that the full potential of these new tools can be realised in practice.

Data retention

Access to electronic data enables competent authorities to investigate a wide range of crimes, including those committed online or facilitated by internet and telecommunication networks, as well as offences occurring in the physical world. Non-content data – such as subscriber information, IP addresses, device location and the time and duration of communications – can be crucial for investigations, helping to identify or locate suspects, accused persons or victims, and providing insights into the commission of an offence.

Access to such data depends on its availability and retention by service providers, who store data for periods necessary to deliver services and for legitimate business purposes, such as invoicing, fraud prevention and ensuring user safety and security. In addition, service providers may retain data to comply with legal obligations, including tax, audit or other regulatory requirements.

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[10] by the Court of Justice of the European Union (CJEU) in 2014, no EU-wide legal framework exists in this area and data retention is governed by national laws within the framework of Article 15(1) of the E-Privacy Directive[11], 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 its jurisprudence, establishing conditions for lawful data retention and access under EU law[12].

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

On 30 April 2024, the CJEU issued its judgement in Case C-470/21 – *La Quadrature du Net and Others v Premier ministre and Ministère de la Culture*. 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 Court's main findings can be summarised 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).
- **Access to civil identity data**: the Court found that EU law does not preclude national legislation authorizing competent public authorities to access civil identity data associated with retained IP addresses. This access must serve the sole purpose of identifying the holders of the relevant IP addresses suspected of being responsible for the alleged infringement. 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 IP addresses for purposes other than the adoption of measures against the suspected infringement.
- **Conditions for access**: the Court emphasized 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.

On 30 April 2024, the CJEU issued its judgment 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 manifestly 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.

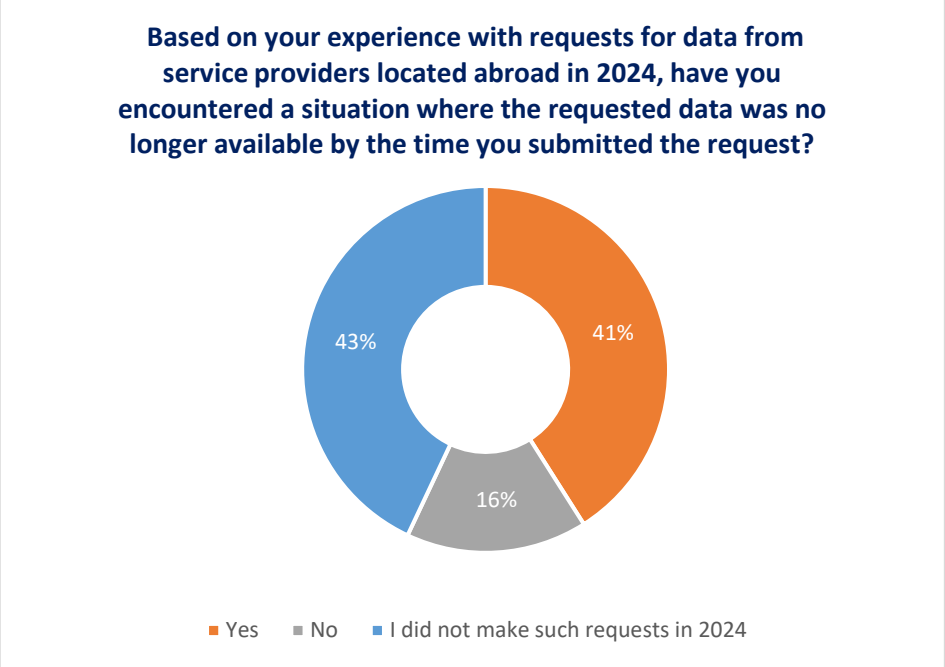
Regarding access to retained data, on 4 October 2024, the CJEU issued its judgment in Case C-548/21 – *CG v Bezirkshauptmannschaft Landeck*. The Court issued important rulings concerning the seizure of a mobile telephone in the context of a narcotics investigation and the subsequent attempts by the Austrian authorities to unlock the device in order to access the data stored on it. The Court's main findings can be summarised as follows.

- **Conditions for access:** national rules may allow access to mobile phone data for prevention, investigation, detection, and prosecution of criminal offences, if they:
  - clearly define the nature or categories of offences concerned;
  - respect the principle of proportionality; and
  - require prior review by a judge or independent administrative body, except in urgent cases.

- **Proportionality and necessity:** any limitation on privacy and data protection rights must be necessary and proportionate to the investigation's objectives. In addition, access, especially to sensitive data, must be strictly limited to what is necessary for the investigation.
- **Notification of the data subject:** authorities cannot attempt access without informing the data subject of the grounds for the authorization issued by a court or independent body, once such notification does not jeopardise the investigation. This ensures the data subject can challenge the decision in court if needed.

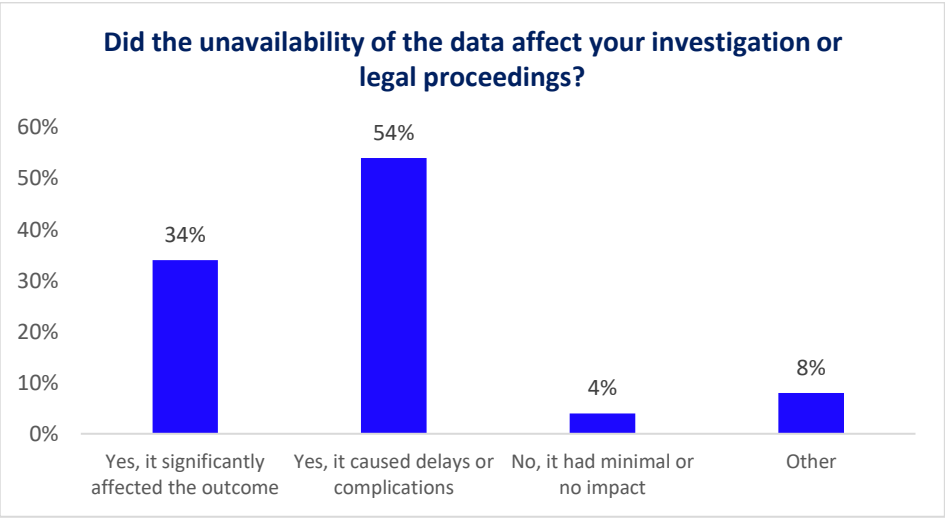
Despite the CJEU's clear guidelines on data retention for law enforcement purposes and regarding access to such data, the lack or limited scope of such frameworks in the EU Member States remains a significant challenge for EU judicial authorities when seeking data from other jurisdictions.

The survey indicates that a significant proportion of EU judicial authorities have encountered situations in which requested data from service providers located abroad was no longer available at the time the request was submitted, with 41% of respondents reporting this issue.



Among these authorities that experienced situations where requested data were no longer available:

- 34% stated that the unavailability of data had a significant impact on their investigations or legal proceedings;
- 54% reported that it caused delays or complications;
- only 4% indicated that the lack of data had minimal or no impact; and
- 8% were unable to predict the operational impact.



These findings underscore the urgent need for a harmonised EU-level data retention framework. Inconsistent or limited retention periods for electronic data can render crucial information unavailable, directly impacting the efficiency, timeliness and effectiveness of criminal investigations and prosecutions. In 2024, work on data retention focused primarily on policy development, laying the groundwork for potential new legislation. The EU High-Level Group on Access to Data for Effective Law Enforcement endorsed 42 recommendations highlighting persistent challenges arising from fragmented and non-harmonised retention rules. Its Concluding Report, adopted in November 2024, further analysed obstacles to accessing digital evidence and stressed the importance of harmonised retention frameworks. Building on these efforts, in 2025 the European Commission initiated an EU-level impact assessment on data retention, with a view to updating and harmonising retention rules. The results of this assessment are expected in 2026, marking a critical step toward ensuring that law enforcement authorities have timely access to the data needed for effective investigations, while maintaining appropriate safeguards for privacy and fundamental rights.

Cost reimbursement

In addition to the challenges faced by competent authorities in accessing electronic data, the growing reliance on such data in criminal investigations and proceedings also entails financial implications. Responding to requests for electronic evidence may generate costs for service providers and, indirectly, for national authorities seeking access to such data. These costs may stem from the allocation of personnel, technical processing, legal review and the development or maintenance of internal systems to handle requests from law enforcement and judicial authorities.

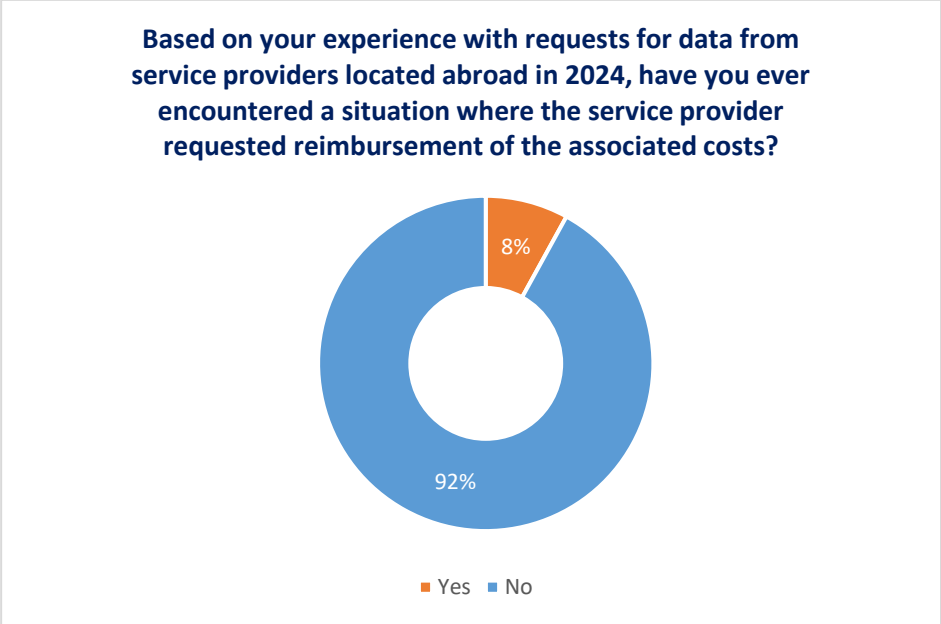
Determining responsibility for bearing these costs is shaped by the fragmented legal framework governing access to electronic evidence. This framework includes national legislation of EU Member States, relevant EU instruments, international agreements applicable to cross-border cooperation and service providers' internal policies. As a result, national competent authorities may encounter varying and sometimes unclear rules on cost reimbursement when carrying out their investigative activities.

National approaches to cost reimbursement vary considerably across jurisdictions. In some Member States, such as Belgium, the Czech Republic and Germany, national legislation provides for the reimbursement of costs incurred by service providers when responding to requests from national competent authorities. In other jurisdictions, no explicit provisions on cost reimbursement exist (e.g. Greece, Ireland and Slovenia), while in certain Member States service providers may be required to comply with requests at their own expense (e.g. Estonia, Hungary and Poland). This diversity of national rules may influence strategic considerations for requesting authorities, as the allocation of costs can become a relevant factor when choosing the legal framework under which to seek electronic evidence. In this context, the EU Electronic Evidence Regulation, requires EU Member States to inform the Commission of their national rules on cost reimbursement, and the Commission is to make this information publicly available.

At the EU and international level, the treatment of cost reimbursement also differs across instruments. The EU Electronic Evidence Regulation includes provisions on cost reimbursement, allowing service providers to seek compensation for expenses incurred in complying with European Production Orders and European Preservation Orders, provided that such reimbursement is permitted under the national law of the issuing

authority in each specific case. In contrast, the Second Additional Protocol to the Budapest Convention does not contain any provisions on cost reimbursement, leaving the issue to be addressed, if at all, under applicable domestic law or through bilateral arrangements.

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 8% of the respondents encountered a situation where a service provider requested reimbursement for costs associated with responding to requests for data. The remaining 92% indicated that they had never received such a claim, suggesting that cost reimbursement has, to date, had a limited practical impact on the data retrieval process.



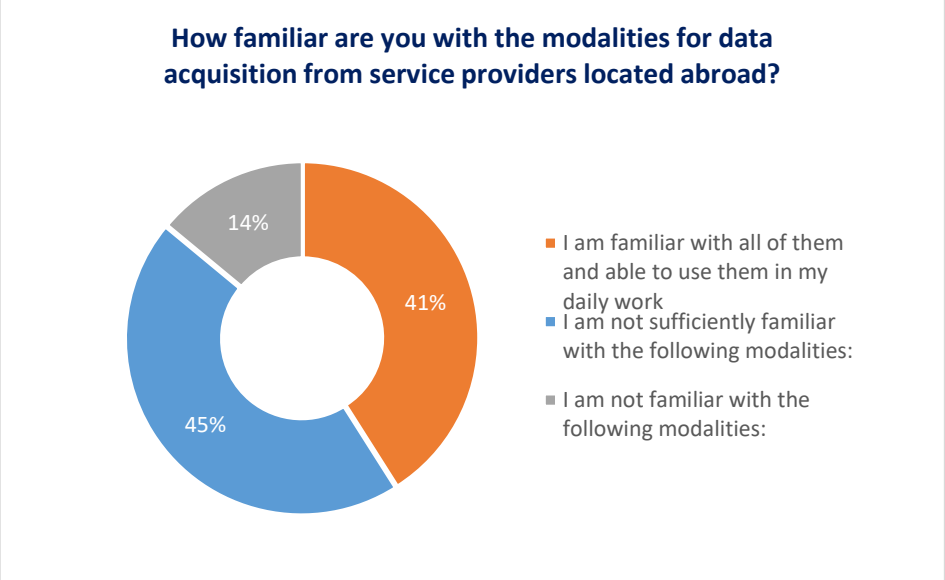
However, this situation may evolve with the application of the Electronic Evidence Regulation. The Regulation introduces strict deadlines for compliance – 10 days for standard requests and 8 hours in emergency cases – which may require service providers to mobilise additional resources, including dedicated personnel, enhanced technical capabilities and streamlined internal procedures. These requirements are likely to increase operational costs, potentially prompting service providers to make greater use of the reimbursement mechanisms foreseen by the Regulation. Given the diversity of national legal frameworks governing cost reimbursement, service providers may face legal and financial uncertainty when assessing their eligibility for compensation, while competent authorities may need to account more explicitly for cost considerations when issuing requests under the new regime.

