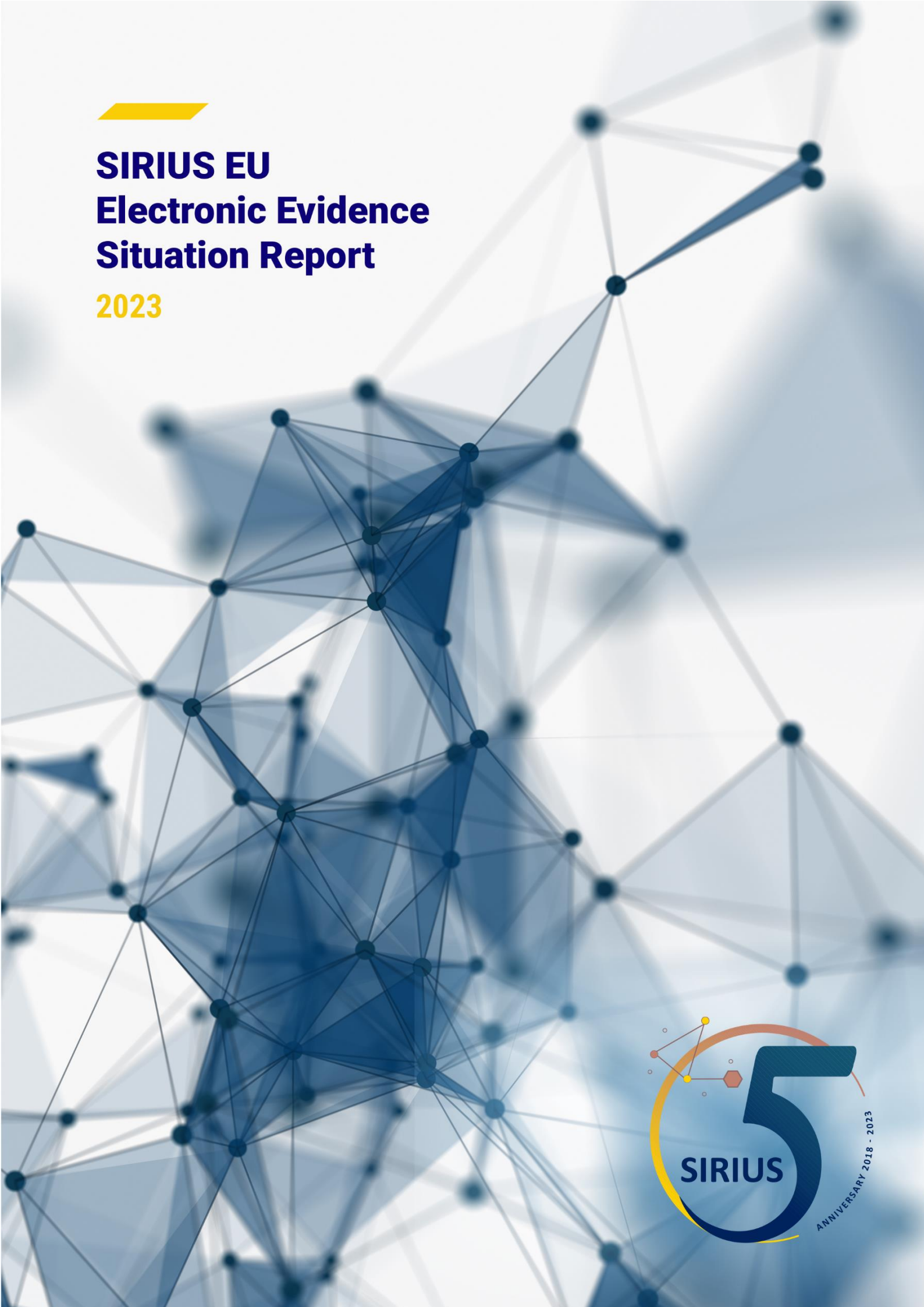
SIRIUS EU Electronic Evidence Situation Report

2023



SIRIUS EU ELECTRONIC EVIDENCE SITUATION REPORT 2023

The Hague, November 2023

SIRIUS CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

EUROPOL

EUROJUST

EUROPEAN JUDICIAL NETWORK
Connecting Justice

5th ANNUAL SIRIUS EU ELECTRONIC EVIDENCE SITUATION REPORT

An updated version of this report was published with editorial amendments on 14 February 2024 and 11 April 2024.

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

Your feedback matters.

By clicking on the following link or scanning the embedded QR code you can share your feedback regarding this report.

Your input will help us further improve our products.

HTTPS://EC.EUROPA.EU/EUSURVEY/RUNNER/SIRIUS_REPORT_FEEDBACK

INDEX

This year's SIRIUS EU Electronic Evidence Situation Report, jointly published by Europol, Eurojust, and the European Judicial Network, represents a continued effort to shed light on the ever-evolving landscape of cross-border investigations involving electronic evidence within the European Union. Now celebrating its 5th anniversary, the SIRIUS Project has grown into a centre of excellence of electronic evidence within the EU.

This report provides an overview of the EU's Electronic Evidence landscape through the lenses of law enforcement, the Judiciary, and Service Providers. Highlighting the profound significance of the forthcoming EU Electronic Evidence legislative package, transformative online technologies and shifting legal landscapes emphasise the need for a prepared, adaptable and pro-active law enforcement.

Not only does this report unveil that the demand for cross-border access to digital evidence remains unabated, it also demonstrates that platforms like social media, messaging apps, and cryptocurrency exchanges still play a key role in criminal investigations. Moreover, EU law enforcement officers still face challenges that result from new technologies, including internet-enabled home devices, smart cars, and artificial intelligence and metaverse platforms.

To meet these challenges head-on, Europol maintains its commitment to deliver security in partnership. We will continue to work closely with partners on both EU and Member State levels in the field of electronic evidence, as well as with private sector entities. Together, we will navigate the complexities of the digital age and ensure that the pursuit of a safer Europe remains undeterred by the criminal abuse of technological innovation.

Catherine De Bolle
EXECUTIVE DIRECTOR, EUROPOL

I thank SIRIUS for saving lives.

Law enforcement access to data can be a matter of life or death. Every day, lives depend on police finding the right IP address or location data. And every day for the last five years, SIRIUS has supported police and judicial authorities' access to digital evidence and data.

SIRIUS is growing day by day, now counting 7,000 law enforcement users, and the list of connected service providers is expanding, in part thanks to EU funding.

I commend Europol's efforts in making SIRIUS successful, and the exemplary cooperation between EU agencies, with Europol and Eurojust jointly in charge and Cepol providing training and innovative tools for online investigations.

In the years ahead, this strong partnership will allow SIRIUS to provide even better support, also in the light of two other recent developments: new EU electronic evidence rules that allow law enforcement swift access to evidence across borders, and the Second Additional Protocol to the Budapest Convention, which improves access to digital data.

In the years ahead accessing data will only become more important to fight crime, and essential to fight the organised crime which poses such a great threat to our societies. As the need to lawfully access information grows, so will the importance of SIRIUS.

SIRIUS allows us to be serious about fighting crime.
I sincerely recommend this situation report.

Ylva Johansson
EUROPEAN COMMISSIONER FOR HOME AFFAIRS

With the end of the year on the horizon, I am very pleased to help introduce to you the SIRIUS Situation Report 2023 on EU Electronic Evidence. There are many things for us to look back at, and this is true both from an operational point of view as well as from a legislative perspective.

As evidenced further on in this report, judicial professionals and law enforcement officers often had to rely on data disclosed by service providers as their only original investigative lead. This prompts the need for further reflection on how and under which circumstances this information can be made available before any such data is forever lost. In that respect, important progress was made earlier this year in July when the EU Electronic Evidence package was voted into law and which we look forward to being fully applicable as of August 2026. Equally important in the field of electronic evidence gathering this year was the gradual roll-out of the EU Digital Services Act's (DSA) provisions, which are likely to have a profound impact on our work with online service providers in and far beyond the European Union.

All these developments will doubtlessly help shape tomorrow's cross-border judicial cooperation landscape, and we are therefore grateful that we can rely on SIRIUS' guidance and expertise. Its work offers a shining light for legal and police practitioners in all corners of our continent faced with an ever bigger digital dimension in their work. With that in mind, I look forward to much more to come from our SIRIUS-colleagues.

Ladislav Hamran
PRESIDENT, EUROJUST

Once again, it is my pleasure to endorse the annual SIRIUS EU Electronic Evidence Situation report. Investigating and prosecuting crime in the digital age is no simple task. For judicial authorities it can be cumbersome and time-consuming to access data from service providers. Recent legal developments, particularly the 2023 EU Electronic Evidence legislative package, offer promising solutions, and will make it possible for competent authorities to issue legally binding orders directly to service providers offering services in the EU, regardless of their place of establishment and of the data storage location. This bolsters the capacity of the EU judiciary to combat crime effectively.

The SIRIUS project, a centre of excellence in the field of cross-border access to electronic evidence in the EU, is in the best position to support EU Member States' authorities in the preparation and application of the new EU electronic evidence legislation, via its capacity-building activities and its repository of data in the field of electronic evidence.

The SIRIUS project is an invaluable tool for anyone with an interest in the use of electronic evidence in criminal investigations. It provides relevant and user-friendly, practical resources, such as an up-to-date contact book listing over 1000 Online Service Providers, and analyses of relevant policy developments to assist investigations. It is essential for all EU law enforcement professionals and for the judiciary.

Didier Reynders
EUROPEAN COMMISSIONER FOR JUSTICE

EXECUTIVE SUMMARY

The need for electronic data in criminal investigations is an unmistakeable reality in the EU and beyond. Investigating and prosecuting crime in the digital age is no simple task. While electronic evidence is crucial in criminal investigations, the legal instruments to request the disclosure of data at international level are deemed lengthy and cumbersome. As a result, voluntary cooperation between law enforcement and service providers has become the preferred solution to obtain non-content data. The volume of requests under voluntary cooperation has increased over the years, but this approach still lacks legal clarity for the involved parties. The recent legal developments in the field of judicial cooperation will redefine the cross-border gathering of electronic evidence. These legal developments are set to dispel the ambiguities surrounding voluntary cooperation channels.

The SIRIUS Project, implemented by Europol and Eurojust, acts as a centre of excellence in the field of cross-border access to electronic evidence in the European Union (EU). Celebrating its fifth anniversary this year, SIRIUS assists over 6500 law enforcement officers and 500 judicial authorities from 47 countries[1] in navigating the complex and constantly-evolving field of electronic evidence.

In July 2023, the EU adopted the Electronic Evidence Regulation[2] and Directive[3] (EU Electronic Evidence legislative package). This new legislative package represents a paradigm shift in electronic evidence, because it will allow competent authorities to issue legally binding orders directly to service providers offering services in the EU, regardless of their place of establishment. The new instruments will introduce new forms of judicial cooperation procedures designed to work faster and more flexible than the existing judicial cooperation channels for collecting electronic evidence (i.e. EIO and MLA processes). However, the new rules will only be applicable as of August 2026.

Taking into account the important developments that occurred in 2023, the three chapters of this report focus mainly on 2022, from three different perspectives. The report demonstrates that numerous stakeholders are positive about the upcoming EU Electronic Evidence legislative package, while acknowledging that commitment and effort will be required to prepare for its practical implementation.

From the perspective of law enforcement, social media platforms, messaging apps and cryptocurrency exchanges were deemed the most relevant online services in criminal investigations. Predominantly direct requests under voluntary cooperation are put forward or issued by police departments. Additionally, connection logs, IP addresses and subscriber information continued to be the most important datasets in criminal investigations in the EU in 2022. Furthermore, only 7% of police officers say they are very familiar with the EU Electronic Evidence legislative package. However, 60% of officers report having received formal training on electronic evidence – this is the highest percentage since the first edition of this report was published in 2019. In 2022, the main issues for law enforcement when trying to obtain electronic evidence across

borders were the delays encountered in the MLA process and the lack of standardisation of the policies of service providers.

From the perspective of judicial authorities, the process of using existing judicial cooperation instruments to access data from service providers situated in foreign jurisdictions often proves excessively time-consuming. This challenge persisted as a significant obstacle faced by the EU judiciary when seeking electronic evidence across borders in 2022. Recent legal developments, particularly in the realm of judicial cooperation, offer promising solutions to mitigate this issue. These developments introduce new legal powers and enhance the role of the EU judiciary in requesting electronic evidence across borders for criminal proceedings. It is therefore essential to bolster the capacity of the EU judiciary to effectively combat crime. However, to successfully obtain access to electronic data, such data must first be available. As already underscored in previous reports, another critical and recurrent challenge faced by EU judicial practitioners is the absence of a data retention framework for law enforcement purposes. As a result, there remains a pressing need for comprehensive legislative efforts at the EU level to address and regulate this matter.

From the perspective of service providers, some of the current challenges in the field of electronic evidence are authenticating incoming requests and allocating resources to communicate with one-time requesters. In this regard, Single Points of Contact (SPoCs) for the centralisation of requests under voluntary cooperation ensure a higher success rate of requests, in comparison with authorities using a decentralised approach. Moreover, the perceptions and the concerns of service providers around the upcoming EU Electronic Evidence legislative package vary greatly. Many of them welcome the new rules, which will provide greater legal clarity, but also express some concerns such as how to prepare to meet the deadlines which will be imposed on them, especially as there is no indication of the expected volume of orders they may receive. At this stage, it is unclear if voluntary cooperation will still be possible and if it will be accepted by service providers once the EU Electronic Evidence legislative package will enter into application in 2026.

RECOMMENDATIONS TO STAKEHOLDERS

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

For EU Law Enforcement Agencies

- Initiate preparations for the implementation of the EU Electronic Evidence legislative package;
- Include training on cross-border access to electronic evidence in routine training programmes for investigators and first responders;
- Ensure active engagement of SPoCs in the SIRIUS SPoC Network.

For EU Judicial Authorities

- Enhance knowledge and build capacity on available legal instruments for cross-border access to electronic evidence;
- Prepare judicial authorities for the use of new instruments under the upcoming legislative changes related to the cross-border gathering of electronic evidence;
- Strengthen mutual trust and exchange of expertise among EU judicial practitioners on cross-border gathering of electronic evidence.

For Service Providers

- Initiate preparations for compliance with the EU Electronic Evidence legislative package;
- Engage in international events organised by SIRIUS and share policy updates with the SIRIUS Team.

KEY FINDINGS

PERSPECTIVE OF LAW ENFORCEMENT IN THE EU

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

Over 75% of officers are satisfied with the SPoC process, in agencies where these are established.

Only 7% of officers consider themselves very familiar with the EU Electronic Evidence legislative package adopted in July 2023.

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

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

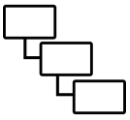
"The new legislative efforts will greatly facilitate time-consuming procedures and significantly speed up the acquisition of electronic evidence."

"The success of the new policy will depend on whether today's process under voluntary cooperation will continue to work. If not, our work will be more challenging"

PERSPECTIVE OF JUDICIAL AUTHORITIES IN THE EU

Lengthy MLA procedures and the lack of an EU-wide data retention framework remain the core issues.

Recent legal developments will create new legal powers and put the EU judiciary in a central role as concerns requesting access to electronic evidence.



Requests for electronic data often take place in a cascading manner, starting from subscriber information, and later traffic and content data.

Capacity building is essential for the EU judiciary to ensure proper awareness, knowledge and skills.

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

"The electronic evidence package opens a new era of faster and effective cross-border cooperation, ensuring that justice finally adapts and becomes agile also in the digital space. As legal practitioners, we welcome this forward-looking approach and are confident that it will strike the right balance between speedy investigations and the protection of fundamental rights"

PERSPECTIVE OF SERVICE PROVIDERS

The volume of EU data disclosure requests increased by 14% from 2021 to 2022.