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 and direct

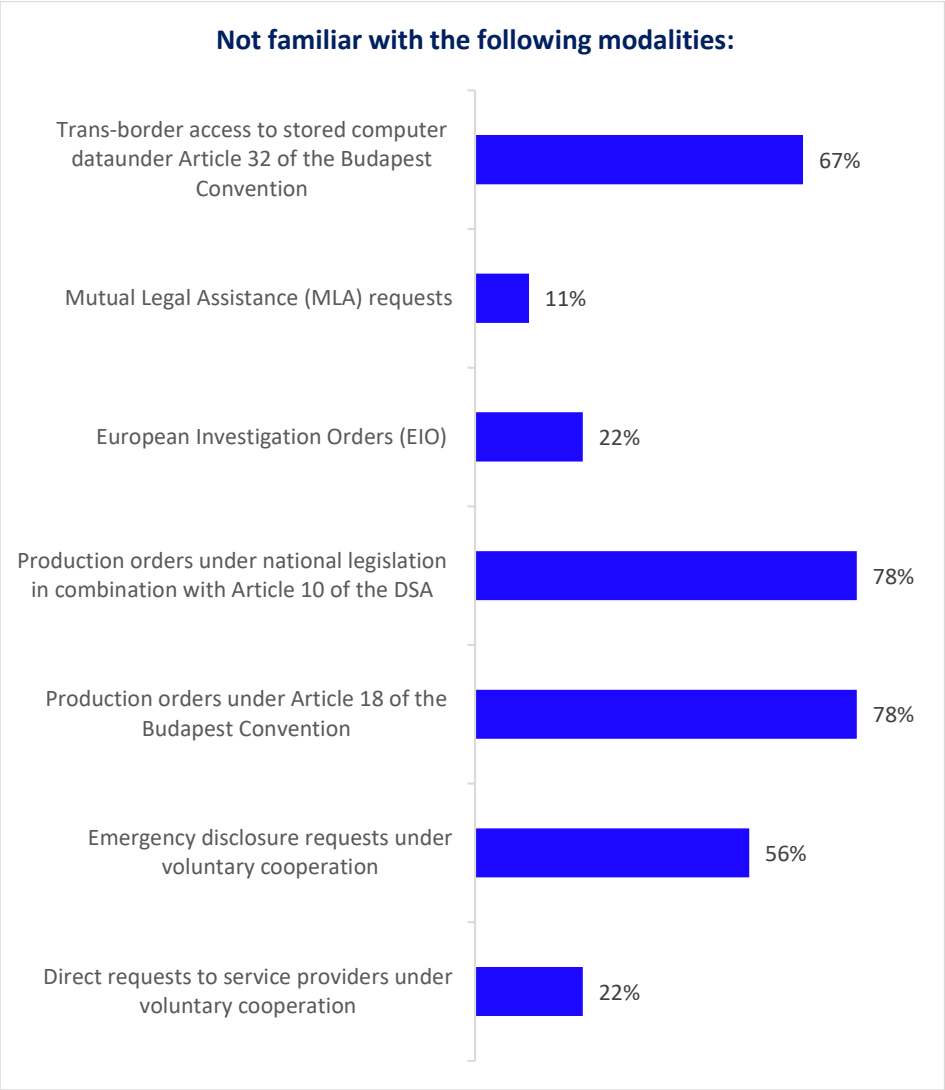
requests to service providers under voluntary cooperation, as well as preparing for future legislative developments in this field.

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, 45% of the respondents reported that they are not sufficiently familiar with the currently available modalities for cross-border data acquisition and 14 % indicated that they are not familiar with some of them.

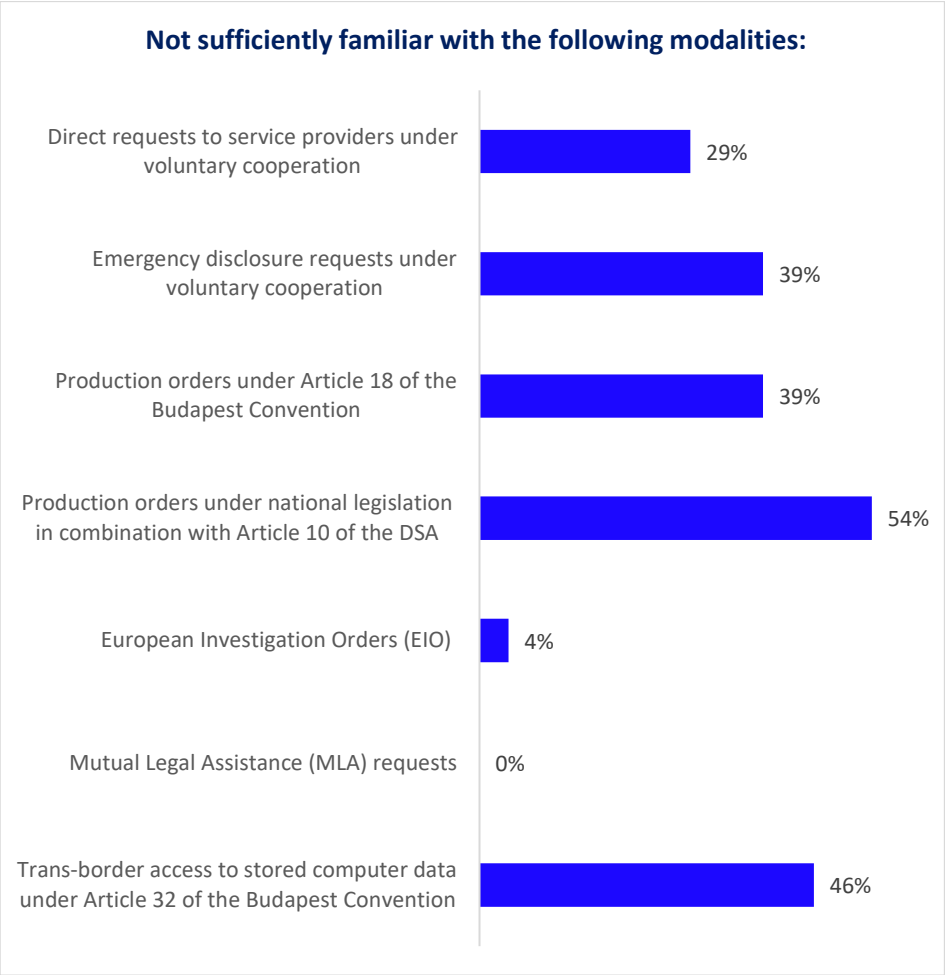


A closer examination shows that several mechanisms require enhanced knowledge and capacity building among EU judicial authorities. These include production orders under national legislation in combination with the newly available Article 10 of the DSA; trans-border access to stored computer data with consent or where such data are publicly available under Article 32 of the Budapest Convention on Cybercrime; production orders under Article 18 of the Budapest Convention; and emergency disclosure requests based on voluntary cooperation. This ties in with the results from the question on the modalities predominantly used by authorities in their investigations in 2024, indicating that these four 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.

Specifically, 78% of respondents who reported a lack of familiarity with certain modalities for data acquisition indicated that they were not at all familiar with production orders under Article 18 of the Budapest Convention, as well as with production orders under national legislation in combination with Article 10 of the Digital Services Act (DSA). Furthermore, 67% indicated a lack of familiarity with trans-border access to stored computer data under Article 32 of the Budapest Convention, while 56% pointed to emergency disclosure requests based on the voluntary cooperation mechanism.



Similarly, 54% of respondents who reported insufficient familiarity with certain modalities for data acquisition indicated a need for increased knowledge regarding production orders under national legislation in combination with Article 10 of the DSA, while 46% pointed to trans-border access to stored computer data under Article 32 of the Budapest Convention. Furthermore, 39% indicated insufficient familiarity with production orders under Article 18 of the Budapest Convention and with emergency disclosure requests based on voluntary cooperation mechanisms.

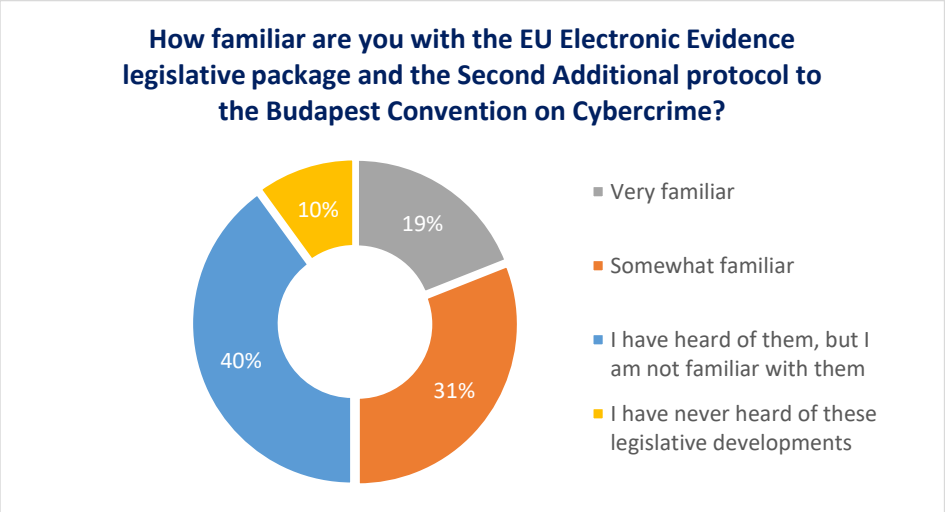


Insufficient familiarity with these methods may lead authorities to underutilise them effectively. Conversely, the lack of utilisation due to unfamiliarity can perpetuate a cycle of inadequate knowledge among judicial authorities, where potentially valuable tools are overlooked. Enhancing familiarity with and capacity to use these modalities is therefore essential to expand the toolkit available for accessing electronic evidence across borders.

Looking ahead, as legislative changes reshape the landscape of cross-border access to electronic evidence, it is essential to prepare judicial authorities for new instruments designed to enhance efficiency in this area. The forthcoming legal instruments will provide important additional tools for accessing electronic evidence across borders more effectively. However, their successful application will depend on judicial authorities being equipped with the necessary knowledge and skills to navigate these new frameworks.

To assess the level of awareness among EU judicial authorities regarding the evolving legal landscape, respondents were asked about their familiarity with recent legislative developments. The survey results indicate that the substantial part of respondents (40%, compared to 37% in 2023) have heard of the EU Electronic Evidence legislative package and the Second Additional Protocol but are not familiar with their content. A further 31% of respondents (up from 28% in 2023) reported having some knowledge of these instruments. More concerningly, only 19% of respondents (down from 26% in 2023)

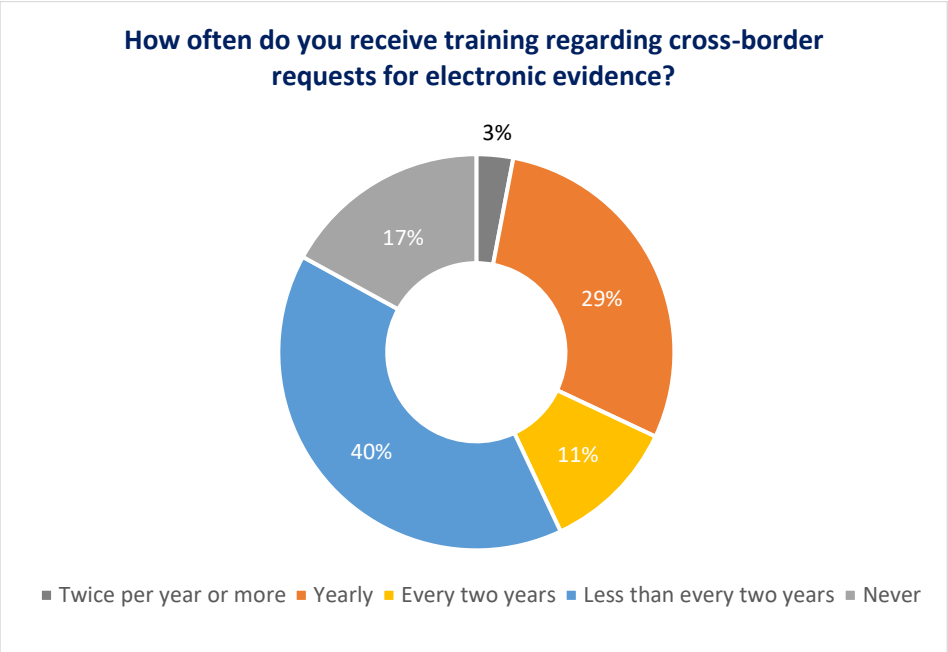
indicated that they are very familiar with these legislative developments, while 10% (up from 4% in 2023) reported having never heard of them.



These findings underscore the urgent need to strengthen knowledge and capacity among EU judicial authorities, particularly with the EU Electronic Evidence legislative package which will become applicable in August 2026. As legal frameworks evolve to address the challenges of obtaining electronic evidence, effective cross-border cooperation will require a thorough understanding of existing tools and preparedness to make use of new legal instruments. Ensuring that judicial authorities are well-informed and adequately prepared is therefore crucial to facilitating efficient and effective access to electronic evidence across borders.

An examination of the recent situation regarding training received by EU judicial authorities on cross-border requests for electronic evidence up to 2024 indicates that significant further efforts are needed in this area. To assess training needs related to cross-border access to electronic evidence, respondents were asked how frequently they receive any form of training on this topic.

The survey results show that 40% of respondents receive training on this subject less frequently than every two years, while 29% reported receiving such training on a yearly basis. A further 11% indicated that they benefit from regular or continuous updates of their knowledge at least every two years, while only 3% of respondents stated that they receive training at least twice per year. Notably, 17% of respondents reported that they have never received any training on obtaining cross-border electronic evidence by 2024.



Electronic evidence for judicial authorities in non-EU countries

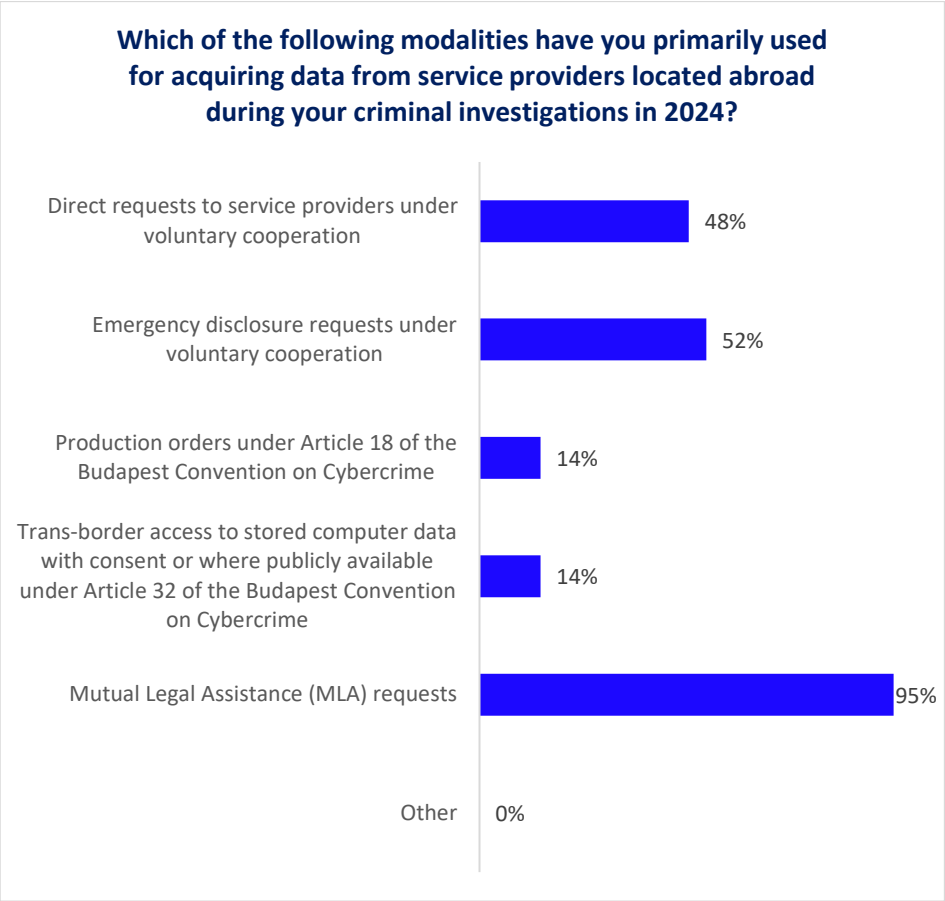
Judicial authorities from non-EU countries cooperating with Eurojust through international agreements, the EuroMed Justice Project, the Western Balkans Criminal Justice Project and the European Judicial Network were invited to complete the same survey as the EU judiciary.