The success rate of EU requests in 2022 was 73%, which is the best result since the first edition of this report.

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

It is not yet clear if the current practice of voluntary cooperation will continue to be accepted by service providers after mid-2026.

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

"The new Regulation will bring more legal certainty to the process of data disclosure in criminal investigations"

"Competent authorities should provide continuous and high-quality training to officials, to ensure that European Production Orders take into consideration the specificities of each service provider."

INTRODUCTION

The SIRIUS Project celebrates its fifth anniversary in 2023. Today, SIRIUS acts as a centre of excellence in the field of cross-border access to electronic evidence in the EU. Implemented by Europol and Eurojust, the project assists over 7200 law enforcement officers and over 500 judicial authorities. SIRIUS is active in all 27 EU Member States, as well as 20 third countries, in the process of requesting data from service providers, in the context of criminal investigations.

About the SIRIUS Project

SIRIUS promotes multi-stakeholder dialogue and fosters cooperation by deploying strong outreach efforts, organising international events for experts, preparing public and restricted knowledge resources. The project also delivers restricted online and in loco training for practitioners. SIRIUS helps practitioners navigate legal and policy developments in the field of electronic evidence. For instance, SIRIUS already provides guidance to authorities on the upcoming EU Electronic Evidence legislative package, as well as the *Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and disclosure of Electronic Evidence* (Second Additional Protocol), and offers information on the negotiations for the United Nations (UN) convention on cybercrime. 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 was able to achieve results by partnering with international stakeholders to promote the standardisation of processes and templates. Not only does SIRIUS contribute to international capacity building activities in the EU, but also to several events worldwide.

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

Highlights:

What the service providers, law enforcement and judicial authorities are saying about the SIRIUS Project:

"Microsoft regards it crucial for the public safety of all EU citizens that their law enforcement agencies know how to lawfully obtain Electronic evidence when they need to. The SIRIUS Project provides a valuable information hub, so police officers and prosecutors in a small village in a rural area of Europe have access to the same specialist knowledge as those in the capital cities."

Assistant General Counsel,
Law Enforcement & National Security, Microsoft

"Through innovation, collaboration, and pragmatism, the SIRIUS Project encouraged and strengthened the SPoC system throughout the EU, fostered smooth information exchange, and promoted efficient coordination among diverse stakeholders. The positive impact of the SIRIUS Project in the area of cross-border access to evidence is beyond question."

Senior Manager,
Law Enforcement Response Team of a service provider

"The SIRIUS project has been extremely useful as a central reference point for knowledge regarding the service providers and obtaining electronic evidence. We have learned new things while having the opportunity to talk with colleagues from other countries. We have also created direct connections with service providers in the SIRIUS events. For example, thanks to a SIRIUS meeting, our country is now receiving data directly from one of the biggest service providers that earlier just released the data through MLAT process form the U.S."

Police Inspector,
National Bureau of Investigation, Finland

"SIRIUS events are necessary for investigation teams to make contacts, learn new techniques and be informed about the latest trends in electronic evidence. This is crucial, because it is difficult for an investigative agency to keep up with all of the changes and new providers, which is why the SIRIUS Project is of great value to the investigative community. For rapid information sharing, coordination among the various SPoCs via the SIRIUS SPoC Network is very important. Establishing good contacts has already led to great results."

Police Officer,
National Police, Netherlands

"Thanks to the SIRIUS SPoC Network, when facing a new situation where we can easily contact the other EU SPoCs, ask if they are having the same situation, and how it is being handled. Sometimes we can get the solution even before the problem arises. It is also thanks to that Network that the experiences learned by one SPoC are shared to all the others, which is of high value."

Police Officer, Head of the SPOC for data requests,
Federal Police, Belgium

"SIRIUS repeatedly provides law enforcement with good answers and useful ideas concerning OSINT and Digital Forensics."

Police Chief Inspector,
Police Security Service, Norway

"The SIRIUS project, implemented jointly by Eurojust and Europol, has created the EU's central knowledge hub for cross-border access to electronic evidence, bridging the gap between online service providers on the one hand and law enforcement and judicial authorities on the other. With its growing community, which includes not only EU authorities but also those from third countries, SIRIUS is an example of the European Union's commitment to wide-ranging cooperation and effective justice in the digital age."

District State Prosecutor,
Supreme State Prosecutor's Office of the Republic of Slovenia

Context

The need for electronic data in criminal investigations is an unmistakeable reality in the EU and beyond. The widespread use of online services by criminals in any crime area requires law enforcement and judicial authorities to constantly adapt themselves to new challenges in order to keep citizens safe. Accessing specific data from targeted individuals needed in criminal investigations can be done in different ways, depending first and foremost on the applicable law, but also on other variables, such as, for example, on where the data is stored and whether or not it is publicly available. Often, authorities resort to directly requesting service providers to disclose specific data about suspects that could not be otherwise obtained.

For competent authorities, obtaining targeted user data from service providers can be a complex and lengthy task. This is mostly due to the fact that service providers are often

based in jurisdictions different from the investigating ones. Moreover, most existing applicable legal instruments for cross-border access to electronic evidence were created before the era of cloud computing and the widespread use of online services. Often, EU competent authorities must deal with cumbersome legal procedures which do not provide the necessary speed for obtaining electronic evidence.

Until now, competent authorities have often resorted in recent years to requesting disclosure of non-content data directly from service providers under voluntary cooperation in jurisdictions where this is possible. However, this approach is not regulated, at national level in all EU Meber States and competent authorities often find themselves having to deal with different legal requirements on top of those established by each service provider and with uncertainty as to whether the data so obtained can be admissible as evidence in court. In addition, competent authorities are also faced with the fact that some service providers do not cooperate voluntarily at all, either because of their legal obligations under domestic law, or due to lack of resources or willingness to establish such policies.

In this context, 2023 marked an important year in the field of cross border access to electronic evidence, as the new EU Electronic Evidence legislative package was adopted[4]. Whereas the new legislation will apply only as of mid-2026[5], its adoption sets a clear path for EU Member States and service providers to adapt existing processes and procedures, bringing more legal certainty and efficiency to the process of obtaining electronic evidence across borders in the future.

The EU Electronic Evidence legislative package is two-fold, composed of a Regulation[6] and a Directive[7].

First, the Regulation represents a paradigm shift in relation to cross-border access to electronic evidence, as it enables competent authorities to send an order requesting the preservation or production of electronic evidence directly to service providers offering services in the EU, regardless of their place of establishment. Such orders will fall under the scope of judicial cooperation and will have to be issued or validated by a judicial authority.

Second, the Directive requires service providers offering services in the EU but based outside of the EU to designate a legal representative in at least one EU Member State, for the purpose of gathering electronic evidence in criminal proceedings. Furthermore, the EU Electronic Evidence legislative package includes strong safeguards to ensure full compliance with the Charter of Fundamental Rights of the European Union[8].

Specific aspects of the future processes remain unclear, including whether or not direct requests under voluntary cooperation will still be accepted by service providers[9]; and how authorities will ensure they remain up-to-date with the fast-evolving particularities of each service provider (e.g. which datasets can be requested, what are valid identifiers per service provider etc.).

In 2023, four other policy developments also unfolded in the field of electronic evidence in the EU and beyond:

- The Second Additional Protocol already received its second ratification[10], and only requires another three ratifications to enter into force. Among other provisions, the Second Additional Protocol introduces novel legal bases for direct cooperation to obtain domain name registration information and subscriber data between competent authorities and service providers and entities providing domain name registration services based in other jurisdictions for the purpose of investigations and prosecutions[11];

- The EU and the US resumed negotiations on an international agreement to remove conflicts of law and facilitate access to electronic evidence[12];
- The EU Digital Services Act (DSA)[13] took effect for very large online platforms[14] in August 2023, introducing standardised minimum requirements for orders to provide information under EU Member States' national laws [15];
- International negotiations also advanced in relation to the UN convention on cybercrime, with chapters dedicated to criminalising certain cyber-dependant and cyber-enabled conducts, providing a framework for international cooperation, mainly through extradition and mutual legal assistance measures, and promoting preventive measures and technical assistance[16].

While acknowledging the important developments of 2023 and future changes to legislation, this report mostly looks back at 2022. Using the most up-to-date data available to describe the state of play regarding the use of electronic evidence in the EU, this report offers a trend analysis. This can serve as an important baseline for authorities and service providers alike, to help prepare for the implementation of the new legal instruments.

In order to ensure alignment with the newly adopted EU Electronic Evidence legislative package, the present SIRIUS report has reviewed the terminology used in previous editions. For example, the title of the report has been changed to "SIRIUS EU *Electronic* Evidence Situation Report", instead of "SIRIUS EU *Digital* Evidence Situation Report", among other specific terms used throughout the text.

Methodology

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

Survey with law enforcement authorities

Europol conducted a survey among law enforcement agencies and collected 250 responses from representatives from all EU Member States, in April and May 2023.

The survey was open also to law enforcement authorities from non-EU Member States which have operational or working agreements with Europol. From Albania, Bosnia and Herzegovina, Canada, Colombia, Iceland, Japan, Moldova, New Zealand, Norway, Serbia, Switzerland and United Kingdom, 42 responses were received. The results relating to contributions from non-EU Member States are presented in a dedicated section in this report for comparison purposes, and they are not considered in the overall results of the chapter Perspective of Law Enforcement.

Survey with judicial authrorities

Eurojust collected feedback from judicial authorities from 24 EU Member States[17]. A survey was administrated from April to June 2023, reaching out to the judicial community on the SIRIUS Platform, as well as European Judicial Cybercrime Network

(EJCN) and European Judicial Network (EJN) Contact Points. In total, 43 in-depth responses were received reflecting the situation in 24 EU Member States. The compilation of this information forms the basis for the analysis and recommendations presented in this report.

Furthermore, this report presents the outcome of the discussions on the experience and way forward for the EJN as regards investigations involving encrypted information. The discussions took place in June 2023 at one of the workshops held during the 60th Plenary Meeting of the EJN under the Swedish Presidency of the Council of the EU. The EJN Contact Points and partners from within and outside of the EU shared their opinions and knowledge about the impact and difficulties of organised crime investigations for which specific encrypted devices/applications were used for communication.

Interviews with service providers

Europol and Eurojust interviewed representatives from Airbnb, Apple, Booking.com, Google, Meta, Microsoft, Snap, TikTok, Uber, WhatsApp and Zoom in May and June 2023[18]. Additionally, an interview with the Rakuten Group took place in Tokyo, in the framework of the SIRIUS Project study visit to Japan. The findings presented in this report should not be taken as the formal position of any of these private entities.

The main topics discussed with these companies were:

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

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

The transparency reports analysed for the purpose of this report were those of Google, Meta, Snapchat, TikTok, LinkedIn and Reddit. The numbers presented in this report for the years 2018 – 2021 differ from the results presented in previous reports. This is because data from Airbnb, Apple, Microsoft, Yahoo and X (formerly known as Twitter) have been removed from the analysis, since their transparency reports for the full year of 2022 had not been published as of 9 October 2023, when the draft of this report was finalised.

PERSPECTIVE OF LAW ENFORCEMENT

Examples of real cases

Europol requested EU law enforcement officers to share examples where electronic data was deemed crucial evidence in criminal investigations. The cases listed below demonstrate how access to specific data from targeted users can be critical for law enforcement to perform their duties when investigating different crime areas.

It is often the case that data disclosed by service providers is the only investigative lead. For instance, some of the cases below show that not receiving the requested data could have resulted in unsuccessful investigations[19].

"At the end of 2022, we had a case involving rape and human trafficking. The victim was lured via a live streaming app. The criminals deleted the app and the victim's account. Later, the victim managed to escape and she called the police. She didn't know the identity of the criminals or any other information about them. Using the SIRIUS Platform, we managed to get the contact details of the legal entity that offers the app. With a Direct Request, we got the details we needed to identify the users and their criminal group."

"A thorough investigation was launched into a series of social media accounts and instant messaging applications from which virtual activities of a jihadist nature were being carried out. Upon legal request, Google provided two IPs from which one of the e-mails used by the person under investigation had been accessed. Thanks to this, it [was] possible for judicial authorities to issue court orders and find the address from which these virtual terrorist activities were being carried out. Once the address was obtained, it was possible to determine who was the person committing the criminal activities and execute a home search warrant."

"There was a threat to a school from an anonymous e-mail address. By sending a direct request to a service provider, we obtained enough data to identify the person and the real nature of the threat."

"In the case of large scale fraud, we sent requests to a cryptocurrency exchange and we quickly received all the necessary data for the investigation. This allowed us to analyse and trace Bitcoin."

"We identified the organiser of a phishing scam in Poland through direct requests for voluntary cooperation to social media platforms, as well as considerable OSINT work."

"By using data received from a social media platform, we identified the accounts of suspects of recruiting money mules. Through further investigation, we found their crypto wallets which were used for money laundering purposes."

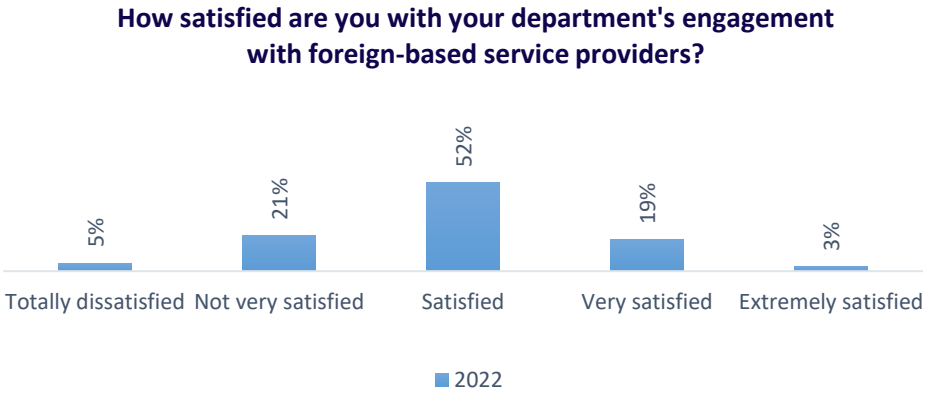
"In a very serious case concerning aggravated sexual assault, we had to try to make a request for user data based on a specific geolocation, along with some other creative investigative measures which we had not tried before. Due to the nature of the crime, we were able to have a meeting with the US Department of Justice, who helped us in formulating the MLA [request] the proper way. The suspect was apprehended before the MLA [request] made it through, but the process was good."

"In connection with an online credit card fraud, the company that we contacted in the US provided all the necessary information to identify the Hungarian perpetrator. An indictment was issued in this case. I use the SIRIUS Platform regularly; it definitely helps my work."