A total of 22 responses were received from Bosnia and Herzegovina, Canada, Iceland, Kosovo, Lebanon, Mexico, Moldova, Montenegro, Palestine, Serbia, Switzerland, the United Kingdom and the United States of America.

Main modalities for acquiring data from service providers located abroad

Regarding the modalities used by judicial authorities in non-EU countries to obtain electronic evidence from service providers located in different jurisdictions in 2024, the responses collected largely mirrored those reported by EU judicial practitioners.

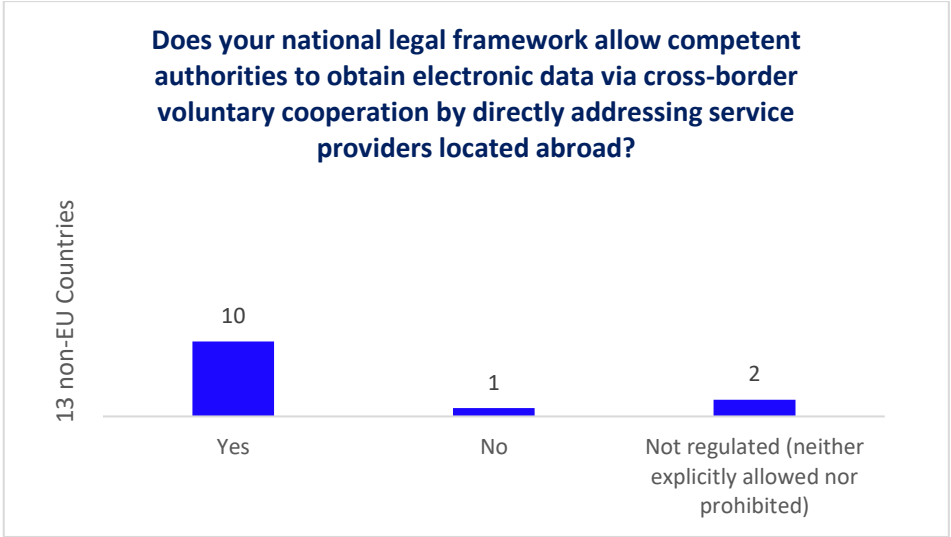
In particular, MLA requests remained the predominant modality for cross-border evidence gathering in criminal investigations in 2024. According to the survey, 95% of responding authorities primarily relied on MLA when seeking data from service providers located abroad. To a lesser extent, emergency voluntary disclosure requests, selected by 52% of surveyed authorities, represented the second most frequently used tool, while direct requests to service providers based on voluntary cooperation constituted the third most common approach, reported by 48% of respondents.



Direct voluntary cooperation with service providers

Regarding national legislation in the surveyed non-EU countries on voluntary cooperation channels, the survey results indicate that, similarly to EU Member States, national legal frameworks in non-EU countries generally allow competent authorities to obtain electronic data through cross-border voluntary cooperation by directly addressing service providers located abroad.

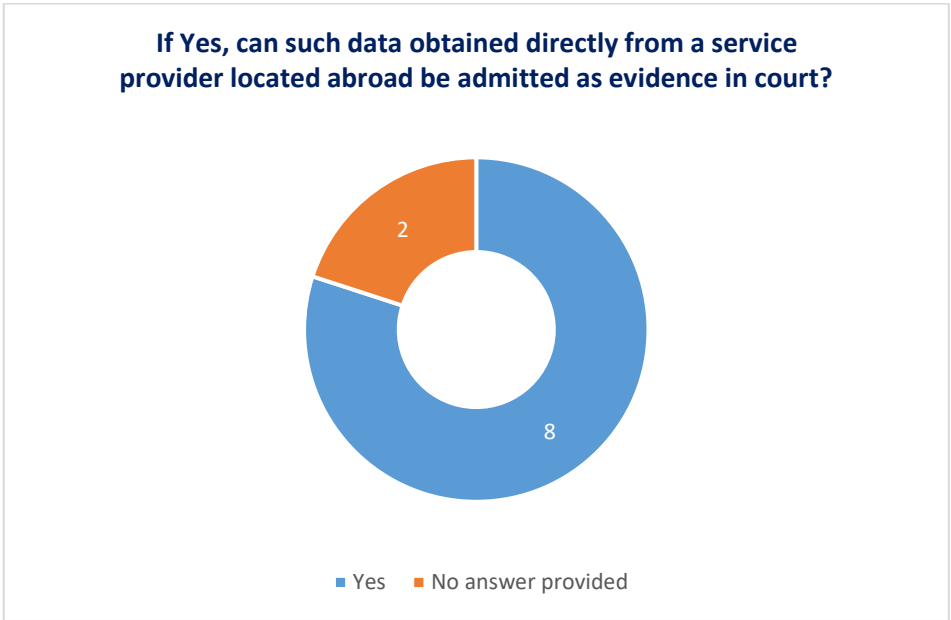
The majority of the surveyed non-EU countries (10 out of 13) permit the collection of electronic data through voluntary cooperation by directly contacting service providers located abroad. One non-EU country was identified as not allowing the use of direct voluntary cooperation for obtaining electronic evidence, while respondents from two non-EU countries reported that their national legal frameworks neither explicitly allow nor explicitly prohibit the collection of electronic evidence through voluntary cooperation channels.



When considering the admissibility of electronic data collected directly from a service provider located abroad through a direct request for voluntary cooperation, the survey responses indicate that in the vast majority of non-EU countries where legal frameworks permit competent authorities to obtain data in this way (8 out of 10), such data can be admitted as evidence in court.

This pattern is largely consistent with the situation in EU Member States, where competent authorities that are legally permitted to obtain data via cross-border voluntary cooperation also report that evidence collected through direct requests to service providers is generally admissible.

These findings underscore the importance of voluntary cooperation as a practical tool for cross-border evidence gathering, complementing more formal channels such as MLA requests. While MLA remains the dominant method for obtaining electronic evidence across borders for non-EU countries, direct voluntary cooperation provides a faster mechanism, provided that the national legal framework permits both the collection and admissibility of such evidence in judicial proceedings.



Some of the respondents shared additional explanations and/or direct references to their national legislation:

Bosnia and Herzegovina	*Formal international cooperation mechanisms, such as MLA and frameworks under the Budapest Convention, remain the official and lawful channels.*
Canada	*The primary complicating factor is acquiring the necessary sworn affidavit as to the authenticity of such records.*
Moldova	*[In Moldova] the court orders are meant to be sent through MLA requests to the country where the service providers are located. In our country competent authorities do not ask information directly from service providers.*
Serbia	*In cases where there is a justified need to obtain data from electronic communications or internet services for the purposes of conducting criminal proceedings, and the data are held by a foreign service provider, the public prosecutor may address the request for such data directly to the service provider abroad, in accordance with the conditions prescribed by international agreements, accepted practice or the service provider's internal rules and procedures.*

Challenges related to direct voluntary cooperation with service providers located in foreign jurisdictions

Judicial authorities from non-EU countries were asked to identify the three most challenging aspects encountered when directly contacting service providers located abroad with requests for electronic data under voluntary cooperation.

The responses indicate that in 2024, the most significant challenge for the majority of respondents from non-EU countries (similarly to EU judicial authorities) was difficulty in identifying how and where to submit such requests, as reported by 62% of respondents.

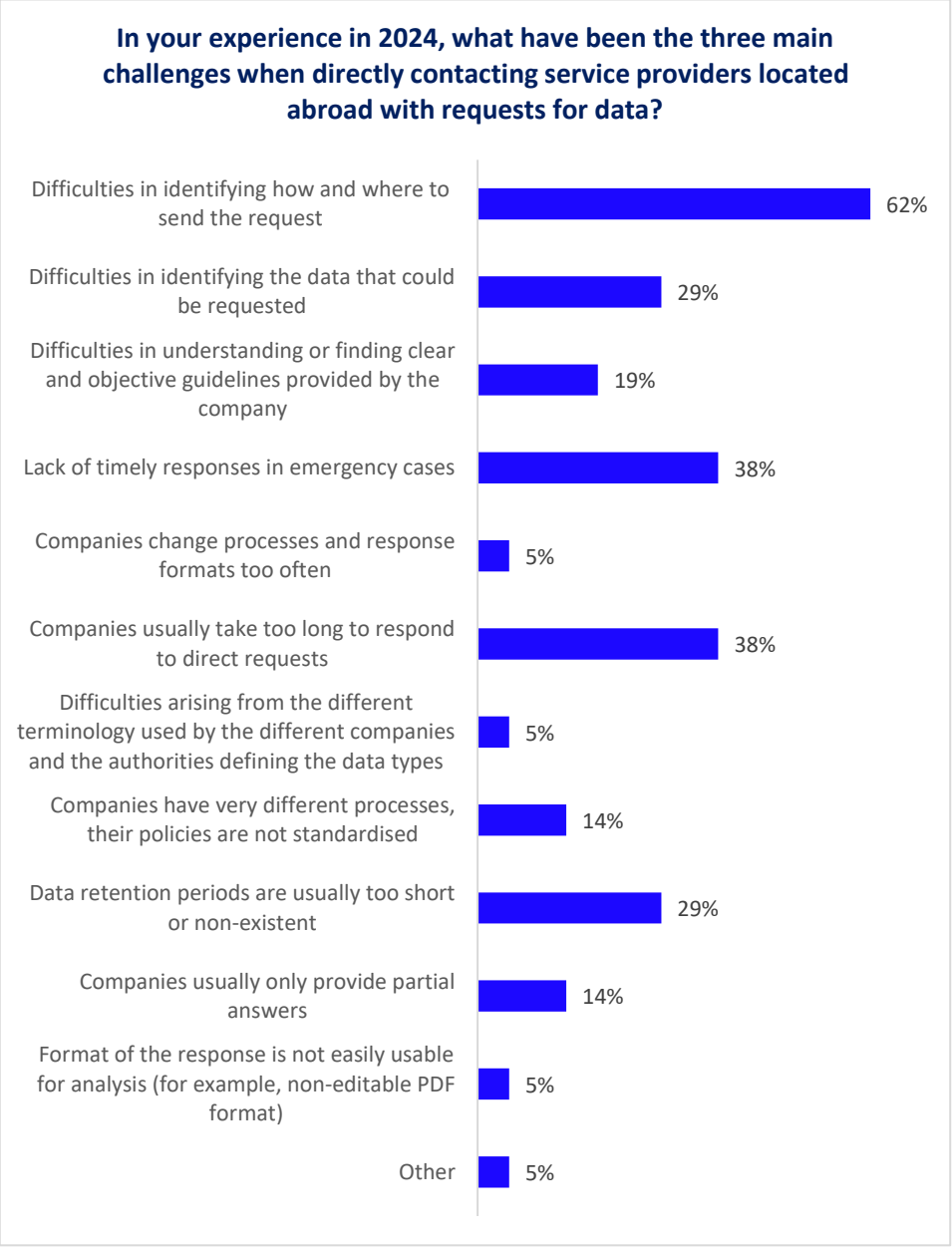
Notably, even though this channel is often considered the fastest means for competent authorities to obtain non-content data, issues related to delays in receiving responses in emergency cases, as well as the time taken by companies to respond to direct requests, were identified as the second most prominent challenges in investigations conducted in 2024, as reported by 38% of respondents.

The third most prevalent challenge identified by non-EU judicial authorities concerned data retention – related issues and difficulties in identifying which data could be requested, as indicated by 29% of respondents.

Additional problems reported with a lower prevalence were as follows:

- difficulties in understanding or finding clear and objective guidelines provided by companies: 19%
- companies usually only provide partial answers: 14%
- companies have very different processes, their policies are not standardised: 14%
- companies change processes and response formats too often: 5%
- difficulties arising from the different terminology used by the different companies and the authorities defining the data types: 5%

- the response format is not easily usable for analysis (for example, non-editable PDF format): 5%
- other: 5% (provided by the respondents: voluntary cooperation is not allowed under the legal framework).



Extraterritorial powers under Budapest Convention on Cybercrime

Non-EU judicial authorities were surveyed on whether their national legal frameworks in 2024 provided a legal basis for issuing production orders or requests for electronic data to service providers located abroad, in line with the modalities set out in the Budapest Convention on Cybercrime and its Second Additional Protocol. Notably, four of the countries represented in the survey are not parties to the Budapest Convention.

The results show that, eight surveyed non-EU countries already provide a legal basis for issuing production orders following the model of Article 18 of the Budapest Convention.

Four surveyed non-EU countries reported having introduced legal bases reflecting the modalities of the Second Additional Protocol, including production orders under Article 7 and requests for domain name registration information under Article 6, despite the Protocol not yet being in force. At the same time, four surveyed non-EU countries indicated that their national legal frameworks do not provide any legal basis for issuing orders or requests to service providers located abroad under the Budapest Convention framework, pointing to a continued reliance on more traditional cooperation channels.

Judicial cooperation

Similarly to EU judicial authorities, and as reflected in the survey findings presented above, MLA remains the primary and preferred channel for non-EU judicial authorities to obtain electronic data across borders.

Against this background, non-EU judicial authorities were asked to identify the main challenges encountered in 2024 when obtaining electronic data through MLA procedures, both in cooperation with EU Member States and with other non-EU countries.