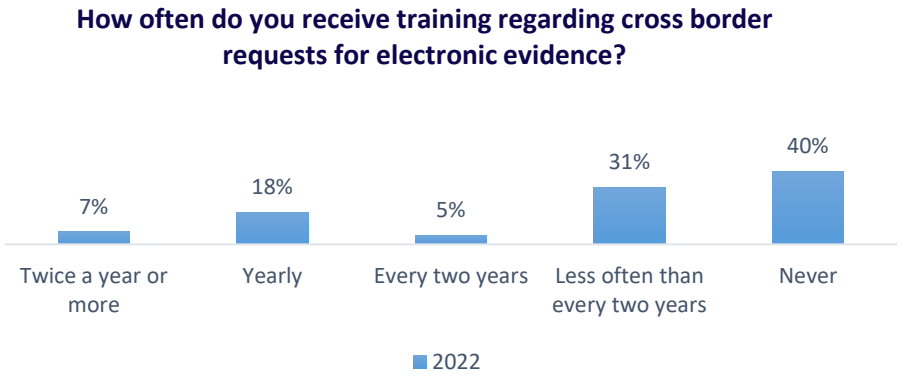
Engagement of EU law enforcement with foreign-based service providers

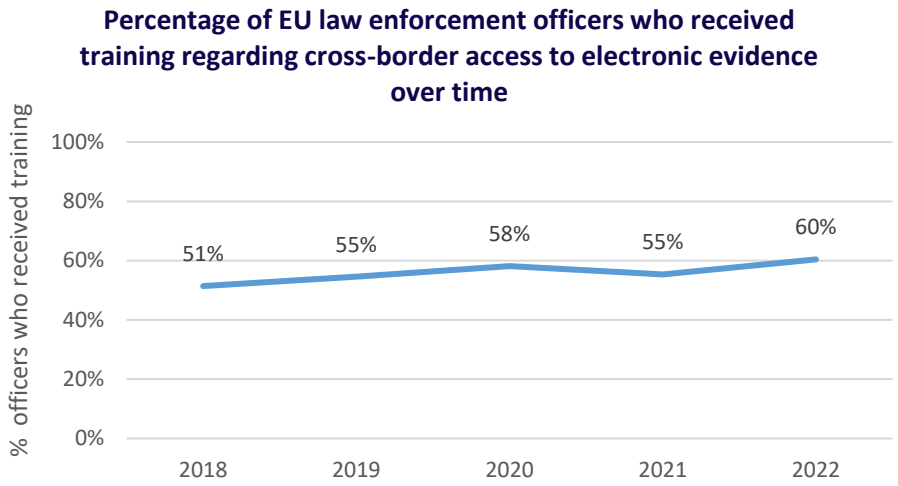
When dealing with requests for data disclosure to service providers, law enforcement officers must evidently ensure compliance with their own domestic regulation. However, there is also an additional layer of complexity, as they must also take into consideration international legislation and law of the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

In spite of the complex landscape in which they currently operate, 74% of EU law enforcement officers reported being satisfied, very satisfied or extremely satisfied with their department's engagement with foreign-based service providers in 2022. The satisfaction rate of 2022 even saw a 4% increase in comparison with the results for 2021, as published in the previous edition of the SIRIUS Report[20].

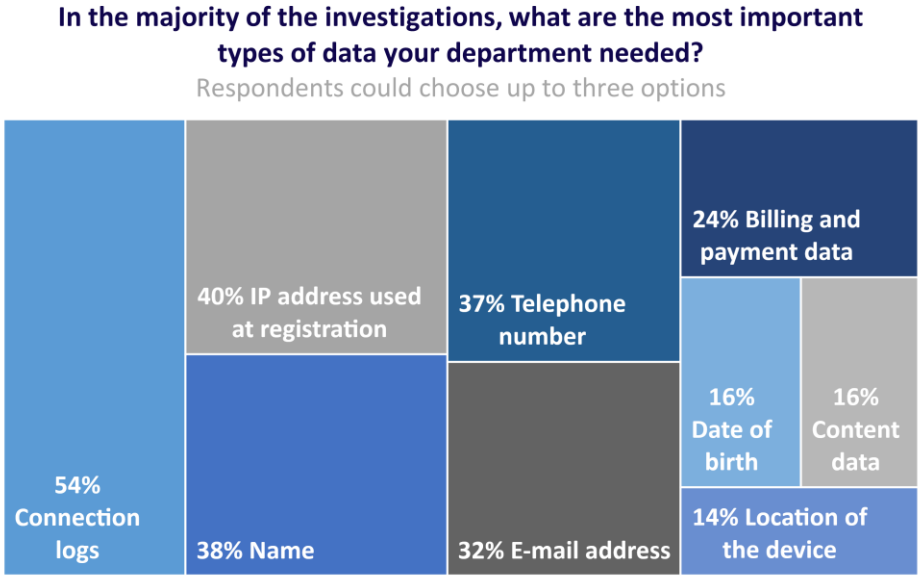


In 2022, the majority of EU law enforcement officers (60%) reported that they have received some training regarding cross-border access to electronic evidence. This year's result is the best ever recorded since the first edition of the SIRIUS Report. It represents a considerable improvement in comparison with 2018, when only 51% of officers reported having received some training on this matter.





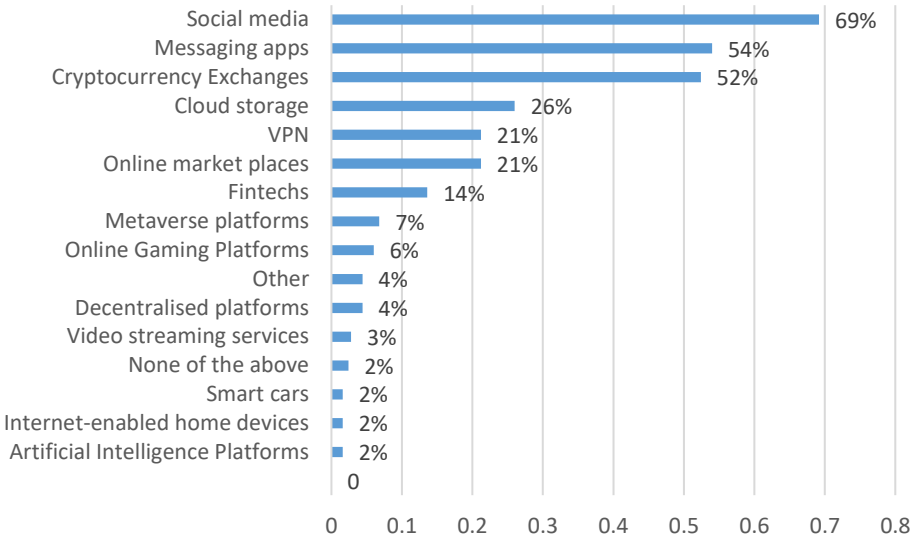
Data disclosure requests in the context of criminal investigations must always be very specific in relation to the persons they are aimed at, as they are somehow involved in the case under investigation (e.g. suspect of a crime). Additionally, requests must abide by the principles of necessity and proportionality by specifying the datasets sought, and the precise timeframe relevant for the investigation. In 2022, officers found that the three most important datasets for criminal investigations were connection logs (date, time and IP address of connection to an online service), IP address used at the moment of first registration to the service, and the name of the user; the exact same datasets as in the previous year. It is worth noting that only 16% of officers considered that content data was among the three most important types of data needed in investigations.



Providers of many different types of services can be deemed relevant by law enforcement for their investigations. In 2022, the five most important types of service providers were: social media platforms, messaging apps, cryptocurrency exchanges, cloud storage and VPN.

Which types of online services were most relevant for the criminal investigations conducted by your department in 2022?

Respondents could choose up to five options



Providers of services such as artificial intelligence (AI) platforms, internet-enabled home devices, smart cars and *metaverse* platforms did not figure among the most important ones in criminal investigations carried out in 2022. However, the law enforcement community observed ongoing developments in these areas with great interest. On the one hand, many officers noted the opportunities new technologies could bring to their daily work to ensure the security of fellow citizens. For instance, officers mentioned that AI could facilitate their work, and lead to more effective and accurate investigations. On the other hand, officers also voiced their concerns over the challenges that could result from implementing such technologies, in the near future. For example, there is a lot of concern in relation to the use of "deep fakes" for criminal purposes, and the potential increase in the volume and complexity of data. Some of the comments provided by officers in this regard are listed below[21]:

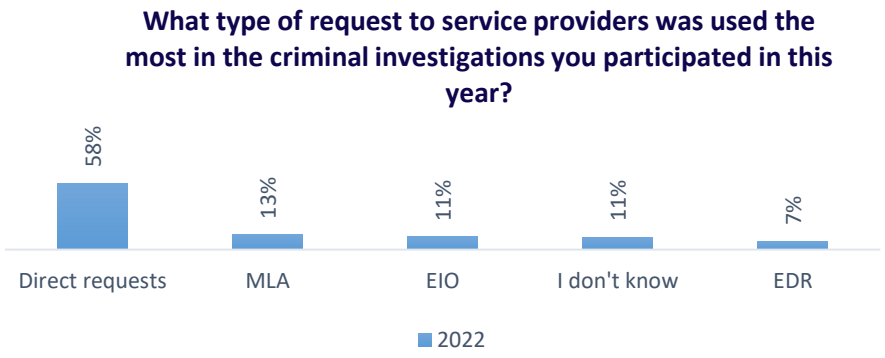
> *"AI will transform everything. Malicious use of AI will make our investigations far more difficult. Long responses were our main problem, now obfuscation techniques will create unique modus operandi (by using AI), and, in my opinion, will make our investigations extremely difficult. Traces of criminals could become more misleading than ever."*
>
> *"Our work will become more and more complex because the volume of data we will need to retrieve and examine will exponentially increase. The future will be for sure challenging, solving crime using electronic evidence will be even more complex."*
>
> *"There will be great challenges for the justice system when trying to identify suspects who commit crimes. Today it is possible to change the face of a person in a picture or video. As technology continues to improve, it will require more of both police and prosecutors to follow developments. Courts will also question the evidence presented by the prosecution more often."*
>
> *"AI could overtake repetitive workload from law enforcement colleagues, so there is more time to do other tasks."*
>
> *"AI-based investigative tools provide the means to simultaneously process multiple sources and cases, structured and unstructured. Therefore, there is potential to produce unseen connections and patterns, as well as to greatly reduce time consuming tasks that are not cost-effective when performed by human hands."*
>
> *"I think AI will have great impact on the work of law enforcement. Large language models can already help us in their current state. They are likely to improve a lot in the*

upcoming future. AI is likely to improve our work soon for automation of monitoring online sources and finding new information."

Submission of cross-border requests

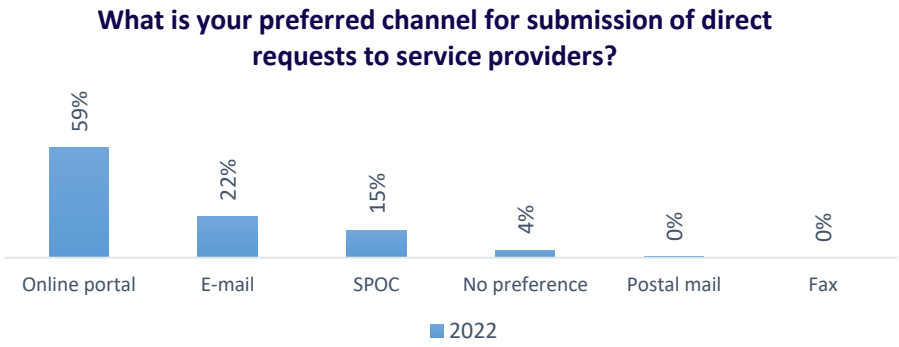
As previously mentioned, direct requests for voluntary cooperation to service providers for disclosure of non-content data have become quite common, compared to other means of obtaining data. Like in previous years, the majority of officers (58%) reported that direct requests were the most used type of requests to service providers in criminal investigations they participated in, in 2022.

When direct requests are not possible, officers must work together with judicial authorities to obtain the necessary data to continue their investigations via MLA or EIOs. It is important to note that the use of international judicial cooperation is a requirement in some countries to ensure that data is admissible as evidence (as described in the chapter Perspective of Judicial Authorities). Additionally, there are many service providers that refuse to cooperate with foreign authorities on a voluntary basis, or that are unable to do so in accordance with domestic regulations. Emergency Disclosure Requests (direct requests for voluntary cooperation in emergency circumstances, usually those involving an imminent threat to life), were considered to be the most important type of request by 7% of officers in 2022.

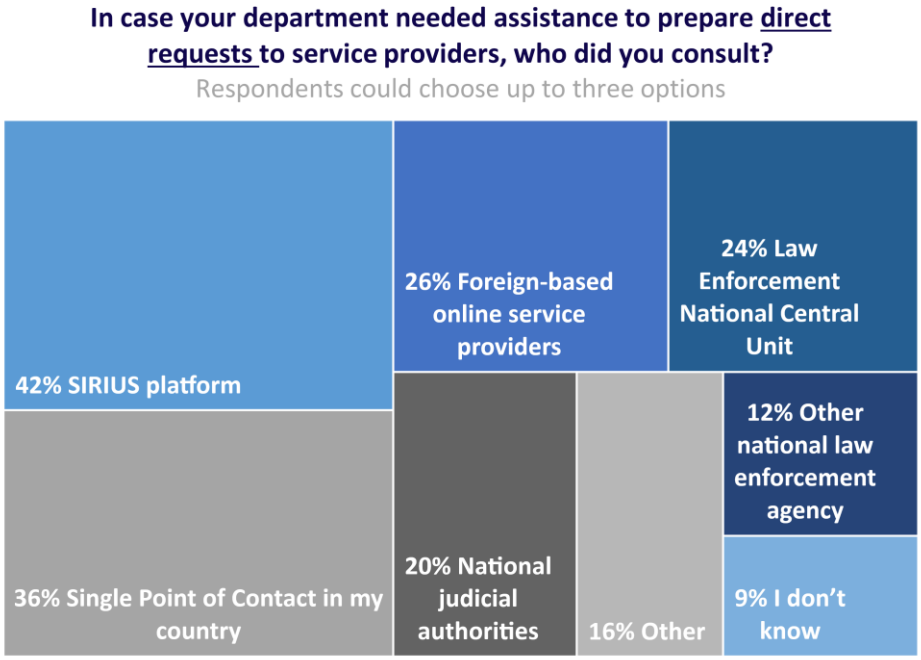


Because direct requests are considered voluntary cooperation, service providers may set up their own rules and requirements for competent authorities to adhere to. The channel for submitting requests is one such requirement that varies among service providers. Some of them choose to create dedicated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

The majority of officers (59%) prefer to submit their requests via online portals, rather than via e-mail. The benefits of using these portals often include the possibility to consult the status of each request, securely download responses, and streamline the communication between competent authorities and representatives of the service providers. The results relating to the preferred channels for submission of direct requests in 2022 are very similar to the results from the previous year, demonstrating stability in law enforcement preferences in this regard.



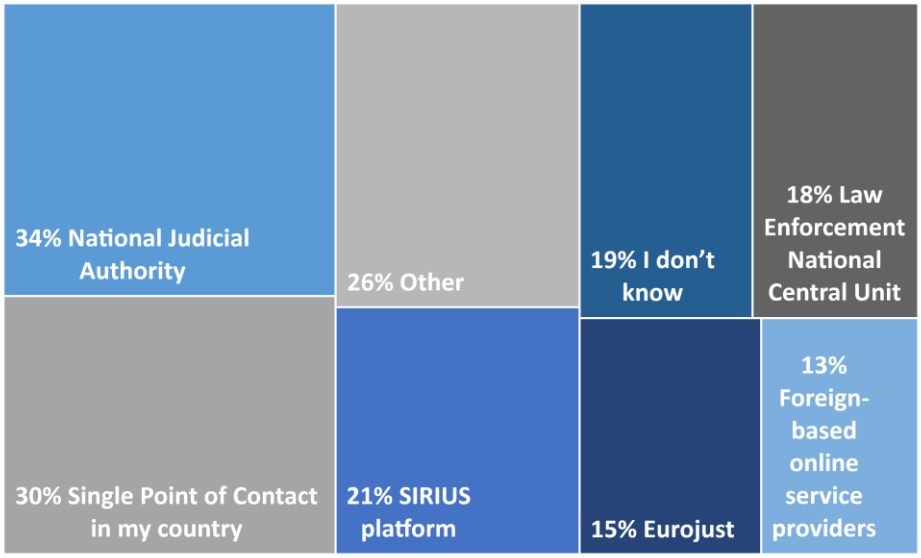
The SIRIUS Platform for knowledge-sharing (restricted to law enforcement and judicial authorities) remains the first ranked source of information in 2022 for law enforcement officers who need assistance to prepare direct requests. The SIRIUS Platform is followed by Single Points of Contact (SPoCs)[22] and the service providers themselves.