Challenges related to the MLA process towards EU Member States

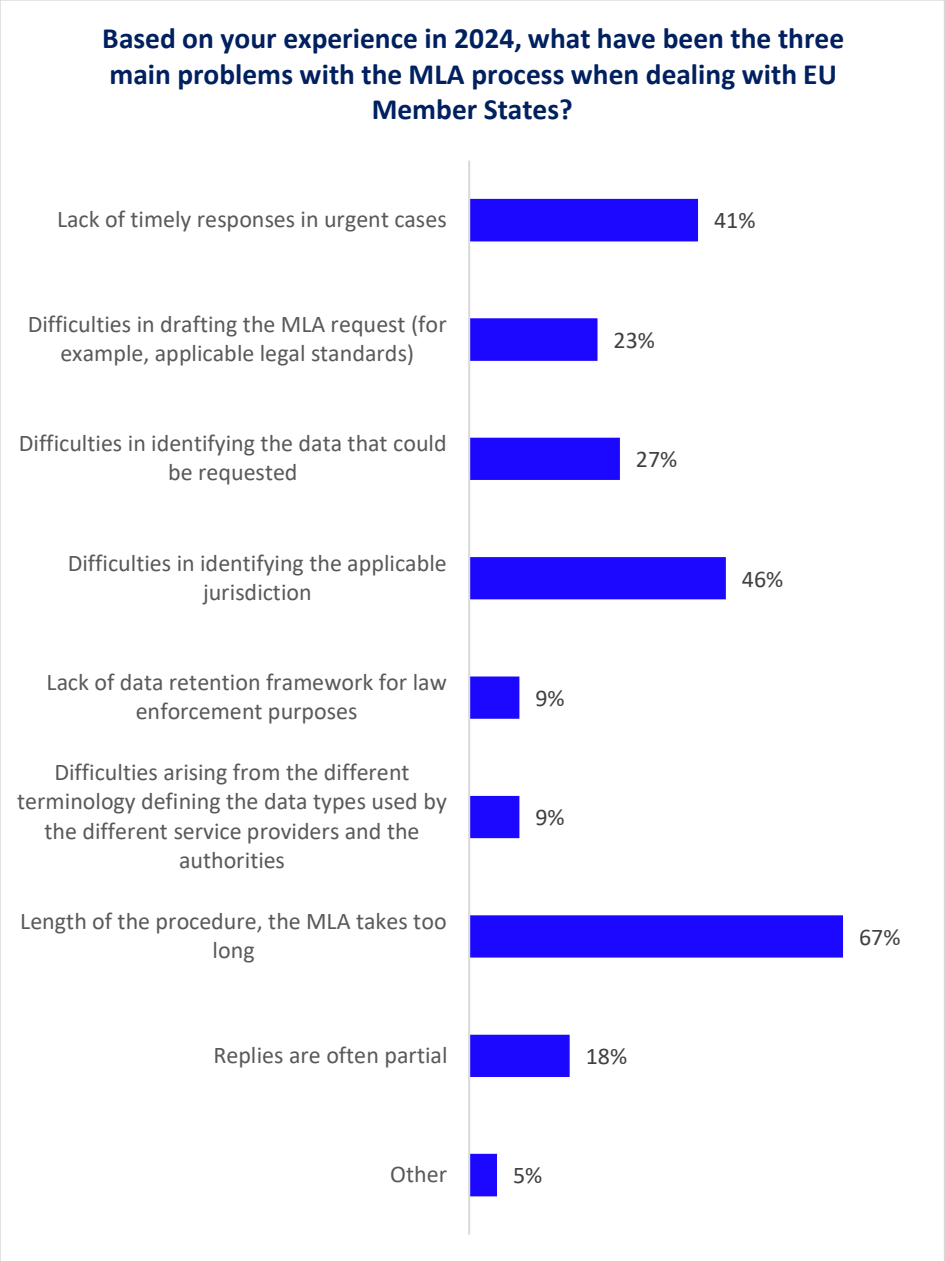
With regard to the MLA process *vis-à-vis* EU Member States, the most pressing challenge identified by respondents in 2024 was the length of the procedure. In particular, a clear majority of respondents (67%) indicated that MLA requests take too long to be executed. In addition, 46% of respondents reported difficulties in identifying the applicable jurisdiction, while 41% identified the lack of timely responses in urgent cases (such as situations involving a risk of evidence destruction or deletion, or the detention of a suspect) as another significant challenge encountered in their investigations.

Other challenges were reported with lower frequency and include:

- difficulties in identifying the data that could be requested: 27%;
- difficulties in drafting the MLA request (for example, applicable legal standards): 23%;
- instances where replies received were only partial: 18%;

- difficulties arising from the different terminology used by the different service providers and the authorities defining the data types: 9%;
- lack of data retention framework for law enforcement purposes: 9%;
- other: 5%.

In addition, a respondent from Mexico highlighted issues related to collaboration agreements and service-related costs when obtaining electronic evidence through MLA procedures with EU Member States.



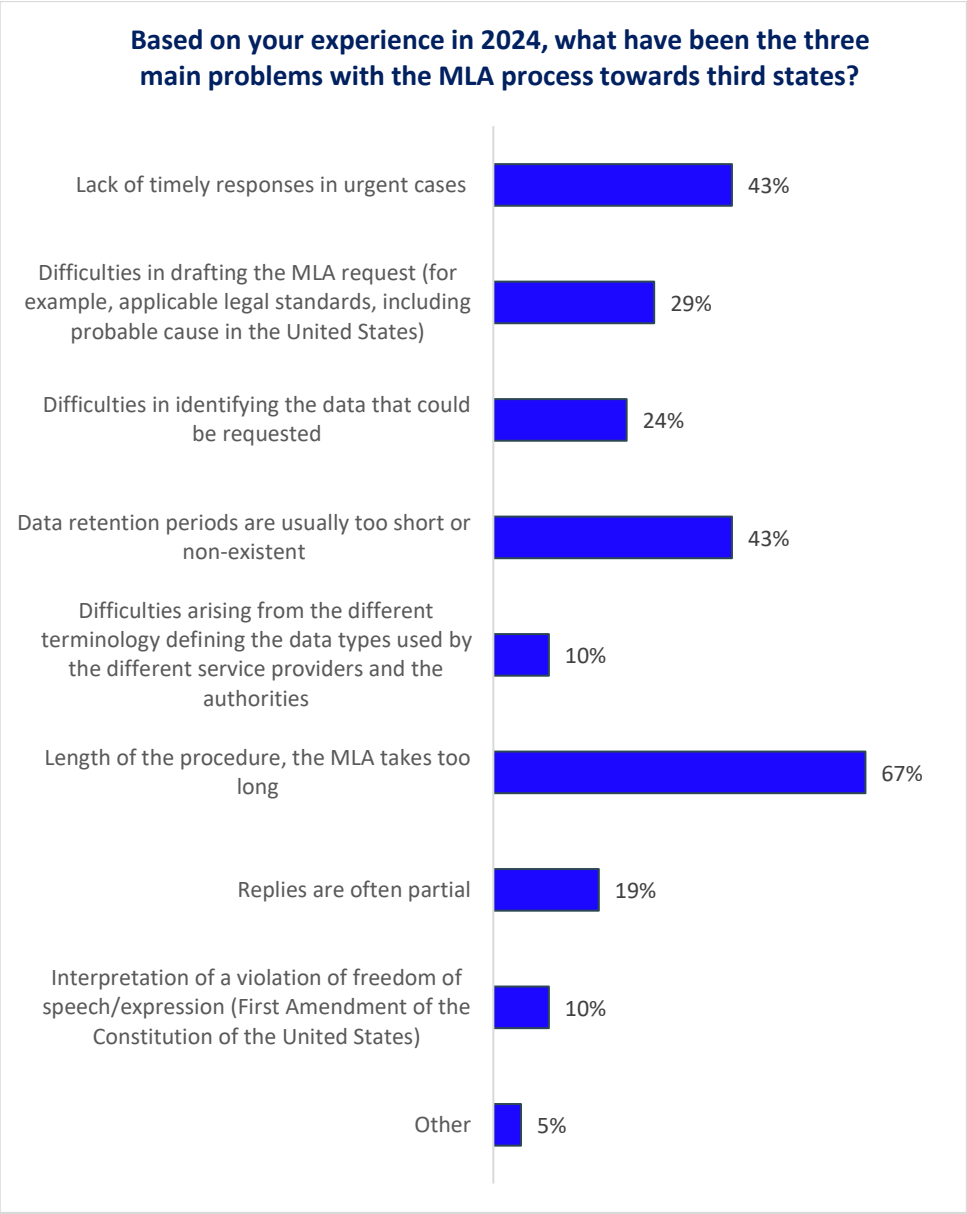
Challenges related to the MLA process towards other non-EU countries

With regard to judicial cooperation for obtaining electronic evidence from other non-EU countries, the length of the MLA procedure continued to represent the most significant challenge in criminal investigations in 2024. This issue was highlighted by 67% of respondents, mirroring the findings reported for cooperation with EU Member States.

In addition, the lack of timely responses in urgent cases (43%) and short or non-existent data retention periods (43%) were identified as among the main obstacles encountered by non-EU judicial authorities. Notably, data retention–related challenges were ranked considerably lower in the context of cooperation with EU Member States, where they were selected by only 9% of respondents. By contrast, such issues emerge as one of the most problematic aspects when cooperation concerns other non-EU countries, suggesting significant divergences in data retention frameworks across jurisdictions.

Other challenges reported with a lower prevalence include:

- difficulties in drafting the MLA request: 29%;
- difficulties in identifying the data that could be requested: 24%;
- instances where replies received were partial: 19%;
- interpretation of a violation of freedom of speech/expression (First Amendment of the Constitution of the US): 10%;
- difficulties arising from the different terminology used by the different service providers and the authorities: 10%;
- other: 5%.



Data retention

The growth in the volume of available personal data has been accelerated by the widespread use of social media and the proliferation of connected devices, leading to increased concerns regarding privacy and data protection. Consequently, data retention rules have been the subject of ongoing discussions, primarily focusing on the balance between obligations imposed on SPs to retain data and the interference with the right to privacy. These developments have undoubtedly influenced data retention regulations across jurisdictions, resulting in a fragmented legal landscape.

In light of the recurrent identification of data retention as a key challenge in the survey, judicial authorities from non-EU countries were asked whether a national data retention regime is in place in their respective jurisdictions.

The analysis of the responses indicates that, in the majority of the surveyed non-EU countries (10 out of 12), a domestic data retention regime is currently in place, namely in Bosnia and Herzegovina, Iceland, Kosovo, Mexico, Moldova, Montenegro, Palestine,

Serbia, Switzerland and the United Kingdom. By contrast, Canada and Lebanon reported that no such national framework exists.

Several respondents also provided additional explanations and/or direct references to their national legislation:

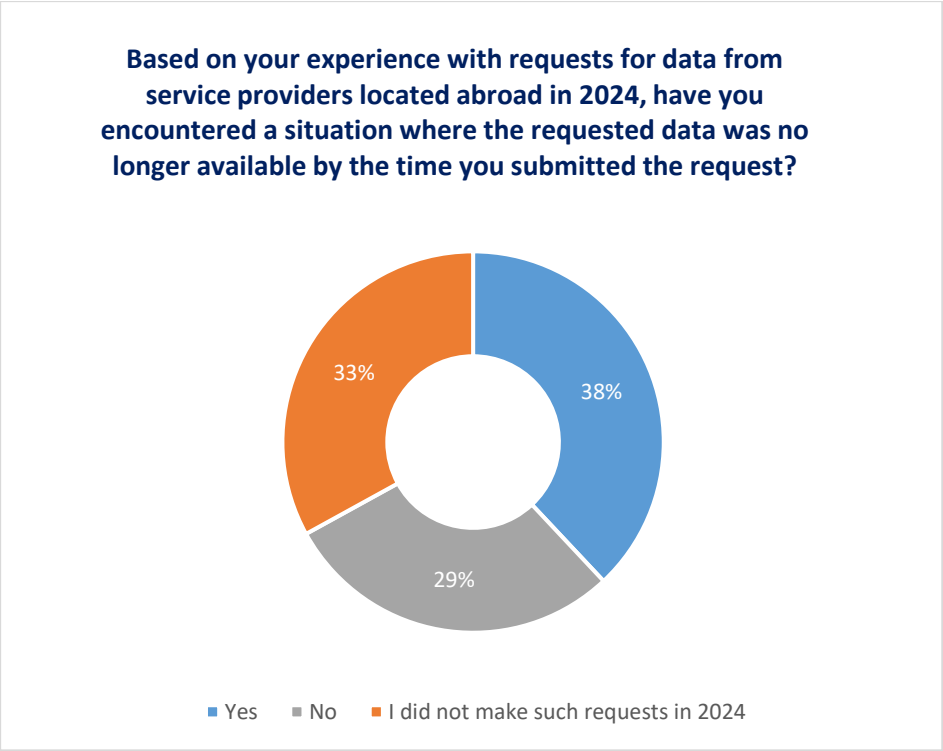
Bosnia and Herzegovina	*Service providers in Bosnia and Herzegovina are required by law to retain certain categories of data for a specific period of time, primarily for purposes such as law enforcement, national security – or regulatory compliance – independently of individual official requests.* *All available data is preserved for six months or within the technical possibilities.*
Canada	*There are no national laws implementing minimum data retention period standards in Canada. In practice, many of the major communication service providers tend to hold data between 90 days to several years, depending on the type of information.*
Kosovo	*The Service providers are obliged to retain data for a period of time for one year.* *LAW No. 04/L-109 ON ELECTRONIC COMMUNICATIONS Article 68.*
Moldova	*The term for retention of data by service providers is 180 days.*
Palestine	*[Retention period is] three years according to the Company Law.*
Serbia	*Operators are obliged to retain data on electronic communications, including data necessary to identify the source, destination, date, time, duration, type of communication, communication device, and the location of the communication device, for a period of twelve months from the date of communication. (Article 128 of the Law on Electronic Communications of the Republic of Serbia).*
Switzerland	*[The retention period is] six months since the last communication.*

Similarly to EU judicial authorities, the counterparts from non-EU countries also highlighted data retention for law enforcement purposes, and regarding access to such data, the lack or limited scope of data retention frameworks is a significant challenge for competent authorities when seeking data from other jurisdictions.

The survey indicates that 38% of the surveyed non-EU judicial authorities have encountered situations in which requested data from service providers located abroad was no longer available at the time the request was submitted.

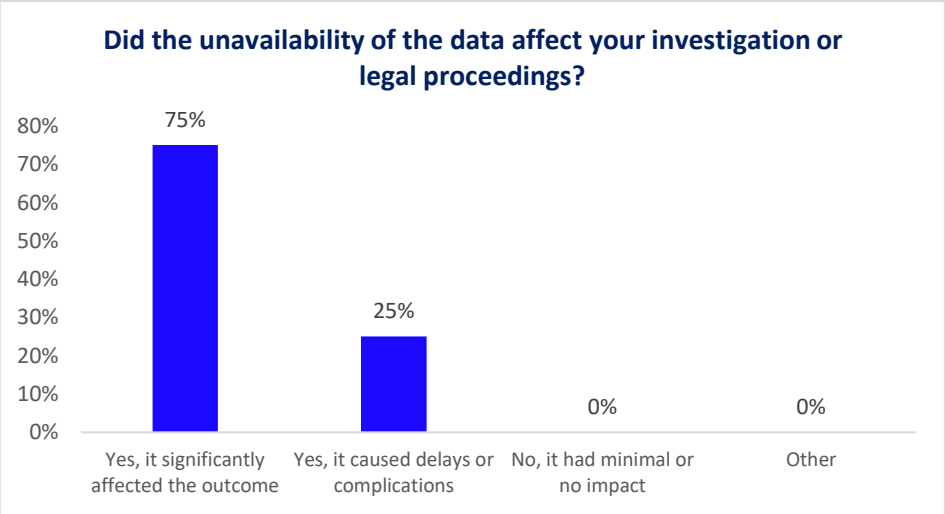
Similarly to EU judicial authorities, their counterparts from non-EU countries also identified data retention for law enforcement purposes, and access to such data, as a significant challenge. In particular, the absence or limited scope of data retention frameworks in certain jurisdictions was highlighted as a key obstacle when seeking electronic data from abroad.

The survey results indicate that 38% of the surveyed non-EU judicial authorities have encountered situations in which the requested data from service providers located abroad was no longer available at the time the request was submitted.



Among these authorities that experienced situations where requested data were no longer available:

- 75% stated that the unavailability of data had a significant impact on their investigations or legal proceedings;
- 25% reported that it caused delays or complications;
- none indicated that the lack of data had minimal or no impact; and
- none reported being unable to assess the operational impact.

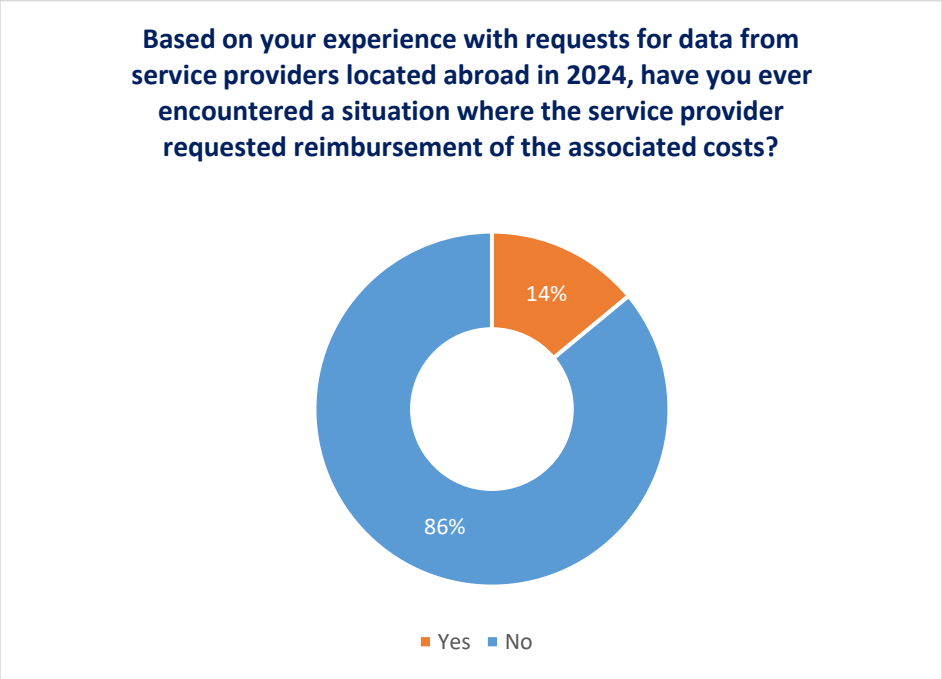


These findings demonstrate that divergent or limited data retention periods for law enforcement purposes can result in the loss of potentially crucial information. This not only affects individual investigations but may also undermine the overall effectiveness of cross-border judicial cooperation. Addressing these challenges may therefore require continued legislative reflection, enhanced coordination between jurisdictions and targeted capacity building to mitigate the operational impact of data unavailability.

Implications of cost reimbursement

As highlighted above by the Mexican judiciary, service-related costs incurred when obtaining electronic evidence may represent a potential challenge for competent authorities seeking access to electronic data. However, at present, the reimbursement of costs associated with compliance with requests from authorities does not appear to have a significant impact on access to electronic evidence in practice.

Similarly to the experience reported by EU judicial authorities, the survey results indicate that only a limited proportion of non-EU respondents (14%) encountered situations in which a service provider requested reimbursement for costs associated with responding to data requests. The remaining 86% reported that they had never received such claims, suggesting that, to date, cost reimbursement has had a limited practical impact on the electronic evidence retrieval process.

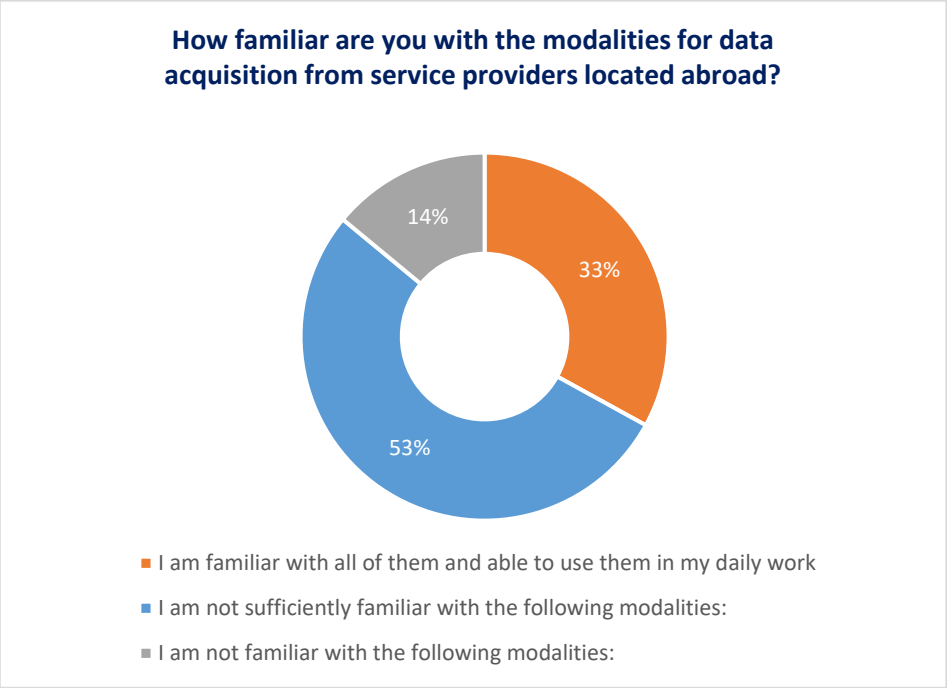


At the same time, the survey reveals a fragmentation of national legal frameworks among non-EU countries that mirrors the situation observed within the EU. National approaches to cost reimbursement vary considerably across jurisdictions. In some non-EU countries, such as Iceland and Switzerland, national legislation explicitly provides for the reimbursement of costs incurred by service providers when responding to requests from competent authorities. In other jurisdictions, no explicit provisions on cost reimbursement exist (for example, Bosnia and Herzegovina), while in certain countries service providers may be required to comply with requests at their own expense, as reported in Canada.

The need for expanding knowledge and capacity

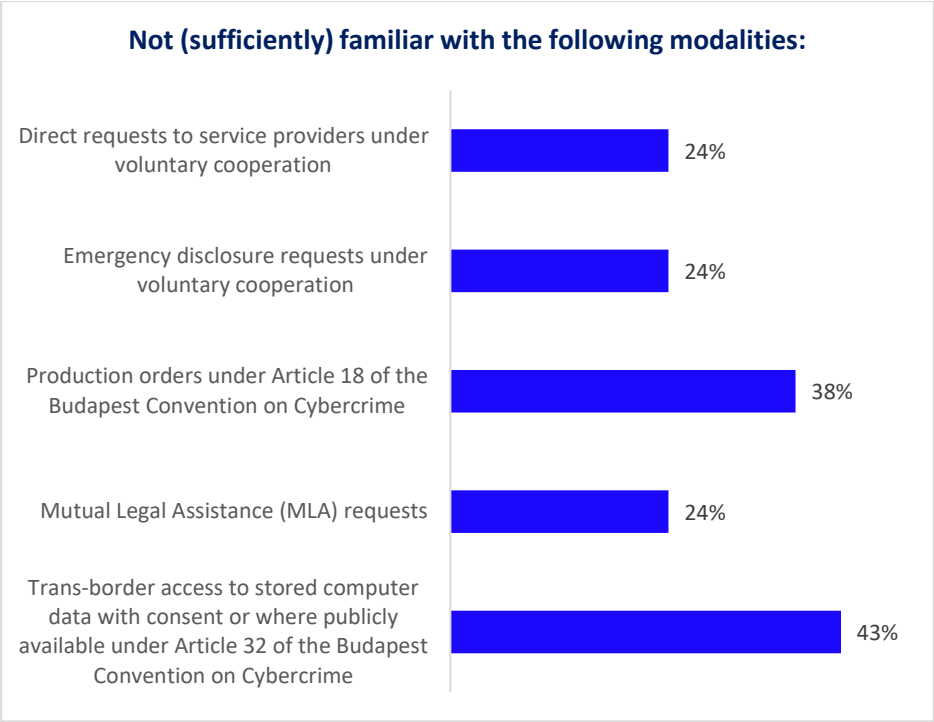
Similarly to EU judicial authorities, judicial authorities from non-EU countries were also surveyed on their level of familiarity with the existing modalities for obtaining data from service providers located abroad. The results point to notable gaps in familiarity with the applicable legal instruments, which may adversely affect their effective and timely use in cross-border investigations.

In particular, 53% of respondents indicated that they are not sufficiently familiar with the currently available modalities for cross-border data acquisition, while a further 14% reported limited familiarity with some of them.



A closer examination shows that, similarly to EU judicial authorities, judicial authorities from non-EU countries would benefit from enhanced knowledge and capacity-building, in particular with regard to trans-border access to stored computer data with consent or where such data are publicly available under Article 32 of the Budapest Convention on Cybercrime; production orders under Article 18 of the Budapest Convention; and emergency disclosure requests based on voluntary cooperation.

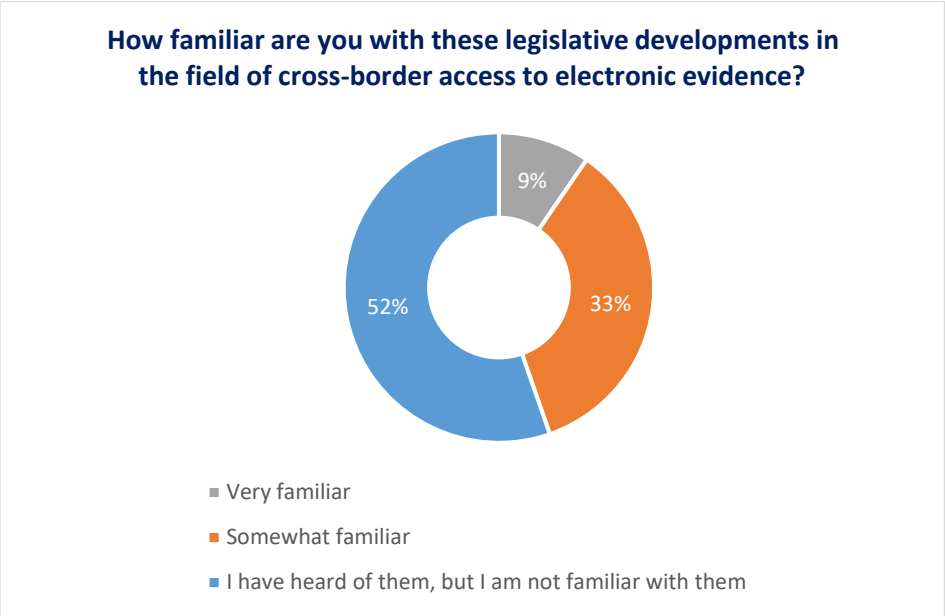
Specifically, 43% of respondents reported either a lack of familiarity or no familiarity at all with trans-border access to stored computer data under Article 32 of the Budapest Convention, followed by 38% who identified production orders under Article 18 of the Budapest Convention as an area requiring further knowledge. Furthermore, direct requests to service providers and emergency disclosure requests under voluntary cooperation, as well as MLA requests, were all identified by 24% of respondents as requiring additional capacity-building.



Taking into account recent legislative developments, the results clearly indicate a need for targeted knowledge enhancement and capacity building for non-EU judicial authorities, particularly with regard to the instruments provided under the Budapest Convention, as well as deeper expertise in the most frequently used channels, notably MLA and measures based on voluntary cooperation.

To assess the level of awareness among EU judicial authorities regarding the evolving legal landscape, respondents were asked about their familiarity with recent legislative developments, in particular the Second Additional Protocol to the Budapest Convention on Cybercrime. This Protocol, which will enter into force following its ratification by five States, introduces additional instruments enabling competent authorities to engage with service providers for the purpose of obtaining data in criminal investigations and proceedings.

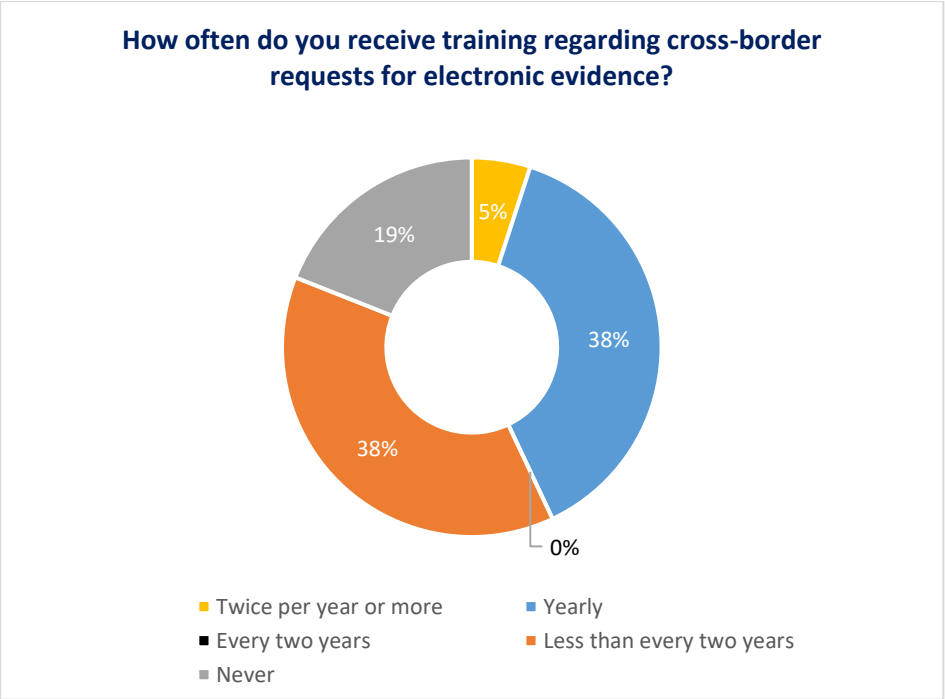
The survey results indicate that slightly more than half of the respondents (52%) have heard of the Second Additional Protocol but are not familiar with its content. A further 33% reported having some knowledge of the instrument, while only 9% indicated that they are very familiar with it.