When it comes to assistance relating to MLA, the national judicial authorities remain the most consulted by law enforcement, followed by SPoCs. In this case, SIRIUS was mentioned as a source of information by 21% of respondents in 2022.

In case your department needed assistance to prepare Mutual Legal Assistance requests, who did you consult?

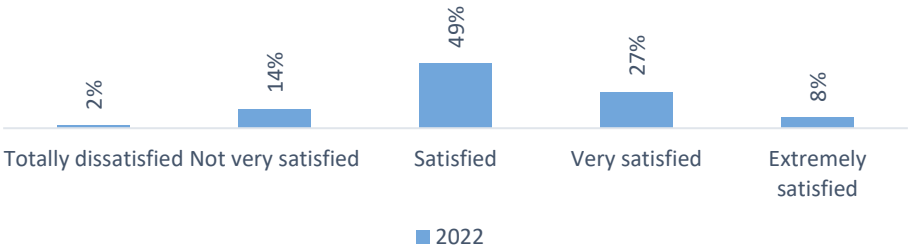
Respondents could choose up to three options



Among the law enforcement agencies where SPoCs have been established, three quarters of officers are satisfied or more than satisfied with their processes. SPoCs are defined as designated persons or units within the competent authorities of a respective country that streamline and channel cross-border data disclosure requests under voluntary cooperation to one or more foreign-based service providers in a centralised manner. Some of the benefits of SPoCs are:

- The establishment of a SPoC process contributes to increased quality of requests. Consequently, it leads to a decrease in response time because officers, who are part of SPoCs, are specialised in electronic evidence. They have, for example, a very good understanding of the applicable requirements, the type of information that must be included in requests and the datasets that can be requested from each service provider;
- SPoCs make it possible to establish streamlined communication in emergency circumstances, ensuring faster processing of information;
- Updates, feedback and training material can be disseminated through a single channel, and questions from the different units can be centralised and routed through the SPoC. This ensures that all law enforcement officers in that agency benefit from the provided information;
- Establishing SPoCs helps minimise duplication of requests regarding the same case from different units or even law enforcement agencies;
- SPoCs are efficient tools to build greater cooperation between service providers and law enforcement agencies.

If a Single Point of Contact has been established to channel requests to Service providers, how satisfied are you with the process?

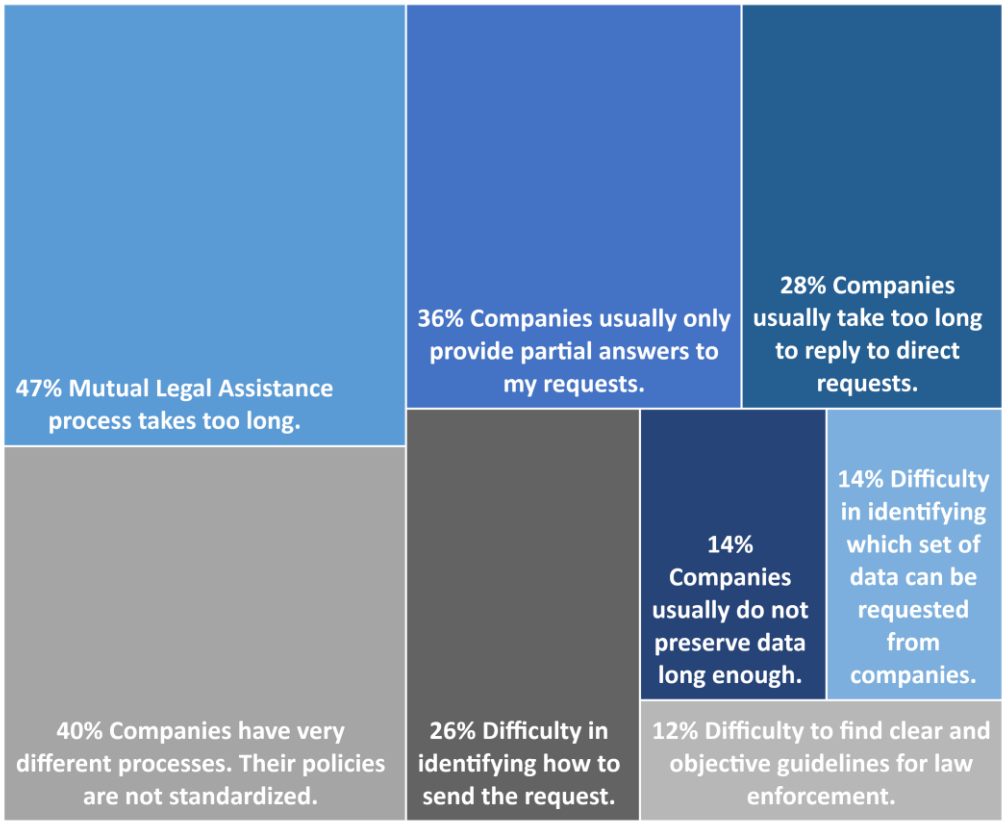


To date, in the EU, 28 law enforcement agencies in 21 EU Member States have established units to act as a SPoC: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Italy, Ireland, Latvia, Lithuania, Malta, Netherlands, Slovenia, Spain and Sweden.

The use of the 24/7 Network established under the Council of Europe Convention on Cybercrime (Budapest Convention) remained stable in 2022 compared to previous years, with one third of officers reporting their department submitted disclosure or preservation requests via this Network. The percentage of officers who do not know whether or not the Network has been used by their department remains remarkably high, at 40%.

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

Respondents could choose up to three options



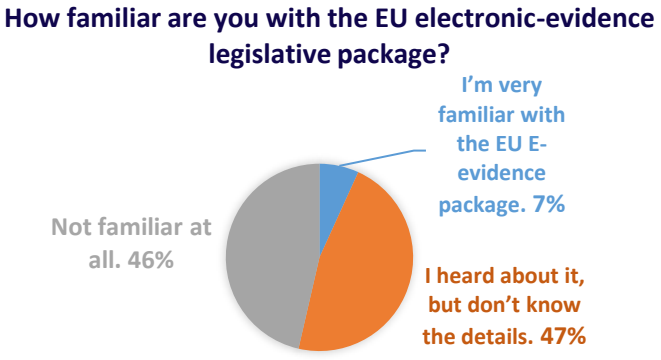
Other issues that were mentioned by less than 10% of officers included:

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

EU Electronic Evidence legislative package

The new EU Electronic Evidence legislative package will introduce new instruments for authorities to request data disclosure from foreign-based service providers. Predictably, the new policy will change the international panorama for access to electronic evidence across borders, as many service providers could introduce changes to their processes, affecting the current practice of accepting direct requests under voluntary cooperation, for example.

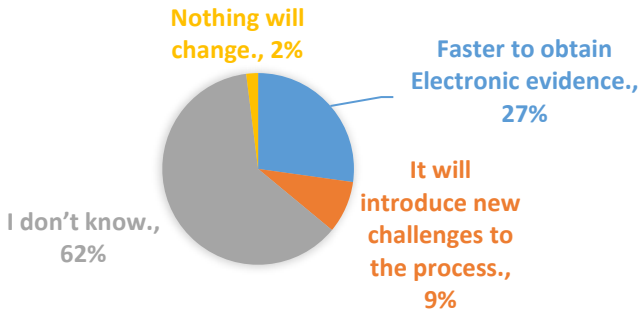
The new rules will have profound implications for the electronic evidence retrieval process. At the moment, only 7% of law enforcement officers reported being very knowledgeable about the legislative package (as of May 2023 when the survey with law enforcement was conducted for this report – which is not surprising, given that the EU Electronic Evidence legislative package was only adopted and published in July 2023). In fact, 47% of officers do not know the details of the new rules yet, while 46% are not (yet) familiar with it at all. For instance, some officers indicated that it is still not clear to them whether or not law enforcement agencies in their country will be in a position to act as an issuing authority for European Production Orders as defined in Article 4(1)(b), 4(2)(b) and 4(3)(b) of the Electronic Evidence Regulation.



Among the officers who have heard about the EU Electronic Evidence legislative package, or those that are very familiar with it, only about one third are positive about the effect it may have. These officers believe it will certainly be faster to obtain electronic evidence from service providers. However, 9% believe there will be additional

challenges to the process, whereas the majority (62%) is still unsure about the effects the new policy will have on their work.

How do you think the EU electronic-evidence package will affect your work, once it comes into force?



Among officers who reported that it will certainly be **faster to obtain electronic evidence** from service providers, the following comments were submitted[23]:

> *"The new legislative efforts will greatly speed up procedures that are currently too time-consuming, and significantly speed up the acquisition of electronic evidence, bypassing existing problems posed by the different legislative system of each EU Member State."*

> *"I think that the direct requests and mandatory quick responses will be game changing. Faster responses lead to faster investigation and better ways to trace criminals."*

> *"The process will be accelerated as a single framework will be established, not depending anymore on the policy of each private company. Undoubtedly, this will facilitate the work of law enforcement authorities, which will be able to set a specific time horizon for the completion of their investigative actions."*

> *"Standardising the forms for submission of data requests to service providers in the EU will make our work much easier and more efficient."*

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

> *"What will happen with direct requests for voluntary cooperation issued by law enforcement authorities if all European Production Orders must be processed by the judicial authority?"*

> *"The success of the new policy will depend on whether today's process under voluntary cooperation will continue to work. If not, my work will be more challenging."*

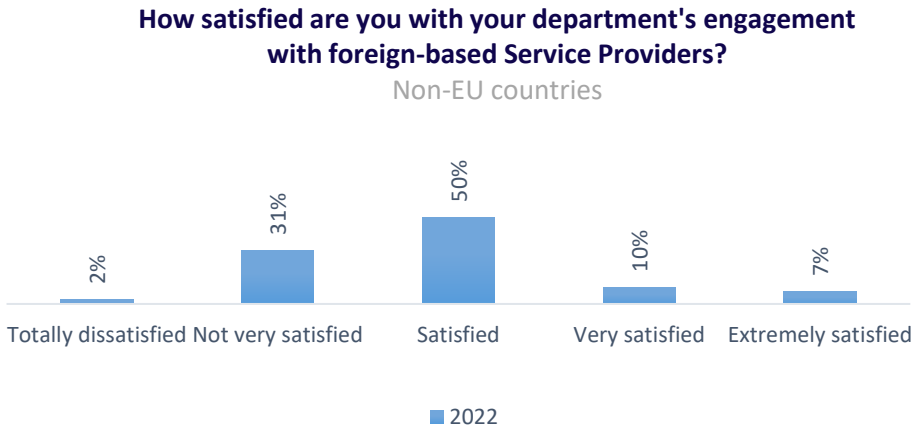
> *"It will potentially be faster to obtain electronic evidence in criminal investigations with the new EU Electronic evidence policy. However, the practical process and compliance is unclear."*

> *"We will surely need to get training on this new process for submission of data disclosure requests."*

Electronic evidence for law enforcement in non-EU countries

Law enforcement authorities from countries outside of the EU, with which Europol has operational or working agreements, were invited to reply to the same survey used to collect feedback from EU officers. From Albania, Bosnia and Herzegovina, Canada, Colombia, Iceland, Japan, Moldova, New Zealand, Norway, Serbia, Switzerland and United Kingdom, 42 responses were received.

In 2022, 67% of officers from non-EU countries reported being satisfied or more than satisfied with their department's engagement with service providers, compared to 74% in the EU.



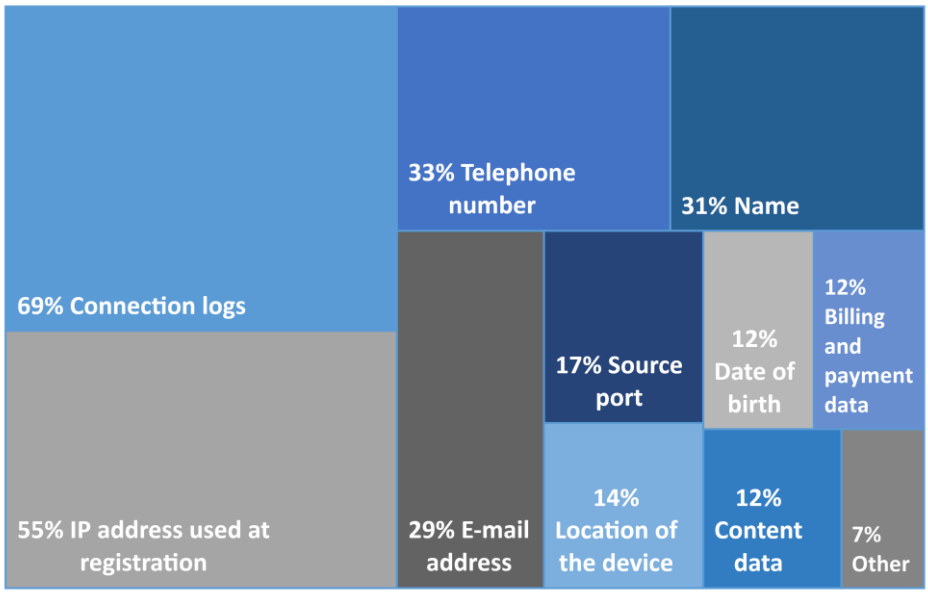
Direct requests for disclosure of data under voluntary cooperation is the most important type of request for respondents from non-EU countries, even more than in the EU (69% in non-EU countries, and 58% in the EU).

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) and the IP address used at the moment of first registration to the service and phone number, appear as the most important datasets for criminal investigations. It is worth noting that content data has been indicated by 12% of respondents as one of the most important types of data in criminal investigations in non-EU countries (which is similar to the result in the case of EU countries, 16%).

In the majority of the investigations, what are the most important types of data your department needed?

Non-EU Countries

Respondents could choose up to three options



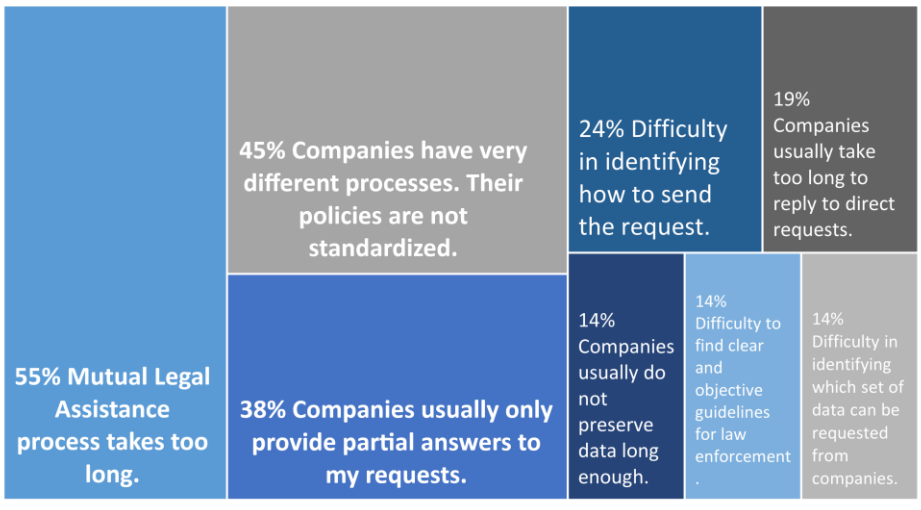
The three main issues encountered by non-EU law enforcement officers when submitting requests to foreign-based service providers in 2022 were exactly the same as in the EU. The main issue is that the MLA process takes too long, followed by the fact that service providers' policies are not standardised. The third issue mentioned the most by officers refers to receiving only partial answers to their requests.

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

What are the main issues your department encountered in requests to foreign-based Service Providers?