The forthcoming legal instruments will provide important additional tools for more effective cross-border access to electronic evidence. However, their successful application will depend on judicial authorities being equipped with the necessary knowledge and skills to navigate and apply these new legal frameworks.

In this regard, the overall picture concerning training on obtaining electronic evidence across borders among judicial authorities from non-EU countries mirrors that observed for the EU judiciary.

According to the survey results, 38% of respondents from non-EU countries indicated that they receive training on this topic either on a yearly basis or less frequently than every two years. This is followed by 19% of respondents who reported that they have never received any training on obtaining cross-border electronic evidence up to 2024. Only 5% indicated that they receive such training at least twice per year, while none of the respondents (0%) reported receiving regular or continuous updates to their knowledge at least every two years.



The findings point to a clear need for strengthened and more systematic knowledge and capacity building for non-EU judicial authorities in the area of cross-border access to electronic evidence, particularly in light of the increasing complexity of the applicable legal frameworks.

Conclusions and implications

The survey demonstrates that both EU and non-EU judicial authorities face similar challenges in obtaining cross-border electronic evidence, particularly with regard to procedural delays, fragmented legal frameworks and limitations in data retention regimes.

MLA remains the principal channel for obtaining electronic data. However, authorities consistently report lengthy procedures, difficulties in identifying the appropriate jurisdiction, and partial or delayed responses from service providers. Voluntary cooperation offers a faster alternative, especially for non-content data, yet reliance on this channel varies across jurisdictions and depends on national legal frameworks and provider practices.

For EU judicial authorities, the introduction of the EU Electronic Evidence legislative package is expected to provide more efficient and harmonised tools for cross-border data access, thereby strengthening their ability to preserve and obtain essential electronic evidence. At the same time, the adoption and implementation of instruments under the Second Additional Protocol to the Budapest Convention will also further expand the available toolbox for non-EU judicial authorities. Nevertheless, authorities in both EU and non-EU countries continue to highlight data retention-related challenges, which may lead to the loss of critical information and adversely affect investigations and prosecutions.

Training and capacity-building emerge as key priorities across all jurisdictions. A significant proportion of EU and non-EU authorities report limited or infrequent training on cross-border access to electronic evidence, which constrains their ability to effectively apply existing instruments and prepare for forthcoming mechanisms. Strengthening practical guidance, reinforcing operational support and expanding

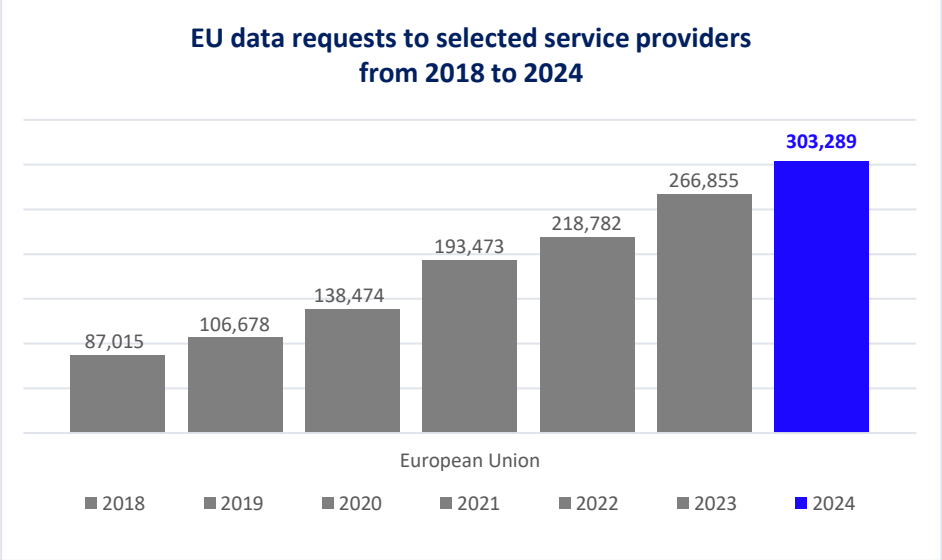
targeted training will therefore be essential to ensure that judicial authorities in both EU and non-EU countries can fully utilise the available tools and effectively access the electronic evidence necessary for successful investigations and prosecutions.

PERSPECTIVE OF SERVICE PROVIDERS

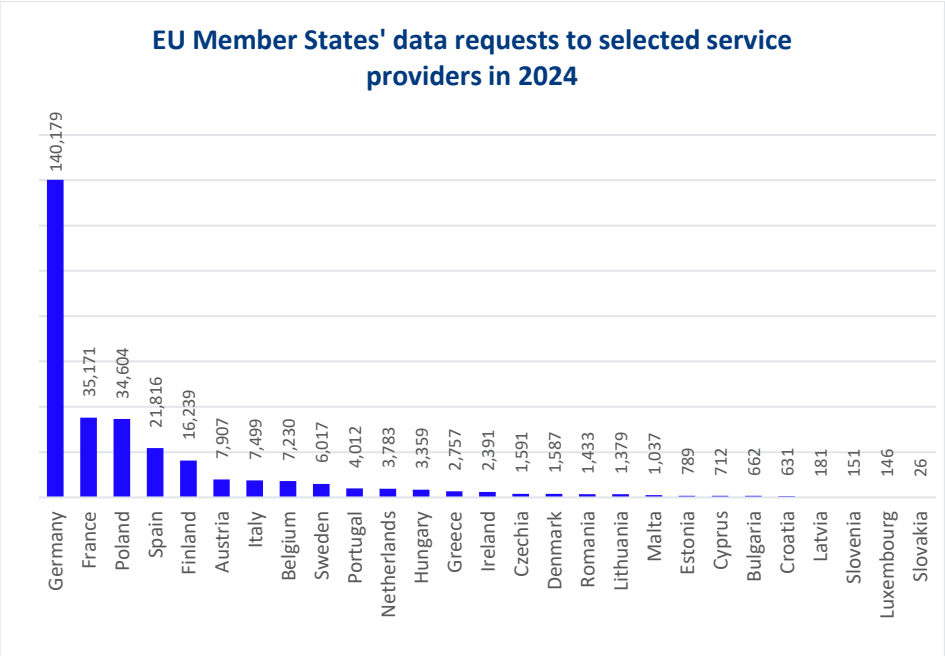
Volume of data requests per country and per service provider

SIRIUS has been analysing data request volumes by EU competent authorities since 2018 and there is one persistent trend: request volumes significantly increase every year. In other words, the 2024 request volume in this sample of providers is about 3.5 times the volume of the base-year 2018.

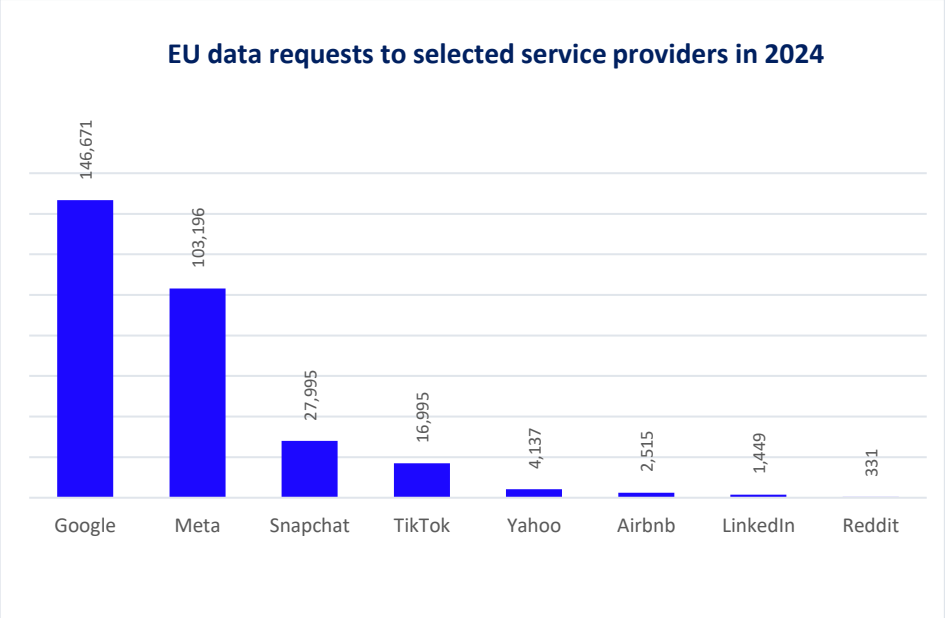
Data disclosure requests submitted by EU competent authorities to the selected eight service providers increased by about 14% from 2023 to 2024, totalling to 303 289 requests submitted to Airbnb, Google, LinkedIn, Meta, Reddit, Snap, TikTok and Yahoo in 2024. This is the result of the analysis of transparency reports published by the service providers.[13]



In 2024, Germany submitted the highest number of requests in the EU (140 179), followed by France (35 171). Combined, they account for more than 58% of requests submitted in 2024 to this sample of eight providers. Overall, there is no Member State with a reduction of more than 25% in its request volume while some have seen significant changes in which the request volume has doubled or even multiplied. First, while Cyprus had less than 30 requests in 2023, in 2024 that number has risen to 712 requests. Second, Finland has seen a tenfold request volume increase of 16 239 compared to the last reporting period of 2023. Third, Estonia, Ireland and Bulgaria have also faced significant increases.



Among the service providers analysed, Google and Meta receive the most requests by far, with 82% (249,867) of the total volume.

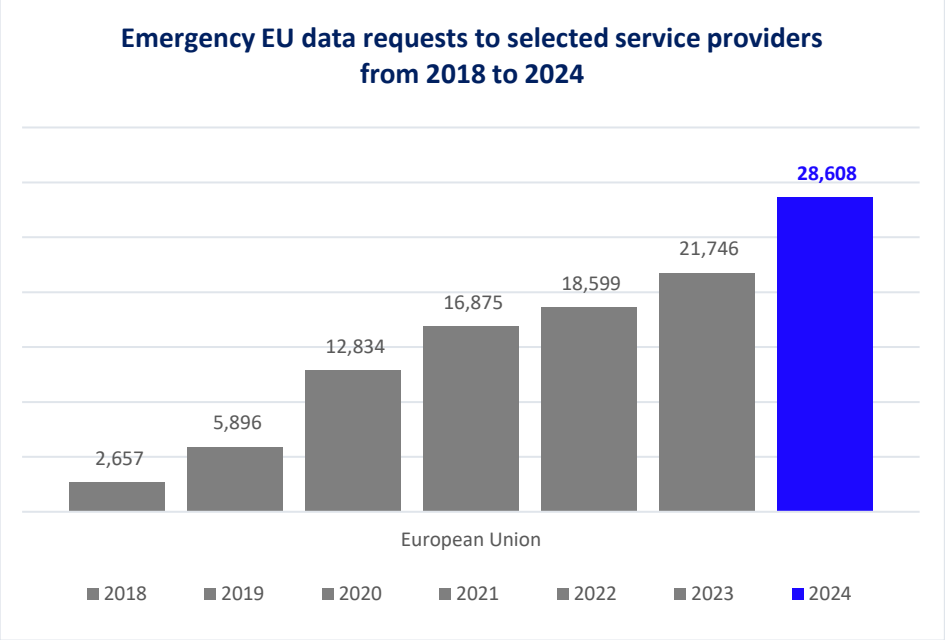


The assessment of requests under Article 10 of the DSA remains ambiguous as the different methodologies used in transparency reports differ by service provider. This undermines the systematic analysis, comparison and interpretation of the results (cf. EESR 2024). With regard to the relevance of request under DSA Art. 10, similarly to last year, only 5% of EU law enforcement survey participants responded that they use this Article in their requests, in combination with a legal basis under EU or national law. During the service provider interviews it was confirmed that only a small fraction of requests is made under Article 10 of the DSA. One explanation for this is that service providers already comply with voluntary requests, and requests made under Article 10 of the DSA are more complex and could therefore lead to higher rejection rates.

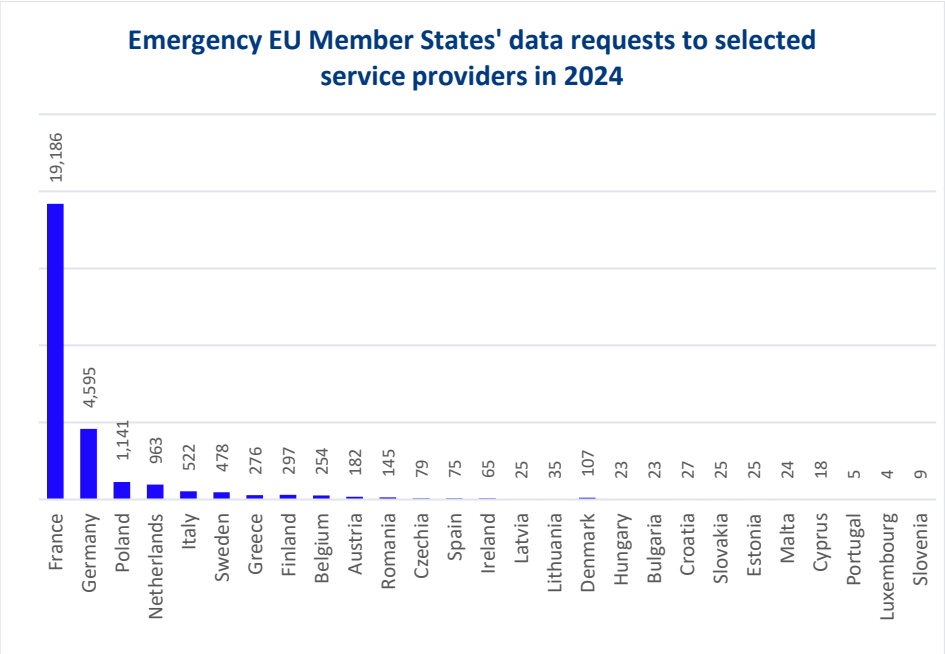
However, it is also possible that if the original order requesting evidence based on national or EU law fulfils the criteria under Art. 10 DSA, there is no need to send another order and the obligation under Art. 10 will be triggered by the original order.