Non-EU Countries

Respondents could choose up to three options



PERSPECTIVE OF JUDICIAL AUTHORITIES

Legal framework and developments

Using judicial cooperation channels to obtain data from providers located in a foreign jurisdiction often takes too long, which can lead to the loss of data. In order to facilitate and accelerate the process of obtaining data directly from service providers, EU Member States have been increasingly using voluntary direct cooperation channels, applying different national tools, conditions and procedures in the process. This has led to a rather fragmented legal framework and to additional challenges for law enforcement and judicial authorities as well as service providers on the receiving end of data disclosure requests (e.g. legal uncertainty, conflicts of law and jurisdiction).

The Digital Services Act[24] (DSA) addresses part of these concerns related to the lack of harmonisation of the rules surrounding cross-border orders for data disclosure directed at service providers. It puts in place common rules on the content and format of orders for information (minimum conditions that such orders must meet) issued directly to service providers and lays down rules on complementary requirements relating to the processing of such orders[25].

Recent legal developments will bring more ground-breaking changes in the process of cross-border gathering of electronic evidence. The new legal powers created by the Second Additional Protocol, and especially the EU Electronic Evidence legislative package, will enable competent authorities to order the preservation and the production of electronic evidence directly from service providers located abroad. The unprecedented procedures envisaged by this legislation are intended to work faster and in a more flexible way than the existing judicial cooperation instruments for the gathering of electronic evidence (i.e. EIO and MLA processes). They will also bring legal clarity in the process of cross-border gathering of electronic evidence, dispelling ambiguities, especially those surrounding voluntary direct cooperation channels, for both:

- Service providers who have to find a way to reconcile their willingness to cooperate with authorities in criminal investigations and proceedings with the need to comply with strict privacy and data protection requirements (e.g. establishing a legal basis for cooperation with the authorities under Article 6 of the GDPR[26]); and

- Law enforcement and judicial authorities, who are dealing with legal ambiguity as to whether direct cooperation with service providers is allowed (as the matter is rarely specifically regulated in national legal frameworks) and questions of admissibility as evidence in court of any data so obtained, in addition to challenges relating to the different requirements imposed by different the service providers, the uncertainty whether the service provider will comply with a request for data, the lack of timely responses in emergency cases, etc.

At the same time, these new legal instruments, while changing the legal landscape in the field of cross-border access to electronic evidence, still fall under the scope of judicial (mandatory) cooperation. Consequently, voluntary cooperation channels for the gathering of electronic evidence might become largely redundant for the competent

authorities or even abandoned by certain service providers (outside emergency circumstances)[27].

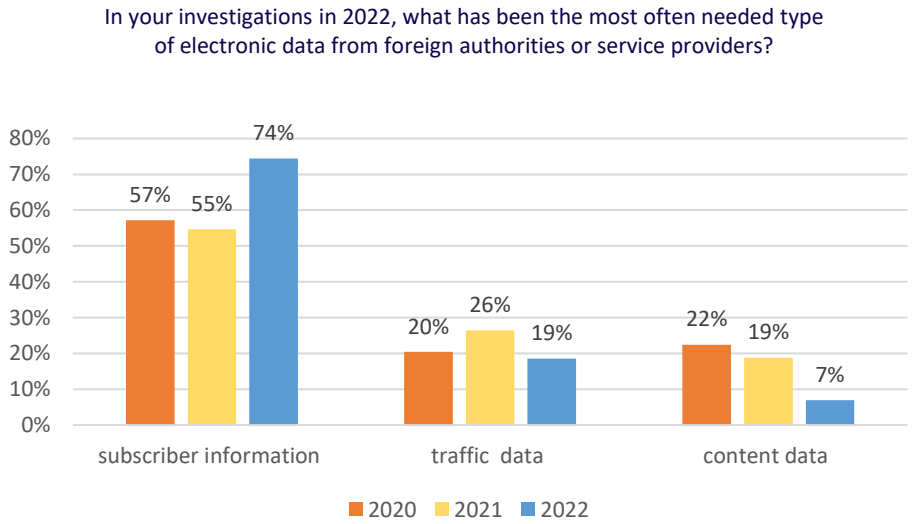
Acquisition of electronic evidence across borders and challenges encountered

Types of data requested

EU judicial practitioners were invited to share what type of electronic data they have requested most often from foreign authorities or service providers based in other countries in their criminal investigations and proceedings in 2022[28].

The information obtained from the surveyed EU judicial authorities shows that requests for data disclosure take place in a cascading manner, starting from the least restricted – namely requests for subscriber information, which is needed in the majority of cases – to requests for data requiring the highest level of procedural protection, namely content data, for which most often an MLA/EIO process would be required.

Subscriber information – such as name, postal or geographic address, billing and payment data, e-mail address or telephone number of a subscriber – was the most sought electronic data from foreign authorities or foreign-based service providers in criminal investigations and proceedings carried out in 2022 (74%). The leading position of this data category remained unchanged compared to 2021 (55%) and 2020 (57%)[29], indicating that gathering subscriber information is often the first step in criminal investigations involving electronic evidence. Cases are then further constructed by adding the necessary traffic data (e.g. source and destination of a message, location of the device, date, time, duration, size, route, format, protocol used) and content data (e.g. text, voice, videos, images, sound).

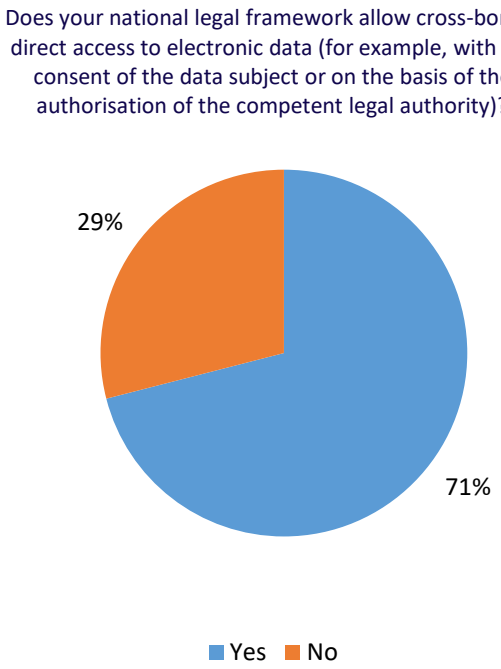


Direct Access

Direct access to electronic data refers to the process of obtaining such data without relying on the involvement of the service provider in possession or control of it.

Within the Budapest Convention, Article 32(b) establishes a provision enabling authorities in one Party to unilaterally access computer data stored in another Party to the Convention, provided the person lawfully authorised to disclose the data gives their consent. Provided that the required national legal framework is in place, such direct access constitutes a rather unproblematic, as well as fast way of accessing data which may be stored in another country, as it does not require any kind of interaction with or response from a foreign authority or foreign-based service provider.

With regard to the availability of this measure in the national procedural laws of the surveyed EU Member States, the results reveal that 71% (17 out of 24 surveyed) have incorporated this measure into their national legislation.



Some respondents from EU Member States whose legal frameworks permit such cross-border direct access to data provided supplementary details, outlined in **Table 1**[30].

TABLE 1 – EU MEMBER STATES WHERE CROSS-BORDER DIRECT ACCESS TO DATA WITH THE CONSENT OF THE PERSON LAWFULLY AUTHORISED TO DISCLOSE THE DATA IS ALLOWED	
Czechia	*According to section 89, paragraph 2, of the Code of Criminal Procedure (Act No. 141/1961 Coll.), everything that may contribute to the clarification of the case, in particular statements of the accused and witnesses, expert reports, objects and documents relevant to the criminal proceedings and examinations, may serve as evidence. Evidence may be sought, produced or proposed by either party. The fact that evidence has not been sought or requested by the prosecuting authority shall not be a ground for refusing such evidence.*
Greece	*When consent is present, it is considered in practice that there are no legal impediments to access data located abroad, after a request is made to the service provider who possesses it.*
Hungary	*In some circumstances, even defendants agree to voluntarily provide access to their data based on Budapest Convention Article 32(b). Goes smoothly and effectively. Especially in drug smuggling cases.*
Ireland	*There is nothing in the legislation to prevent cross-border data sharing provided the consent is full and freely given by the data subject […], provided that there is no other legal impediment to such data sharing.* *However, the answer to this question depends on the data […] and the status of the data subject. If the data subject is a suspect in a criminal investigation, consent may not provide a legal basis for [access to data].*
Ireland	*Access to data held abroad must be by consent or lawful order or a court order to search which includes accessing data held online and accessible at the time and location of the search. Various warrants exist, e.g. s7 Child Trafficking & Pornography Act 1998, s48 Criminal Justice (Theft & Fraud Offences) Act 2001.*
Slovakia	*Strictly within the meaning of Article 32(b) of the Budapest Convention on Cybercrime and within the meaning of the TC-Y Guidance Note on this issue.*
Sweden	*It was previously allowed only in Article 32(b) cases. But a new ruling from the Supreme Court issued on 30 March 2023 allows law enforcement to access data regardless where it is stored. As long as it can be done through authentication (i.e. login with username and password) the data can be obtained and used in court.*

Direct voluntary cooperation with service providers located abroad

National legal frameworks regarding direct requests for data

Direct requests for data are requests submitted by competent authorities directly to foreign-based service providers for the preservation and/or production of non-content data under voluntary cooperation. Such requests are not legally binding. Thus, they are dependent on the willingness of service providers to cooperate with public authorities, their internal policies, as well as the domestic legislation of both the place where the requesting authority is based and the place where the requested service provider is based. In practice, this means that different conditions and procedures apply to the issuance of such requests.

The results of the survey show that the national legislation of the majority of the EU Member States surveyed, 74% (17 out of 23 surveyed)[31], allows collecting electronic data via voluntary cooperation by directly addressing service providers located abroad. However, the findings also indicate that even if direct voluntary cooperation with private entities situated abroad is perceived as possible in a majority of the EU Member States, the competent authorities' interpretation as regards the availability of this measure may vary due to the lack of explicit regulation.

Some respondents from EU Member States whose legal frameworks permit competent authorities to obtain electronic data via cross-border voluntary cooperation by directly addressing service providers located abroad provided additional information, outlined in **Table 2**.

TABLE 2 – EU MEMBER STATES WHERE DIRECT VOLUNTARY COOPERATION WITH FOREIGN BASED SERVICE PROVIDERS IS ALLOWED	
Bulgaria	*In accordance with Article 159 and 159a of the Code of Criminal Procedure of the Republic of Bulgaria:* *Article 159* *(Re-designated from Article 159, SG No. 32/2010, effective 28.05.2010, amended, SG No. 24/2015, effective 31.03.2015)* *Upon request of the court or the pre-trial authorities, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerised data and other data, that may be of significance to the case.* *[…]* *Article 159a (New, SG No. 24/2015, effective 31.03.2015)* *(1) Upon request by a court as part of court proceedings or based on motivated order by a judge of the respective court of first instance, issued by request of the supervising prosecutor of pre-trial proceedings the enterprises, providing public electronic communication networks and/or services shall make available the data, generated in the course of performance of their activities, which may be required for:* *1. tracing and identification of the source of the communication link;* *2. identification of the direction of the communication link;* *3. identification of the date, hour and duration of the communication link;* *[…]* *Since the Bulgarian Code of Criminal Procedure does not limit the application of the above provisions only to addressees in Bulgaria, the possibility of obtaining electronic data from service providers located abroad exists.*
Lithuania	*[…] Only subscription and traffic data can be obtained directly. For content data, a request for legal assistance must in all cases be made to the competent authorities of the foreign country. When contacting directly service providers registered and operating in foreign countries for subscription and traffic data, the prosecutor's access to information order, approved by the pre-trial judge in accordance with the procedure laid down in Article 155 of the Criminal Procedure Code, must be submitted, together with an English translation of the decision.*
Luxembourg	*In practice, we always file a national court order together with our request to the service providers. All data covered by the court order may then also be admitted as evidence in court.*
Romania	*Yes, [based on] Articles 152 & 170 Code of Criminal Procedure and Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector.*
Sweden	*Allowed if permitted in the other state (e.g. USA).*

Conversely, respondents from some EU Member States whose legal frameworks do not currently allow direct voluntary cooperation provided additional explanations, which can be found in **Table 3**.

TABLE 3 – EU MEMBER STATES WHERE DIRECT VOLUNTARY COOPERATION WITH FOREIGN-BASED SERVICE PROVIDERS IS NOT ALLOWED	
Croatia	*It is always on request by MLA.*
Malta	*[Voluntary cooperation is not allowed], subject to the legal framework (Data Protection Act, Chapter 586 of the laws of Malta and subject to its subsidiary legislation) that the Information and Data Protection Commissioners Office is subject to.*
Slovenia	*[No.] Exchange of evidence on a voluntary basis is not regulated in Slovenia. The formal-regulated way to obtain evidence from third countries is via diplomatic channels and via letter of request or EIO for EU, depending who and what we are asking.*
Greece	*There is no specific procedure in the national law for that, but in practice it is accepted to directly request data from service providers abroad, provided that all internal safeguards are complied with and that such access has been approved by the pre-trial council as the national law requires. The ratification of the 2nd Additional Protocol to the Budapest Convention is expected to introduce an explicit legal framework in this regard.*
Hungary	*There are no specific legal provisions in this context. It is not prohibited, but neither allowed.*
Ireland	*The legislation neither precludes it nor provides for it. As it is voluntary it is entirely a matter for the service provider, but in most cases the data is provided as intelligence […].*
Slovakia	*We do not have legislation concerning voluntary cooperation, so it is not clear if it is possible or not.*

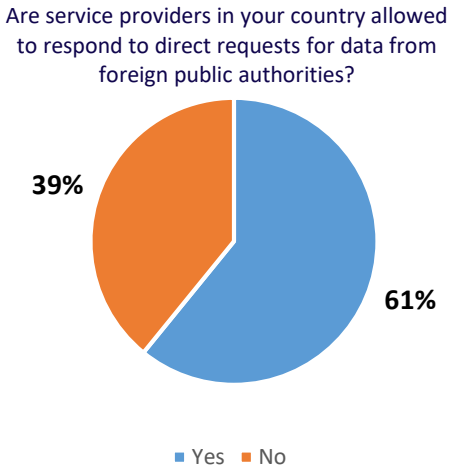
However, the regulation in national legislations of direct voluntary cooperation mechanisms is often far from being a clear-cut issue, leaving practitioners from some EU Member States in legal uncertainty. In this regard, some respondents indicated that their legal framework neither permits nor prohibits obtaining electronic data via direct voluntary cooperation mechanism, as further set out in **Table 4**.

TABLE 4 – EU MEMBER STATES WHERE DIRECT VOLUNTARY COOPERATION WITH FOREIGN-BASED SERVICE PROVIDERS IS NEITHER ALLOWED NOR PROHIBITED	
Greece	*There is no specific procedure in the national law for that, but in practice it is accepted to directly request data from service providers abroad, provided that all internal safeguards are complied with and that such access has been approved by the pre-trial council as the national law requires. The ratification of the 2nd Additional Protocol to the Budapest Convention is expected to introduce an explicit legal framework in this regard.*
Hungary	*There are no specific legal provisions in this context. It is not prohibited, but neither allowed.*
Ireland	*The legislation neither precludes it, nor provides for it. As it is voluntary it is entirely a matter for the service provider, but in most cases the data is provided as intelligence […].*
Slovakia	*We do not have legislation concerning voluntary cooperation, so it is not clear if it is possible or not.*

National legal framework — approach to service providers

In addition to the already complex matters related to the availability of direct voluntary cooperation mechanisms in the national legal frameworks, it is also important to assess the approach taken towards service providers in the applicable legal framework.

In this regard, judicial authorities were asked whether their respective national legal framework allows domestic private entities to respond to direct requests for data received from foreign public authorities. The results of the survey reveal that the legislation in more than half of the EU Member States surveyed allow domestic service providers to respond to such requests (14 out of 23 surveyed[32]).