Volume of Emergency Disclosure Requests per country and per service provider

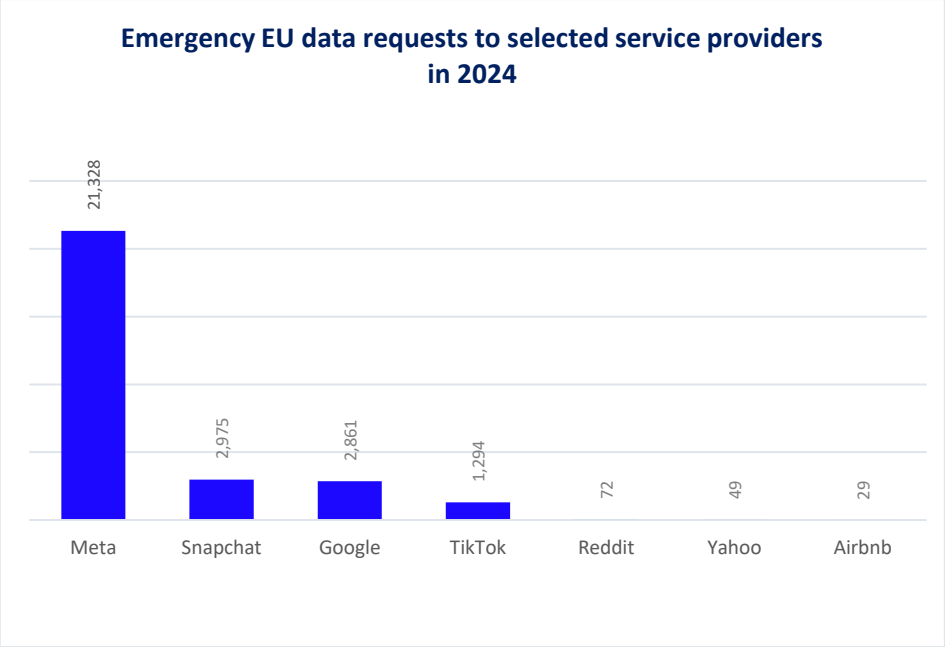
Emergency circumstances usually constitute situations where there is imminence of harm or serious physical injury to a person. Some service providers adopt a wider definition of emergencies to include imminent and serious threat to the security of a State, the security of critical infrastructure or installation or crimes involving minors. From 2023 to 2024, the absolute volume of Emergency Disclosure Requests issued by EU competent authorities jumped by 32% to 28 608, in the selected sample of service providers.[14] In relative terms, the proportion of emergency requests to total requests has slightly increased from 8% in 2023 to 9% in 2024.



While Germany tops the chart in terms of volume of voluntary requests, followed by France, they trade places in the case of emergency requests, with 19 186 requests by French and 4 595 requests by German authorities. Together, these account for the majority of emergency requests submitted, amounting to 83% (23 781) of the total. The results are presented overleaf.

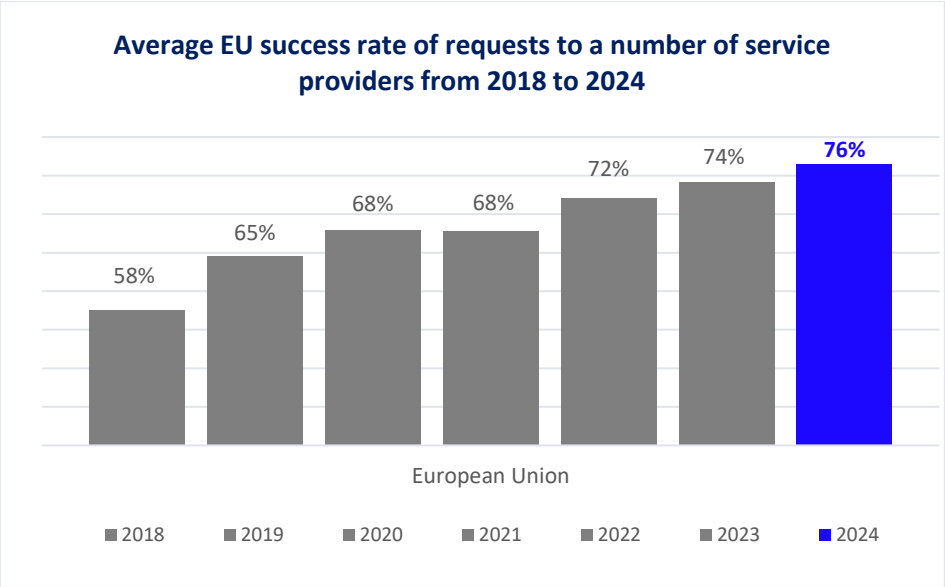


Meta received by far the most emergency requests in this sample of providers, with 75% (21 328) of the total volume.



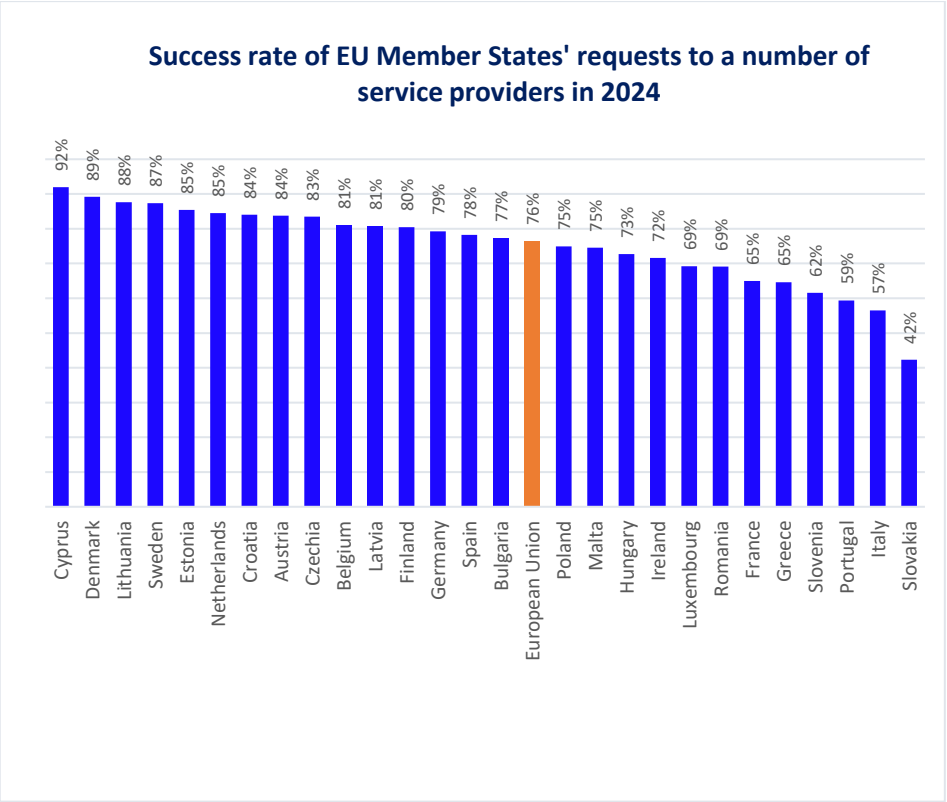
Success rate of EU cross-border requests for electronic evidence

The average success rate[15] of data disclosure requests submitted by EU competent authorities increased to 76% in 2024, continuing the positive trend of recent years. On average more than three out of four data requests are successful in the sample of providers used for this report. This is the best result since the first edition of this report in 2018.

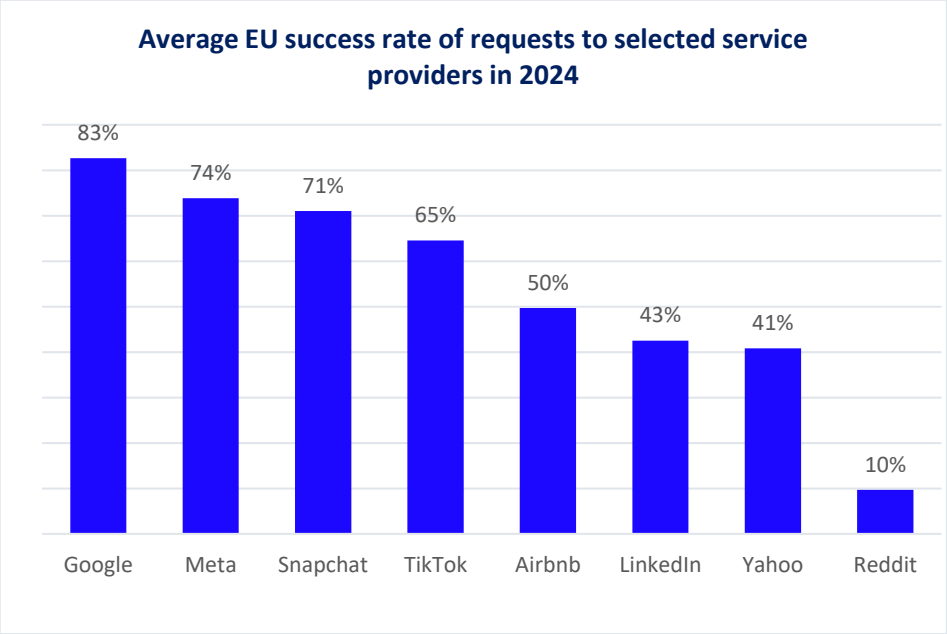


Similar to the last reporting, 15 Member States have success rates higher than the EU average in 2024. Among these, Cyprus, Denmark, Lithuania, Sweden, Estonia, Netherlands, Croatia, Austria, Czech Republic, Belgium, Latvia and Finland reach success rates of 80% or above. On the contrary, France, Greece, Slovenia, Portugal, Italy and Slovakia have success rates of less than 66%; at least every third request from these jurisdictions fails to retrieve data from the selected service providers analysed for this report. While the absolute number of requests varies greatly among these Member States and this affects interpretation, the results warrant further analysis of the causes for relatively low success rates in the interest of harmonising data requests among the Member States and to reach high success levels across the EU.

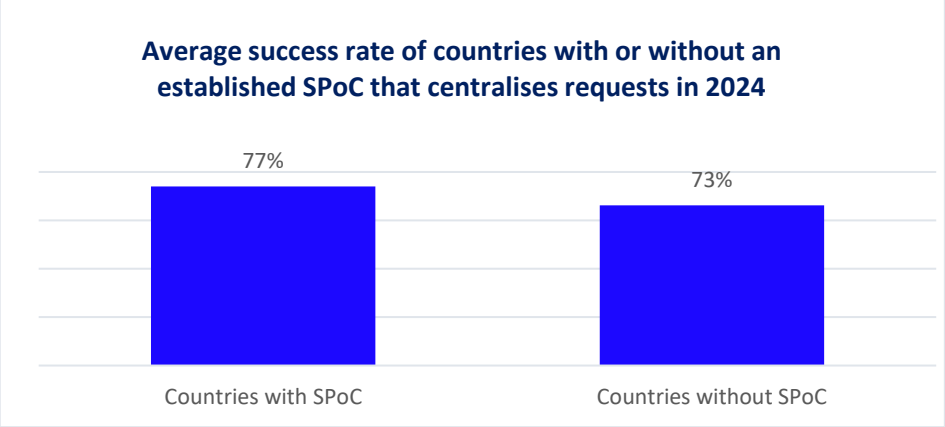
In the 2024 edition, Cyprus scores a success rate of 92% which is a sharp departure from the year 2023 where 0% was reported, as well as from previous years characterised by lower and fluctuating success rates in the Member State. The results are presented overleaf.



Among the companies analysed, Google had the highest success rate (83%) and Reddit the lowest (10%).



The average success rate of Member States with SPoCs for direct requests under voluntary cooperation in this analysis is 77% compared to 73% in those Member States without such units. The small difference in success rates might come as a surprise given the positive statements and experiences shared by authorities and service providers about SPoCs. One explanation for this is methodological. Due to the small sample size of service providers included, the explanatory value is biased. These providers are among those from which data is requested frequently; hence, requests to these providers have become more and more standardised over time, leading to efficiency gains made without dedicated SPoC units. To better measure SPoCs' efficiency, we advise taking other criteria into account and broadening the sample.



In the following sections, the quantitative perspective on service provider requests is complemented with qualitative evidence from interviews.

Reasons for refusal or delay to process requests from EU-authorities

Refusals or delays in the request process waste resources on both sides: for requestors and for service providers. While the average success rate for 2024 indicates that the voluntary request system is more efficient than ever, key issues remain that lead to refusals and delays. Some can be avoided. The below aggregation of reasons provides guidance for requesting authorities to further improve their success rates and to rule out common pitfalls.

Please bear in mind that individual service provider policies can vary greatly and require individual assessment per request. More detailed service provider specific information can be found in the SIRIUS guidelines on the Europol Platform for Experts.

Key reasons for refusals:

- **Wrong legal entity or data controller addressed**

  SIRIUS Tip: Entities and data controllers can change frequently. Make sure to regularly update this information and to avoid typos.

- **Legal defects**

  SIRIUS Tip: State a valid legal basis under national or EU law in requests and elaborate on it succinctly.

- **Service provider policy for voluntary requests not taken into account**

  SIRIUS Tip: Check the latest SIRIUS guidelines, service provider policies and standards. Seek clarification from the law enforcement response team of service providers, if in doubt.

- **Missing requirements to process the request**

  SIRIUS Tip: Include unique identifiers applicable to the service provider you are requesting data from. Make sure other requirements are met, too.

- **A “full dump” of data is requested**

  SIRIUS Tip: Do not make overly broad requests. Be as precise as possible and list the data categories and data types you are requesting. Avoid to use “full dump” as a description.

- **Avoid “impossible” requests**

  SIRIUS Tip: Assess if the data and data categories requested are available at the service provider before making a request. Indications for this can be found in the SIRIUS guidelines and service provider policies.

Key reasons for delays:

- non-unique identifiers used in request [can also lead to a direct refusal];
- incorrect information used in request;
- user is out of jurisdiction and service provider asks for EIO or MLA. This leads to a refusal of the specific requests, but might result in successful data received via another legal instrument, albeit with significant delay;
- request too broad (e.g. targeted number of accounts or time frame);
- weak justification for request;
- additional vetting of requesting authority;
- requests have become more complex over time.

Challenges for service providers with EU authorities

The challenges for service providers relate to the reasons for refused or delayed requests. Overall, collisions of different legal frameworks or legal conformity to adhere to in voluntary requests top the list. One additional factor to improve cooperation is the provision of context information on investigations that facilitates both the justification of a request and the fulfilment. Notably, the verification of requestors from EU law enforcement authorities has been mentioned several times during the interviews. These are the key challenges for service providers with EU authorities:

- collision of different legal frameworks (e.g. with privacy regulations) or legal conformity with multiple regimes;
- lack of understanding of company policy by requestor;
- not enough or non-unique identifiers provided by LEA (e.g. phone numbers are not always a strong identifier);
- non-harmonised request forms;
- lack of context or information on the investigation complicates request fulfilment;
- verification of requestor.

To address concerns related to the verification of requestors, the SIRIUS project has published an extensive whitelist of authorised email domains on the restricted SIRIUS platform for service providers. This resource is continuously updated and accessible to registered service providers. Additonal measures and coordination efforts between service providers and authorities, facilitated by the SIRIUS project, have taken place to ensure high levels of credibility.