Some respondents provided further considerations regarding their respective national legal frameworks and the applicable conditions, which may affect the possibility for domestic service providers to respond to direct requests for data under voluntary cooperation received from foreign public authorities, as outlined in **Table 5**. The provided considerations of EU judicial practitioners also indicate that their perception

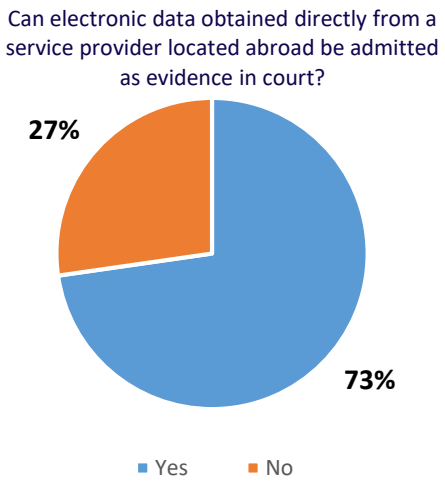
of the national legislation regarding this matter often varies due to the lack of explicit regulation.

TABLE 5 – EU MEMBER STATES WHERE DOMESTIC SERVICE PROVIDERS ARE CONSIDERED TO BE ALLOWED TO RESPOND TO DIRECT REQUESTS FOR DATA FROM FOREIGN PUBLIC AUTHORITIES	
Austria	*Yes, according to the standards of Directive 2016/679 of the European Parliament (27/4/2016).*
Bulgaria	*It is not explicitly prohibited by law, so it is allowed.*
Czechia	*Yes, and on a voluntary basis by national service providers with international law enforcement agencies which approach them directly, but only under certain conditions (for example, only in emergency circumstances).*
Hungary	*There is no specific legislation in this context, service providers may decide whether to comply based on their internal policy.*
Ireland	*The answer to this question depends entirely on the data being sought, for example a court order is likely to be required to obtain personal data. However, there is a vast range of information which may become evidence in a civil or criminal case, which is not private personal data and which may be provided voluntarily, should the service providers wish to do so.*
Malta	*The consistent advice given by the Information and Data Protection Commissioners Office to controllers established in Malta when receiving requests for information from foreign authorities is to demand the legal basis on the basis of which such requests are made.*
Netherlands	*This is only possible if there has been an EIO or MLA request in the past. For example in the case of a long investigation from [Country X] we made it possible that data ran directly from the service providers to [Country X]. As a judicial authority, we were involved in the matter but did not see the data before it went abroad.*
Sweden	*No positive or negative obligations exist apart from those following GDPR.*

Admissibility as evidence of data collected via direct voluntary cooperation

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 (73%) of the EU Member States surveyed (16 out of 22[33]), data gathered via direct voluntary cooperation can be admitted as evidence in court.



For some of the countries where such data can be admitted as evidence in court, further explanations were provided as set out in **Table 6.**

TABLE 6 – EU MEMBER STATES WHERE DATA OBTAINED VIA DIRECT VOLUNTARY COOPERATION CAN BE ADMITTED AS EVIDENCE IN COURT	
Bulgaria	*As long as the Court does not require the evidence in question to be obtained only via techniques for establishing evidence as prescribed under Article 136 of the Code of Criminal Procedure of the Republic of Bulgaria, then the applicable provision will be again Articles 159 and 159a of the Code of Criminal Procedure. The data collected through the application of the provisions of Articles 159 and 159a of the Code of Criminal Procedure could be admitted by the court only as written or physical evidence, depending on the carrier on which they are materialised.* *However, it should be noted that when it comes to traffic data, a court order is needed in order for the evidence to be admissible in court.* *It should be emphasised that the lack of explicit legal regulation of this issue leaves the possibility for different interpretations of the law by different judicial panels. However, as the admissibility as evidence of data directly obtained from a service provider located abroad is not explicitly prohibited by law, it is allowed.*
Czechia	*The admissibility of evidence is explained in Law on International Judicial Cooperation in Criminal Matters (Act No. 104/2013 Coll.), specifically in Article 42 (3) where it is stated that:* *(3) […] evidence provided by a foreign authority without a request for legal assistance may also be used in criminal proceedings in the Czech Republic.*
Hungary	*As far as information is relevant to the case, it can be used as evidence, except if such data was obtained directly in breach of specific legal provisions (e.g. torture, coercion, etc.). If it is not directly forbidden, it is considered to be allowed.*
Lithuania	*Only subscription and traffic data can be obtained directly. For content data, a request for legal assistance must in all cases be made to the competent authorities of the foreign country. […] Only data obtained by lawful means and verifiable by the procedural steps provided for in the Criminal Procedure Code (CPC) may be accepted as evidence by the court (Article 20(4) of the CPC).*

In some EU Member States, electronic data collected directly from a service provider situated abroad via a direct request under voluntary cooperation can only be used for intelligence purposes and/or as a steering point in criminal investigations.

However, in some instances there is no clear-cut way of deciding whether electronic data collected via direct voluntary cooperation can be admissible as evidence in the national courts. Such considerations are well reflected in the additional explanation received from the Irish survey respondent:

- The answer depends on the type of data under request, the purpose of the data, the type of case in which the data is being produced and the context of the case. For example, different considerations apply to private personal data than apply to public data or company data. Subject to all of these variables, obtaining the data by way of mutual assistance may be required (Ireland).

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

Even though the mechanism of direct voluntary cooperation is often perceived as the fastest channel for competent authorities to obtain non-content data, it is also not void of its 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.

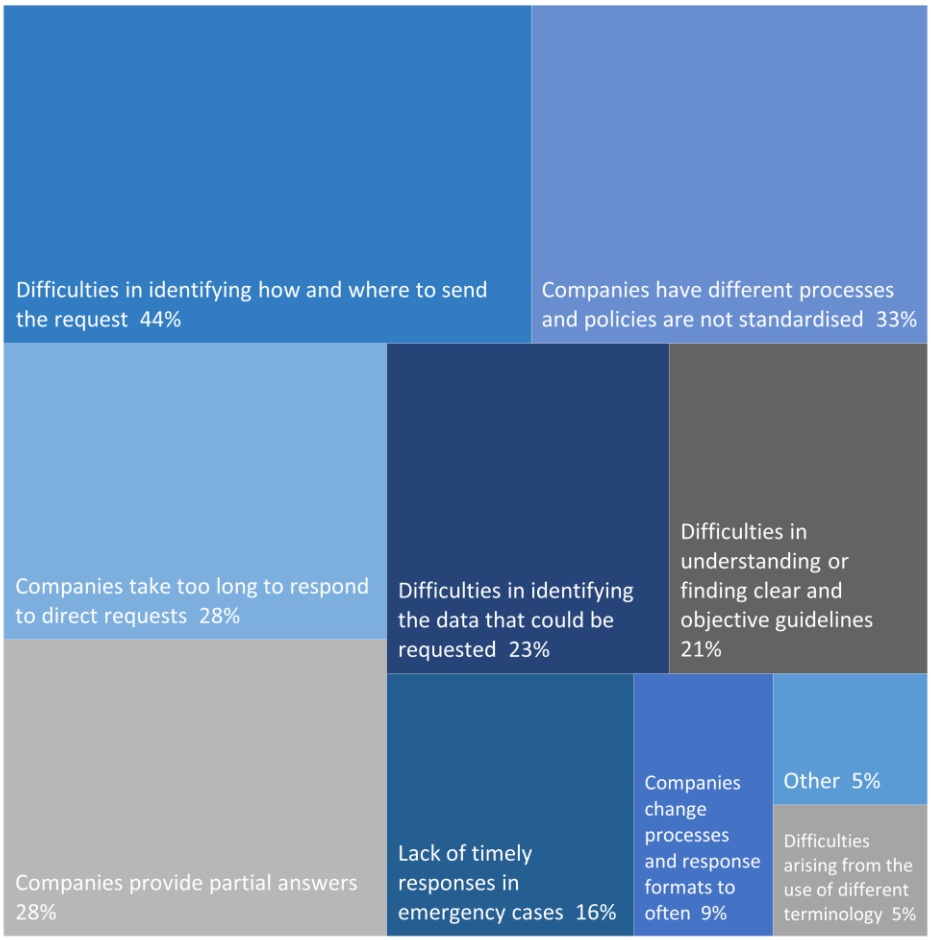
The collected responses reveal that the predominant issue for most respondents were data retention related challenges[34] (pinpointed by 47% of the respondents) in 2022. This comes with no surprise, as data retention related issues were emphasised as a prevalent challenge faced by EU judicial authorities also under other types of cooperation, including judicial cooperation.

The second most prevalent challenge indicated by the EU judiciary were difficulties in identifying how and where to send the request, particularly referring to the identification of the location where a service provider or the legal entity responsible for cooperation with public authorities on a voluntary basis is established (selected by 44% of the respondents). Issues related to different processes and policies applied by service providers were identified as the third most prominent problem in investigations carried out in 2022 (33% of the respondents). Other issues identified are the fact that companies usually only provide partial answers (28%) and that they take excessive time to respond (28%).

Additional problems reported with a lower prevalence were:

- Difficulties in identifying the data that could be requested: 23%;
- Difficulties in understanding or finding clear and objective guidelines provided by companies: 21%;
- Lack of timely responses in emergency cases: 16%;
- Companies change processes and response formats too often: 9%;
- Difficulties arising from the different terminology used by the different companies and the authorities defining the data types: 5%;
- Other: 5%.

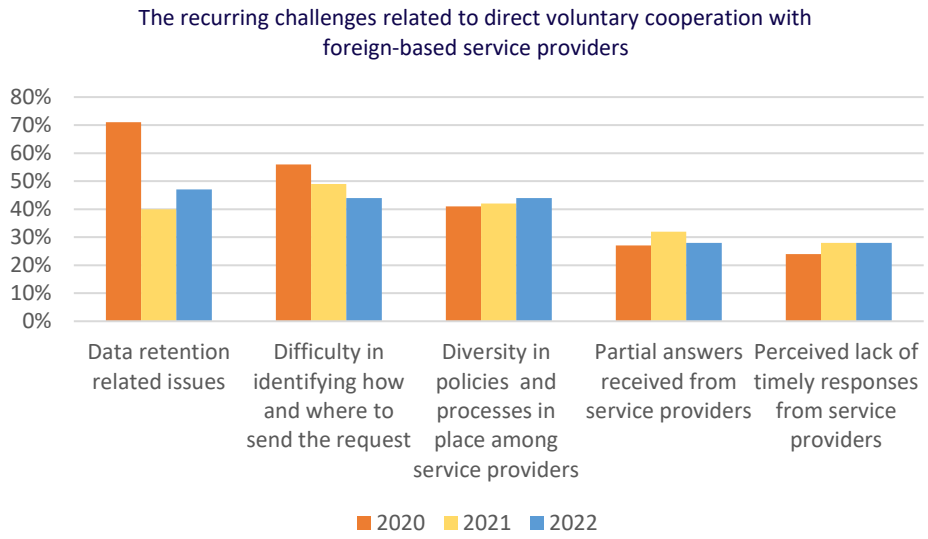
In your experience, what have been in 2022 the three main problems when contacting service providers located abroad with requests for data?



Placing the collected data into the perspective of the results included in previous SIRIUS EU Digital Evidence Situation Reports[35], the most pressing issues faced by judicial authorities when reaching out to service providers located in other jurisdictions with requests for data under voluntary cooperation remain unchanged. Comparing the information collected in recent years, a clear tendency of recurring issues is emerging.

While carrying different weights, the recurring challenges related to direct voluntary cooperation with foreign-based service providers polling highest in recent years refer to:

- Data retention related issues;
- Difficulties in identifying how and where to send the request;
- Diversity in policies and processes in place among service providers;
- Partial answers received from service providers; and
- Perceived lack of timely responses from service providers.



In addition to the above-mentioned trends regarding the main problems encountered by EU judiciary when opting for direct requests for data under voluntary cooperation, an additional consideration provided by a respondent from the Slovakia brought the issue back to its roots:

- [There is] no legal framework for direct voluntary cooperation. (Slovakia)

The fragmented legal framework, as well as the lack of enforceability of direct requests under voluntary cooperation, create additional challenges. Moreover, there is lack of clarity for public authorities as well as for service providers, which are faced with legal uncertainty and, potentially, conflicts of law. In this respect, it is expected that the new rules on cross-border judicial cooperation for preserving and producing electronic evidence set out in the EU Electronic Evidence legislative package will provide a solution to these and some of the other above-mentioned problems pinpointed by EU judicial practitioners in recent years. For example, the rules set out in the EU Electronic Evidence legislative package will include an obligation for service providers falling under the scope of this new legal framework to designate a legal representative in the EU for the enforcement of orders. Furthermore, a "contact book" with the contact details of service providers will be publicly available on a dedicated page of the EJN. Combined with clear communication channels established between competent authorities and service providers (via a dedicated decentralised IT system), this will help address the issue of identifying how and where to send requests for data.

Requests for data in emergency circumstances

The definition of "emergency circumstances" varies from country to country. In this regard, EU judicial practitioners were asked how "emergency circumstances" in the context of access to data held by service providers are defined in the legal framework of their respective countries.

The explanations received indicate that under the respective national legal frameworks, emergency disclosure procedures most often apply in case of the existence of an imminent danger to the life, health or freedom of a person; a dangerous attack; a terrorist threat; or a threat to the security of the State (see **Figure 1** below).

Considering future legal and policy developments, definitions of “emergency” refer to:

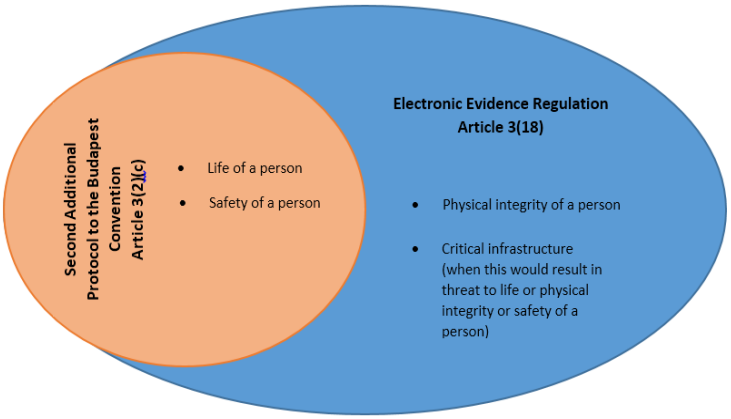
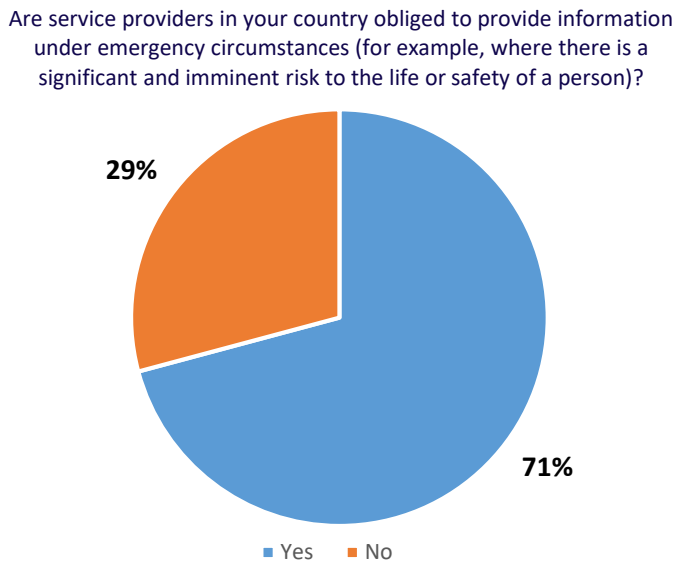


Figure 1 - Definition of “emergency” in accordance with the Electronic Evidence Regulation and the Second Additional Protocol to the Budapest Convention

Accordingly, the Electronic Evidence Regulation refers to situations in which there is an imminent threat to the life, physical integrity or safety of a person or to a critical infrastructure, where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State[36]. Similarly, though with a narrower scope, the Second Additional Protocol defines “emergency” as “a situation in which there is a significant and imminent risk to the life or safety of any natural person”[37].

Judicial authorities were also asked whether service providers, which provide services in their respective country, are obliged to provide information under emergency circumstances. The results of the survey show that a special regime for collecting information in emergency circumstances is available in the national legislation of the majority (71%) of the EU Member States surveyed (17 out of 24).



Some respondents from the EU Member States surveyed provided supplementary details on obtaining information under emergency circumstances, as outlined in **Table 7.** The additional explanations provided reveal that different legal provisions may apply to obtaining different types of data.

TABLE 7 – EU MEMBER STATES' LEGISLATION RELATED TO DATA DISCLOSURE REQUESTS UNDER EMERGENCY CIRCUMSTANCES	
Austria	*Paragraph 53 of the Austrian Security Police Law* *[…]* *(3a) The security authorities shall be entitled to demand information from operators of public telecommunications services [...] and other service providers […]:* *1. about the name, address and user number of a specific connection if this is necessary to fulfil the duties assigned to them under this federal law,* *2. about the Internet protocol address (IP address) for a specific message and the time of its transmission, if they consider this data to be essential for the defence against:* *a. a concrete danger to the life, health or freedom of a person within the scope of the first general duty to render assistance (Section 19),* *b. a dangerous attack (Section 16(1)(1)), or* *c. of a criminal connection (§ 16 par.1 line 2) need,* *3. About the name and address of a user to whom an IP address was assigned at a certain point in time, if they need this data as an essential prerequisite for the defence against:* *a. a concrete danger to the life, health or freedom of a person within the scope of the first general duty to render assistance (§19),* *b. a dangerous attack (§ 16 par. 1 fig. 1) or* *c. of a criminal connection (§ 16 para. 1 line 2) need,* *4. About the name, address and user number of a specific connection by referring to a call made from this connection by designating as precise a time period as possible and the passive subscriber number, if this is necessary to fulfil the first general duty to provide assistance or to defend against dangerous attacks.* *(3b) If, on the basis of certain facts, it can be assumed that there is a present danger to the life, health or freedom of a person, the security authorities shall be entitled, in order to render assistance or avert this danger, to demand from operators of public telecommunications services information on the location data and the international mobile subscriber identifier (IMSI) of the terminal device carried by the endangered person or by the person accompanying the endangered person, and to use technical means to locate the terminal device.* *(3c) In the cases referred to in paras. 3a and 3b, the security authority shall be responsible for the legal admissibility of the request for information. The requested body shall be obliged to provide the information without delay and, in the case of par. 3b, against reimbursement of costs in accordance with the Surveillance Costs Ordinance - ÜKVO, Federal Law Gazette II No. 322/2004. In the case of para. 3b, the safety authority shall also provide the operator with written documentation without delay, at the latest within 24 hours.*

Bulgaria	*Art. 251d of the Electronic Communications Act:* *(1) In cases of imminent danger of committing a crime under Art. 108a (1-4; 6; 7), Art. 109 (3), Art. 110, Art. 110 (1), alternative 6, Art 110 (2) (these are terrorism and crimes related to the national security), Art. 308 (3.1) (documentary offence, which facilitates any of the previously mentioned crimes) and Art. 320 (2) (public incitement to committing terrorism or a crime against the national security) the undertakings providing electronic communications networks and/or services shall provide instant access to […] traffic data based on the request of […] Police authorities, National security authorities, Military police, Military intelligence, State intelligence service, Fire safety and protection of the population authorities.[…]* *(2) The request […] shall absolutely contain:* *1. the legal basis for granting access;* *2. the data that should be reflected in the report;* *3. (amend. – SG, 20/21) a reasonable period of time, which should cover the reference;* *4. the designated official, to whom to provide the data.* *After the access is granted, the requesting authority should receive a court approval immediately after the traffic data is received. If the court refuses the access, the traffic data is immediately deleted.* *[…]*
Czechia	*[…] according to the Police Act of the Czech Republic (Act No. 273/2008 Coll.), specifically pursuant to Section 68 concerning the search for persons and things and Section 71 on the basis of a request from a police department whose task is to combat terrorism, in order to prevent and detect specific threats in the field of terrorism, it states, inter alia, the following;* *Section 68 (2) - For the purposes of an initiated search for a specific wanted or missing person and for the purpose of establishing the identity of a person of unknown identity or the identity of a found corpse, the police may request the provision of operational and location data from a legal or natural person providing a public communications network or providing a publicly available electronic communications service in a manner allowing remote and continuous access.* *Section 71 - A police unit tasked with combating terrorism may, to prevent and detect specific terrorist threats, request, to the extent necessary, from a) a legal or natural person providing a public communications network or providing a publicly available electronic communications service to provide operational and location data in a manner allowing remote and continuous access, unless another legal regulation provides otherwise; the information shall be provided in the form and to the extent provided by another legal regulation, (b) banks transmitting data on the time and place of use of the electronic means of payment, (c) a health insurer or health service provider providing information on the time and place of provision of health services.*

Germany	*The legal basis for official data disclosure requests derives from Sections 94, 98, 100g, 100j of the Code of Criminal Procedure. According to these provisions, the court and, under emergency circumstances, the prosecutor's office can order the disclosure of subscriber data, traffic data and content data.* *Requirements for information disclosure differ depending on whether or not the service provider is considered a "communications provider" (then the TKG applies) or another form of "electronic information and communication services" (then the TMG applies) and depending on which kind of information are sought (subscriber data, traffic data, content data).* *In general, companies must provide information if approached by an entitled agency (for example, § 174 TKG has a list of agencies and scenarios in which information must be provided).* *"A person (or company) who provides or participates in the provision of telecommunications services on a business basis shall immediately and completely transmit the data to be provided." This is the case in emergency and non-emergency scenarios. "Immediately" is generally interpreted as "without undue delay" which in turn is interpreted depending on the situation. There are no fixed time limits.*
Hungary	*Under Hungarian legislation, there are no specific rules related to the obligation of service providers in emergency circumstances, so the general rules are applicable to the entitled authorities and how to comply with disclosure requests (including time limits). However, law enforcement authorities may send a disclosure request even without a prior prosecutorial permission, in case obtaining such a permission would cause any delay that would significantly jeopardise the purpose of the request. This kind of situation covers emergency circumstances, but may be applicable for other scenarios as well.* *The legal provisions regarding data requests (disclosure requests) in Act XC of 2017 on the Code of Criminal Procedure are as follows:* *[…]* *Section 262: (3) If obtaining permission for a data request would cause any delay that would significantly jeopardise the purpose of the data request, data provision may be requested even without a permission. Data provision may not be refused on the ground that the permission of a prosecutor is missing. In such a situation, the permission of the prosecution service shall be obtained ex-post without delay. If the prosecution service does not permit the data request, data obtained in this manner may not be used as evidence and shall be deleted without delay.*

Ireland	*Section 6 "Requirement to disclose user data" of the Communication (Retention of Data) Act 2011, which was revised and updated on 1 August 2023, provides that:* *(1) A member of the Garda Síochána not below the rank of superintendent may require a service provider to disclose to that member user data in the possession or control of the service provider—* *(a) where the member believes that the data relate to a person whom the member suspects, on reasonable grounds of—* *(i) having committed an offence, or* *(ii) presenting an actual or potential threat to the security of the State,* *or* *(b) where the member has reasonable grounds for believing that the data are otherwise required for the purpose of—* *(i) preventing, detecting, investigating or prosecuting offences,* *(ii) safeguarding the security of the State,* *(iii) protecting the life or personal safety of a person, in circumstances where the member believes that there is a serious risk to the life or personal safety of the person,* *[…]* *The full text of this Act is available at: https://revisedacts.lawreform.ie/eli/2011/act/3/front/revised/en/html.*
Lithuania	*The Law on Electronic Communications of the Republic of Lithuania provides that, in order to ensure the provision of emergency medical or other necessary assistance, where there is information that a person's life and/or health is threatened […], and the person's whereabouts cannot be established by other means, or the use of other means is impossible or inappropriate because of the need to provide assistance to the person or to protect other persons without delay, and any delay could have irreparable consequences for the life and/or health of the person or other persons, service providers shall provide real-time location data to the police authority free of charge. Such data shall be made available as soon as an authorised officer of the police authority makes a reasoned request in writing or by electronic means.*
Malta	*Subsidiary Legislation 399.47, Emergency Communications, The Single European Emergency Call Service ("112" Number) and The European Harmonised Services of Social Value ("116" Numbering Range) Regulations:* *5 (1) A provider shall ensure that caller location information is made available to the most appropriate [Police Safety Answering Point] without delay after emergency communication is set up. This shall include network-based location information and, where available, handset-derived caller location information.*

Slovenia	*Art. 220 of Electronic Communication Act (ZEKom-2) regulates delivery of traffic and location data in cases of protection of life and limb:* *(1) In order to protect the vital interests of an individual, the operator shall, if necessary in the circumstances of a particular case, on the basis of a written request from the police, provide the police with the information necessary to establish the last location of mobile communication equipment or, if technically possible, the last several locations of equipment, provided that:* *1. there is a reasonable likelihood that the life or body of a person who is in possession of, or is believed to be in possession of, mobile communication equipment is in imminent danger and it is necessary to obtain that information in order to prevent death or serious injury to that person, […].* *(7) Upon receipt of a request under paragraph 1 of this Article, the operator shall send the requested information to the requester as soon as possible or as soon as technically possible. The operator shall bear the burden of proving technical impossibility.*

Extraterritorial powers: Production orders and requests with extraterritorial effects

Production orders for electronic data are a type of domestic orders, which may have extraterritorial effects in countries that have established the necessary legal framework.

Asked on this specific matter, 50% of the respondents (12 out of the 24 EU Member States surveyed) indicated that their domestic laws encompass provisions for the issuance of such domestic production orders to service providers situated abroad.

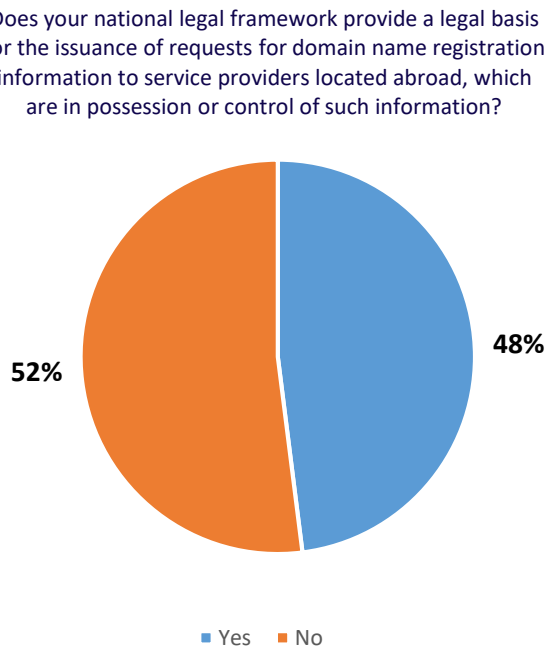
Some of the respondents who indicated that it is possible to issue such domestic production orders shared additional explanations and/or direct references to their national legislation, as further set out in **Table 8**[38].

TABLE 8 – EU MEMBER STATES' LEGISLATION ALLOWING THE ISSUANCE OF DOMESTIC PRODUCTION ORDERS ADDRESSED TO FOREIGN-BASED SERVICE PROVIDERS	
Germany	*Section 100j of the Code of Criminal Procedure:* *Subscriber data request* *(1) Insofar as it is necessary to establish the facts or determine the whereabouts of an accused person, information may be requested* *1. on subscriber data pursuant to section 3 no. 6 of the Telecommunications Act and on data collected pursuant to section 172 of the Telecommunications Act (section 174 (1) sentence 1 of the Telecommunications Act) from the person who, on a commercial basis, provides or collaborates in the provision of telecommunications services and* *2. on subscriber data pursuant to section 2 (2) no. 2 of the Telecommunications and Telemedia Data Protection Act (section 22 (1) sentence 1 of the Telecommunications and Telemedia Data Protection Act) from the person who, on a commercial basis, makes available for use or provides access for the purpose of the use of their own or others' telemedia.*
Poland	*Yes, there is such a possibility based on the provisions of Article 236a of the Polish Code of Criminal Procedure in conjunction with the other provisions of Chapter 25 of the Polish Code of Criminal Procedure.* *According to Article 236a of the Code of Criminal Procedure: The provisions of Chapter 25 apply accordingly to the administrator and user of a device containing IT data or of an IT system, in Article 236b.* *IT companies shall be obliged to provide to the court or to the public prosecutor, in accordance with the request contained in the decision, in cases of utmost urgency, by the police or other authorised body.*

As regards challenges faced by competent authorities when applying this legal framework, a respondent from Lithuania provided further details:

- National courts sometimes refuse to sanction prosecutors' orders for access to documents/information (production orders), arguing that such orders should be sanctioned by the competent authorities of foreign countries. (Lithuania)

As regards to the possibility for competent authorities to directly cooperate with entities providing domain name registration established in another country, the survey results indicate that such the possibility exists in 48% of the surveyed EU Members States (11 out of 23 surveyed[39]).



As regards challenges faced by competent authorities when applying this legal framework, some of the respondents provided further details, as set out in **Table 9**.

TABLE 9 – CHALLENGES FACED BY COMPETENT AUTHORITIES WHEN ISSUING REQUESTS FOR DOMAIN NAME REGISTRATION INFORMATION ADDRESSED TO FOREIGN-BASED SERVICE PROVIDERS	
Czech Republic	*Official court proceedings under Title 18 of the US Code, Sections 2703 and 2711. Where the principle of voluntariness applies, a US company does not always provide a response.*
Germany	*Uncooperative/elusive service providers abroad.*
Ireland	*It is a matter for the service provider to decide whether to respond or not. There is no legal obligation.*
Lithuania	*The risk that some foreign service providers warn the users whose data is being requested about the requests (ignoring our request not to do so).*

Pending the entry into application of the Electronic Evidence Regulation, production orders with extraterritorial effects can be issued by authorities in countries which have implemented Article 18 of the Budapest Convention and/or Article 7 of the Second Additional Protocol (not yet in force) into their national legislation. Specifically, competent authorities can order the production of data in a service provider's possession or control, where either:

- The service provider is offering its services in the territory of the requesting country (Article 18 of the Budapest Convention); or

- The service provider is in the territory of any other Party to the Protocol (Article 7 of the Second Additional Protocol).

Furthermore, Article 6 of the Second Additional Protocol, if implemented into the national legal framework, establishes a legal basis for direct cooperation between competent authorities in one Party and entities that provide domain name registration services in any other Party to the Protocol for disclosure of domain name registration information in their possession or control through the issuance of requests with extraterritorial effects.

The type of data that can be obtained is typically confined to subscriber information[40] or, in the case of requests pursuant to Article 6 of the Second Additional Protocol, domain name registration information. It is also important to note that competent authorities cannot unilaterally enforce domestic orders or requests in the territory of another country, except through established channels of judicial assistance.

However, it is crucial to acknowledge that domestic orders and requests with extraterritorial effects represent a significant and essential instrument that appropriately addresses the worldwide presence of service providers. Furthermore, the future entry into force and broad implementation of the Second Additional Protocol, specifically, would greatly benefit both competent authorities and service providers, for a number of reasons. Primarily, it would establish a well-defined legal framework for cooperation between competent authorities and service providers/entities providing domain name registration services operating within *any* Party to the Protocol. Secondly, Articles 6(2) and 7(2) of the Second Additional Protocol specifically mandate Parties to adopt all necessary measures to ensure that entities/service providers within their jurisdiction can effectively respond to requests/orders issued by competent authorities in other Parties. Consequently, this provision would alleviate concerns of liability for service providers who act in good faith and comply with requests/orders from foreign authorities.