The experience of service providers with SPoCs

From the perspective of service providers, the overall quality of SPoCs has consistently improved over the years. However, providers report significant fluctuations in quality between different SPoCs within and across jurisdictions. Moreover, most service providers see the continued relevance of SPoCs after the decentralised EU electronic evidence system is operational (planned for August 2026). However, a few providers are more sceptical about the future of SPoCs, noting uncertainty about processes under the new system with a potential limited role of SPoCs and further assessment required. Overall, SPoCs are described as follows and with these purposes valued most by service providers:

- very valuable and highly efficient;
- reduce friction;
- EU SPoC system as a global role model;
- important for vetting new LEAs;
- to verify requests in case of doubt;
- training and outreach.

EU Electronic Evidence legislative package

Most providers have started with the assessment and preparations for legal compliance under the new rules. The new legislative package is considered to bring legal certainty, albeit at significant transformation costs. During the interviews in late 2025, several concerns were raised regarding the implementation:

- globally operating service provides face conflicting legislation in the EU and US;
- uncertainty on the (feasibility of the) implementation timeline;
- uncertainty about how many platforms will be affected;
- uncertainty about how many requests will be generated;
- uncertainty if the decentralised IT system is fit for purpose;
- file size limit too low;
- new IT system not designed for the highest level of industry standards in encryption, such as end-to-end encryption across all processes;
- more details required on how the reimbursement process for requests will be implemented;

- trust between service providers and LEAs has been build-up over years, this process has to be started with judicial authorities now;
- increased training needs on the new IT system.

The continuation of voluntary cooperation

Voluntary cooperation remains a mechanism to engage with SPs to request data in cases not covered by the legislation. However, the EU Electronic Evidence legislative package is a partial transition from a voluntary request system to a system of mandatory responses to orders that comes with opportunities to streamline the request processes, but also with risks associated due to the transition. With the legislative package applicable and the decentralised IT system operational planned for August 2026, we have asked service providers bound by the new EU Regulation about their intent to maintain the voluntary cooperation mechanism. The answers were quite diverse: from undecided, to running a parallel system, to a hard shift to the new system, including discontinuation of voluntary disclosure of data. If challenges arise during the implementation of the new legislation and providers opt for a hard shift, risks to cross-border access to electronic evidence may emerge.

THE RELEVANCE OF SIRIUS FOR AUTHORITIES AND PROVIDERS

For many law enforcement officers, and increasingly for judicial authorities, SIRIUS has become synonymous with the facilitation of cross-border access to electronic evidence. This report marks the conclusion of Phase 2 of the SIRIUS project, which ran until the end of 2024.

The feedback received from law enforcement and judicial communities at this pivotal stage of the project, particularly in light of the forthcoming legislative transition from a voluntary to a mandatory request mechanism for electronic evidence in the EU in August 2026, highlights a strong need for structured support to facilitate this evolution. The perspective of the service providers complements this.

Finally, SIRIUS also presents a success story of two EU agencies jointly implementing a project over the course of several years, demonstrating how sustained cooperation can provide tangible added value to EU Member States and countries outside the EU, their authorities and ultimately to citizens.

For law enforcement

SIRIUS supports law enforcement in the EU and third countries. Continued support for EU Member States' authorities remains highly valued among the law enforcement community. When asked about the impact of discontinued support to EU authorities, these were some of the responses we received:

- *'It would be a major step back.'*
- *'Highly negative impact.'*
- *'It would be a disaster as its the only information available.'*
- *'Loss of a centralised knowledge hub.'*
- *'We would lose a hub of information, guidelines and sparring regarding all things e-evidence related.'*
- *'Sirius is the 'Bible'. Without it we have a lot less info.'*
- *'Reduced access to guidance, loss of insights.*
- *'Would have a very big impact, as it now helps us a lot in obtaining data as a SPoC.'*
- *'I would lose powerful tools provided by SIRIUS.'*
- *'If SIRIUS's support to EU authorities were to be discontinued, the impact on my work would be significant, particularly in the context of international cooperation and digital evidence gathering.'*
- *'It would be difficult to keep up with current trends in the field of digital evidence and international cooperation, which would slow down and reduce the efficiency of conducting investigations.'*

- *'Discontinuing SIRIUS support would slow down our access to digital evidence from service providers and reduce our capacity to handle cross-border investigations effectively and lawfully.'*
- *'The materials provided by SIRIUS are very helpful in everyday work, especially since they often concern rare cases related to international institutions. It is hard to imagine functioning without this organization.'*
- *'Your role is very important in the entire process. You have a wealth of knowledge and expertise about the possibilities for recovery, knowledge of legislation, and you have a very good network. Together, this gives you a unique position, making you the hub for both Law Enforcement and companies.'*

For judicial authorities

SIRIUS supports judicial authorities in the EU and third countries. EU judicial authorities rely on the SIRIUS project to strengthen their capacity, particularly in the following areas:

- *'[…] information about new/additional instruments in the field of acquiring data from service providers'*
- *'What kind of information the different service providers can provide and what each provider considers to be basic subscriber information'*
- *'Practical tools, best practices and information on how other EU member states are implementing the E-evidence package'*
- *'Practical implication with examples for EU E-evidence legislative package and Second Additional Protocol to the Budapest Convention on Cybercrime'*
- *'Methods and procedures of gathering electronic evidence abroad'*
- *'Usage of cross-border requests for electronic evidence'*
- *'Voluntary cooperation forms and guidelines'*
- *'Enhancing knowledge about the use of different legal instruments to obtain digital evidence in different countries'*
- *'Practical guidance on requests to service providers; Legal frameworks and recent updates on cross-border access; Technical aspects of evidence collection and preservation; Effective use of cooperation channels and networks'*
- *'Production orders under Article 18 of the Budapest Convention on Cybercrime; Production orders under national legislation in combination with Article 10 of the Digital Services Act'*
- *'How to acquire information from other countries or providers based in other countries'*
- *'Direct requests to service providers under voluntary cooperation, Emergency disclosure requests under voluntary cooperation, Production orders under Article 18 of the Budapest Convention on Cybercrime, Production orders under national legislation in combination with Article 10 of the Digital Services Act'*
- *'Strengthening efforts and collaborations with service providers'*
- *'E-evidence Regulation'*
- *'How to reach out to companies/providers abroad'*

For service providers

Throughout the number of interviews conducted, service providers reiterated the current and future relevance of SIRIUS. Most of them asked for SIRIUS to continue to be a facilitator between private sector entities and authorities, and described the training of law enforcement as one reason why request success rates have improved constantly over the last few years. Here are five additional aspects shared by service providers on SIRIUS:

- continue the SIRIUS EPE platform for service providers;
- continue the Annual SIRIUS Conference;
- grow the SPoC network;
- continue to train authorities;
- expand trainings to authorities to educate them on requests to small- and medium-sized service providers;

RECOMMENDATIONS

As the EU approaches the August 2026 transition towards a mandatory request mechanism for cross-border access to electronic evidence, it is crucial to maintain the flow of information between all stakeholders. The SIRUS community is one of the first stops to receive updates about the latest company policies and to facilitate outreach to national law enforcement or judicial authorities. Hence, SIRIUS highly recommends making use of this resource and network. From the insights of the 2025 SIRIUS Electronic Evidence Situation Report, the following specific recommendations can be derived for each of the three stakeholder groups.

For law enforcement agencies

Increase training to request cross-border access to data from service providers

First, success rates for requests have improved over the past few years and reached the high level of 76%. However, this means that 24% of the requests and thereby almost every fourth request is not successful. This number could be improved by a detailed analysis of why requests are not successful on the level of jurisdictions and even agencies to tailor training programmes accordingly.

This report provides several overarching reasons why requests are not successful as a starting point for further analysis. Among them are recurring mistakes reported by service providers, such as addressing the wrong legal entity in the request. These common mistakes could be addressed in these training sessions. In light of the new IT system, additional training could also be provided for the issuance of orders in emergency situations without prior judicial validation and if legal conditions are met.

Assess the potential of introducing or expanding the SPoC approach in your jurisdiction and/or agency

Streamlining processes and coordination with service providers is one key aspect of the work of SPoCs. Establishing or expanding this system can be beneficial to the success rates of requests in the jurisdictions and/or agencies, as accounts described in previous versions of this report have demonstrated.

Despite the upcoming system transition and the introduction of the decentralised IT system, several service providers interviewed for this report value the positive impact of SPoCs and see their relevance under the new system in the future.

Prepare for the effective application of new legal frameworks on cross-border access to electronic evidence

This final recommendation reiterates the need to prepare for the application of new legal frameworks on cross-border access to electronic evidence, particularly the EU Electronic Evidence legislative package. The recommendation holds across all stakeholder groups, but law enforcement potentially faces significant changes to long-standing established processes.

Therefore, national law enforcement authorities should continue to prepare for testing their IT systems to ensure they are ready for the planned go-live of the decentralised IT system in August 2026. This ensures that the transition to a mandatory system poses as little risk as possible for investigations from the perspective of law enforcement. Finally, to accommodate the new processes, further discussion and cooperation between law enforcement authorities and judicial authorities could be beneficial.

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

For judicial authorities

Strengthen capacity and practical expertise on available legal instruments for cross-border access to electronic evidence

Investment in continuous training on existing legal instruments and specific procedures for requesting the preservation and production of electronic evidence across borders is essential to equip judicial practitioners with the expertise required to obtain electronic evidence effectively, using tailored solutions that meet the specific requirements of each case.

To access specialised resources on cross-border electronic evidence, judicial authorities may contact the SIRIUS Project team at Eurojust via email at sirius.eurojust@eurojust.europa.eu.

Prepare for the effective application of new legal frameworks on cross-border access to electronic evidence

With the forthcoming entry into application of the EU Electronic Evidence legislative package and the anticipated entry into force of the Second Additional Protocol to the Budapest Convention on Cybercrime, building knowledge and capacity is pivotal to prepare judicial authorities for the procedural and practical changes these instruments will introduce.

Early engagement with training programmes, implementation guidance and awareness-raising initiatives is critical to ensuring a smooth transition, legal certainty and consistent application across jurisdictions. Structured preparedness will be essential to fully realise the potential of the new cross-border mechanisms introduced by these legal frameworks.

Enhance cross-border cooperation, mutual trust and knowledge sharing

Given the persistent challenges related to jurisdictional complexity, procedural delays and fragmented legal frameworks, strengthening mutual trust and promoting knowledge exchange among judicial authorities remain essential.

Judicial authorities are encouraged to actively participate in dedicated events, expert networks and platforms, such as those provided by the SIRIUS Project, to exchange best practices, clarify procedural approaches and improve coordination in accessing electronic evidence. Increased transparency, communication and peer engagement will contribute to greater consistency, predictability and efficiency in cross-border investigations.

For service providers

Assess the final readiness for the go-live of the decentralised IT system of the EU Electronic Evidence legislative package from a service provider perspective

With the planned go-live of the decentralised IT-system of the EU Electronic Evidence legislative package in August 2026, now is the time to perform last readiness checks and complete finals steps towards compliance.

Engage with the responsible authorities for final updates on the status of the implementation and ensure that cross-border access to electronic evidence remains available throughout the transition from a service provider perspective.

Engage with the SIRIUS community and share your company policy updates with the SIRIUS team

SIRIUS offers an online platform for service providers as well as events to disseminate policies and relevant updates to law enforcement and judicial authorities. In addition, the SIRIUS Project provides dedicated webinars to train law enforcement about specific company policies. Service providers can address a large number of officials in these sessions. Upon approval, the sessions can be recorded and made available on the restricted SIRIUS platform to reach all of the 7800+ members of the SIRIUS community.

Service providers may contact the SIRIUS Teams at Europol or Eurojust to make use of this opportunity: sirius@europol.europa.eu or sirius.eurojust@eurojust.europa.eu

END NOTES

[1] COM(2025) 349 final: Roadmap for lawful and effective access to data for law enforcement

[2] The service providers were chosen based on their relevance as indicated by competent authorities on previous occasions, as well as their availability to contribute to this report.

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

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

[5] 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.

[6] 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.

[7] 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.

[8] The official short name "Czechia" is used in graphics for better readability. This use is in accordance with guidelines from the Ministry of Foreign Affairs of the Czech Republic.

[9] SIRIUS EU Electronic Evidence Situation Report 2024, 6th Annual Report, 28 November 2024; SIRIUS EU Electronic Evidence Situation Report 2023, 5th Annual Report, 18 December 2023; SIRIUS EU Digital Evidence Situation Report 2022, 4th Annual Report, 22 December 20022; SIRIUS EU Digital Evidence Situation Report 2021, 3rd Annual Report, 24 November 2021; and SIRIUS EU Digital Evidence Situation Report 2020, 2nd Annual Report, 1 December 2020.

[10] 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, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0024.

[11] 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), available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

[12] A comprehensive review can be found consulting: SIRIUS EU Digital Evidence Situation Report 2022, 4th Annual Report, 22 December 2022; SIRIUS EU Digital Evidence Situation Report 2021, 3rd Annual Report, 24 November 2021; SIRIUS EU Digital Evidence Situation Report 2020, 2nd Annual Report, 1 December 2020; Eurojust, Cybercrime Judicial Monitor – Issue 8, 22 June 2023; Eurojust, Cybercrime Judicial Monitor – Issue 7, 30 June 2022.

[13] Apple, Microsoft and X (formerly known as Twitter) have been removed from the analysis in the 2024 report. This is kept in the 2025 report to ensure comparability between the reports.

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

[15] The definition of "success" relies on the individual definitions of success in the transparency reportings of the providers.

REFERENCES

The transparency reportings from the selected service providers of this report can be accessed through the following links:

- **Airbnb Law Enforcement Transparency Reports**
  https://news.airbnb.com/transparency/
- **Google Global requests for user information**
  https://transparencyreport.google.com/user-data/overview
- **LinkedIn Government Requests Report**
  https://about.linkedin.com/transparency/government-requests-report
- **Meta Government Requests for User Data**
  https://transparency.fb.com/data/government-data-requests/
- **Reddit Transparency Report**
  https://redditinc.com/policies/transparency
- **Snap Transparency Report**
  https://values.snap.com/privacy/transparency
- **TikTok Information Request Report**
  https://www.tiktok.com/transparency/en/government-removal-request-2025-1
- **Yahoo Government Data Requests**
  https://www.yahooinc.com/transparency/reports/government-data-requests/JUL-DEC-2024/index.html

The links were first accessed in Q4/2025 and last checked in Q1/2026.

ACRONYMS

AI	Artificial Intelligence
AR	Augmented Reality
CJEU	Court of Justice of the European Union
CJICO	Criminal Justice International Cooperation Office
DSA	Digital Services Act
EDR	Emergency Disclosure Requests
EIO	European Investigation Orders
EJCN	European Judicial Cybercrime Network
EJN	European Judicial Network
EU	European Union
IP	Internet Protocol
LEA	Law Enforcement Agency
MLA	Mutual Legal Assistance
OSINT	Open-Source Intelligence
SPoC	Single Point of Contact
US	United States of America
VLOP	Very Large Online Platform
VLOP(s)	Very Large Online Platforms
VLOSE	Very Large Online Search Engine
VLOSE(s)	Very Large Online Search Engines
VPN	Virtual Private Network
VPN	Virtual Private Network
VR	Virtual Reality