Judicial cooperation

Judicial cooperation refers to issuing formal legal requests for electronic evidence. Such requests are submitted by the competent authorities of one country to the competent authorities of the country where the relevant service provider is based, on the basis of provisions set out in applicable bilateral or multilateral treaties. In order to obtain data via judicial cooperation, competent authorities of EU Member States must issue an EIO – for EU countries other than Denmark and Ireland – or follow an MLA process – for Denmark, Ireland and any country outside of the EU.

In the future, the EU Electronic Evidence legislative package will further expand the mechanism of judicial cooperation with two new legal instruments – European Production Orders and European Preservation Orders. This will go hand in hand with entrusting the judiciary with an increased role for requesting cross-border electronic evidence in criminal proceedings. As an example, under the Electronic Evidence Regulation, production orders for all types of electronic evidence will have to be issued or otherwise validated by a judicial authority (depending on the type of data, this will have to be either a judge, a court, an investigating judge or, in some limited instances[41], a public prosecutor).

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

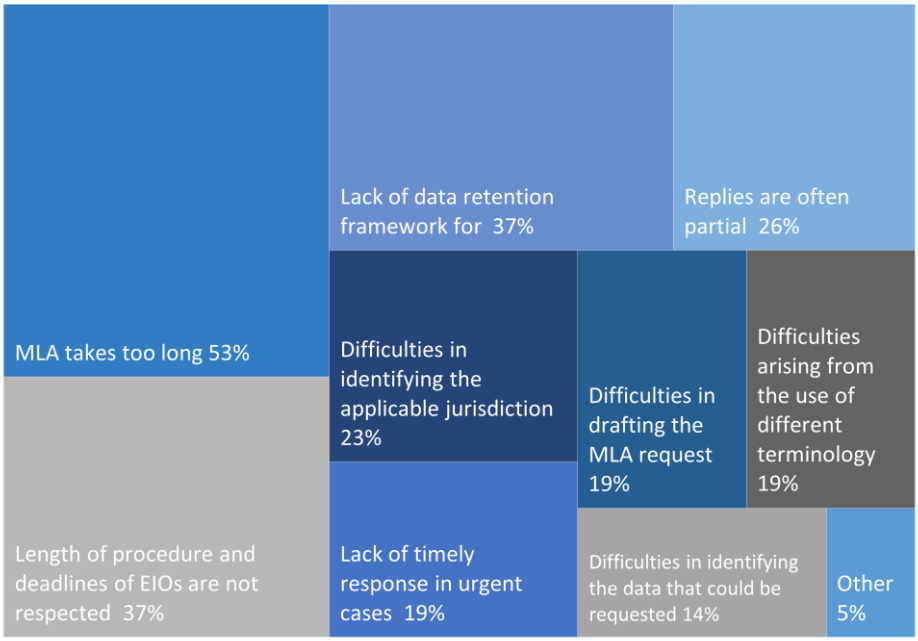
Judicial authorities were asked to identify the main problems with the EIO/MLA process towards other EU Member States[42]. In this respect, the majority of the respondents identified the lengthy procedure, namely the fact that the MLA process takes too long

(53%) and that the deadlines for recognising and executing EIOs are not always respected (37%) as the most challenging issues encountered in their investigations in 2022. The lack of a data retention framework for law enforcement purposes was also ranked among the three most prevalent problems (37%). The fact that the replies received are often partial was selected as the fourth most prominent issue (26%).

Additional challenges reported with a lower prevalence are:

- Difficulties in identifying the applicable jurisdiction: 23%;
- Difficulties arising from the different terminology used by the different service providers and the authorities defining the data types: 19%;
- Difficulties in drafting the MLA request (for example, applicable legal standards): 19%;
- Lack of timely response in urgent cases (such as when there is a risk of destruction/deletion of evidence, detention of a suspect, etc.): 19%;
- Difficulties in identifying the data that could be requested: 14%;
- Other: 5%.

What have been in 2022 in your experience the three main problems with the EIO/MLA process towards EU Member States?



Challenges related to the MLA process towards third States

Considering that a large number of service providers are currently based outside the EU, judicial authorities were asked to identify the main problems encountered with the MLA process towards third States (i.e. non-EU Member States). In this respect, the length of the MLA process was reported as the most challenging issue encountered in investigations in 2022 by the respondents from the EU Members States surveyed (77%).

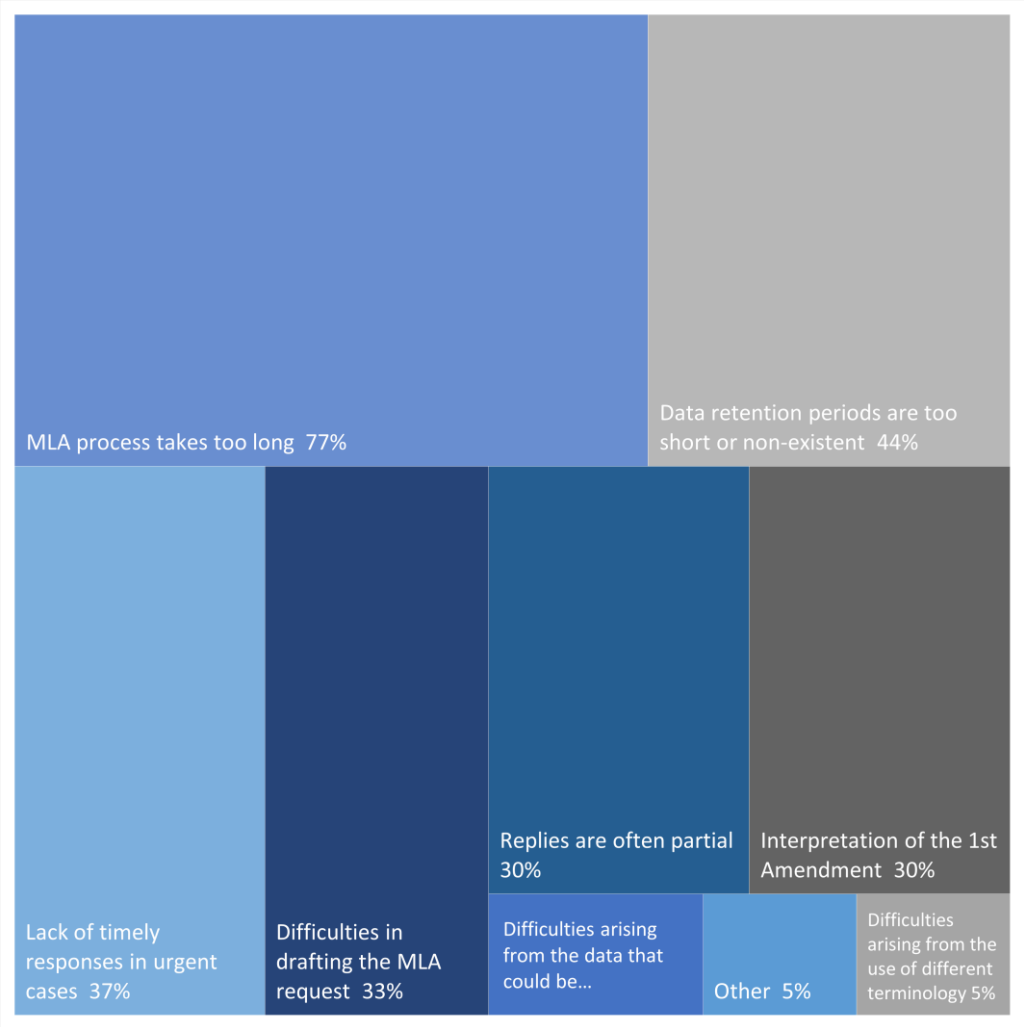
Following this challenge, short or non-existent data retention periods were indicated as another major problem by 44% of the respondents from the EU Members States surveyed. Furthermore, 37% of the respondents referred to the lack of timely responses in urgent cases as one of the main issues encountered.

This comes as no surprise as the same issues were also indicated by representatives of the EU judiciary as top challenges in previous editions of this report. This demonstrates that these issues are recurring and long-standing challenges for EU authorities.

Additional challenges reported with a lower prevalence are:

- Difficulties in drafting the MLA request: 33%;
- Interpretation of a violation of freedom of speech/expression (First Amendment to the Constitution of the US): 30%;
- Partial replies: 30%;
- Difficulties in identifying the data that could be requested: 14%;
- Difficulties arising from the different terminology used by the different service providers and the authorities defining the data types: 7%;
- Other: 5%.

What have been in 2022 in your experience the three main problems with the MLA process towards third States (i.e. non-EU Member States)?



Further information regarding the problems related to the MLA process towards third States was reported by two of the respondents:

- Different classification of crimes based on national criminal law and different standards to access data based on such classification of crimes. (Greece)

- Changes in understanding of what is [to be classified as] child pornography, based on the recent case law in one State. (Slovakia)

Comparing this year's survey results with the information included in previous editions of this report, the results received from all surveyed judicial practitioners are not surprising. On the contrary, the main problems polling highest in recent years indicate a clear tendency of recurring issues repeating over time:

- The lack of a data retention regime for law enforcement purposes;
- The length of the MLA process;
- The fact that the deadlines for recognition and execution of EIOs are not respected;
- The fact that the replies received are often partial.

Implications of cost reimbursement

The growing demand for electronic evidence in criminal investigations and proceedings causes additional costs for service providers and/or national authorities requesting access to such data. Determination of the party which should bear the costs associated with the processing of requests and the disclosure of electronic evidence varies across national legislations in the EU, international/EU legal documents regulating cross-border access to evidence, as well as service providers' internal policies. In the face of this legal fragmentation, the question of the entity bearing the costs of access to electronic evidence could become one of the most important factors for the requesting authorities deciding under which legal framework (e.g. Electronic Evidence Regulation vs. Second Additional Protocol) to issue their requests in the future (even resorting to "legal venue shopping" to minimise the costs for them).

Currently, the reimbursement of costs associated with complying with such requests for data does not appear to have any noticeable effect on access to electronic evidence. Service providers seem to, in general, prefer to abstain from requesting any kind of compensation for providing information. This may change in the future, especially in light of the new Electronic Evidence Regulation, which will allow the authorities from EU Member States to directly order the preservation and production of all types of data, while imposing rather strict time-limits for service providers to comply with such orders (which may, in turn, e.g., lead to additional human resources costs). According to the new Regulation, service providers will be able to claim reimbursement of the incurred costs from the State issuing the order only when so provided in the national law of the issuing State.

The feedback received from judicial authorities on the matter shows that the majority of the EU Member States surveyed do not have any national rules for cost reimbursement in place (14 out of 24). In the context of the application of the Electronic Evidence Regulation, this would mean that service providers will not be able to claim any reimbursement of costs incurred for complying with European Preservation and Production Orders addressed to them from the majority of EU Member States.

Some respondents from EU Member States with legislation that allows service providers to claim reimbursement of costs provided additional information and extracts from their national legislation, which are further detailed in **Table 10**.

TABLE 10 – EU MEMBER STATES' LEGISLATION ON COST REIMBURSEMENT	
Austria	*Reimbursement is to be done in accordance with the Ordinance of the Federal Minister of Justice on the reimbursement of the costs of providers for the provision of information on data of a message transmission, information on stock data and the monitoring of messages (Monitoring Costs Ordinance - ÜKVO):* *Scope of application* *- 1. (1) The reimbursement of the costs for the participation of a provider (Section 92 subsection 3 Z 1 TKG) in the provision of information […] shall be invoked and determined in accordance with the provisions of this Regulation.* *[…]* *Scope of the cost compensation* *- 3. (1) The scope of the compensation is based on the costs (personnel and material expenses) incurred by the provider by the fulfilment of the order (Section 1 paragraph 2). It shall be determined in accordance with the provisions of Section 2. […]* *Determination of master data and access data - 8b. The costs for the determination of master and access data are Euro 40.00.*
Czechia	*Two laws apply to Internet services, namely Act No. 127/2005 Coll. on electronic communications and Act No. 480/2004 Coll. on certain information society services. Those who fall under the first law are charged by Decree "Collection of Laws No. 41 / 2022" and those who fall under the second are not charged.* *Section 97 of the Electronic Communications Act* *[…]* *(3) […] A legal entity or natural person retaining the operating and location data shall provide it without delay upon request* *a) to law enforcement authorities for the purposes and under the conditions laid down by special legislation,* *[…]* *(7) For fulfilling the obligations specified in Subsections 1, 3 and 5 above, the legal entity or natural person is entitled to reimbursement for the efficiently incurred costs from the entitled entity that requested or ordered such an action. The amount and method of reimbursement for the efficiently incurred costs shall be specified in an implementing legal regulation.*

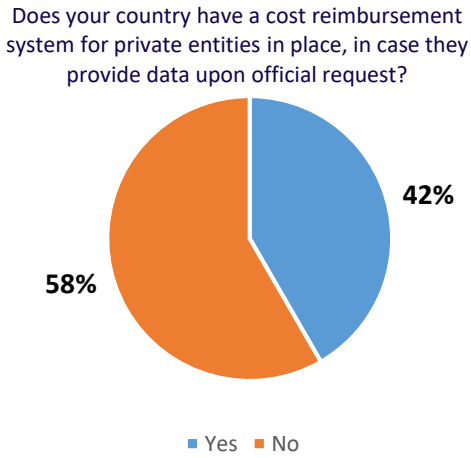
Lithuania	*Article 77 of the Law on Electronic Communications* *Supervision and monitoring of electronic communications traffic* *1. […] Main institutions of criminal intelligence services and pre-trial investigation institutions designated by the Government shall be provided with the above mentioned information by undertakings providing electronic communications networks and/or services immediately, free of charge and in electronic form in response to the enquiries of the said institutions. […] All persons taking part in the exchange of information shall make necessary arrangements to ensure data security in accordance with the procedure and under the conditions set forth by the Government; the additional equipment necessary for this purpose shall be obtained from and maintained with Government funds.* *[…]* *4. Where there is a reasoned court ruling or any other legal basis provided for in the laws, undertakings providing electronic communications networks and/or services must provide entities of criminal intelligence, intelligence institutions in accordance with the procedure established by the law, and pre-trial investigation institutions in accordance with the procedure established by the Code of Criminal Procedure, with technical possibilities to exercise control over the content of information transmitted by electronic communications networks. Equipment necessary for this purpose shall be obtained from and maintained by Government funds.*

Respondents from some EU Member States whose legal frameworks do not currently allow service providers to claim reimbursement of costs also submitted explanatory information, which can be found in **Table 11**.

TABLE 11 – EU MEMBER STATES WHOSE LEGAL FRAMEWORKS DO NOT CURRENTLY ALLOW SERVICE PROVIDERS TO CLAIM REIMBURSEMENT OF COSTS

Croatia	*Operators must ensure at their own expense all necessary technical and organisational measures (Article 53, Paragraph 6 of the Law on Electronic Communications).*
Hungary	*Section 264 (2) of the Act XC of 2017 on the Code of Criminal Procedure* *The organ requested to provide data shall comply with the request free of charge, including in particular the processing, as well as the recording and transfer of the data in writing or by electronic means.*

In addition, the results of the survey confirm that only 7% of the respondents encountered the situation where a service provider requested reimbursement of the costs associated with responding to requests for data. The vast majority of the respondents (93%), including those from the EU Member States with a cost-reimbursement system in place, indicated that they have never received such a claim for compensation, attesting to how exceptionally the service providers' expenses and the reimbursement systems in place currently affect the process of obtaining data from service providers.



Data Retention

Data retention constitutes the continued storage of data by a service provider for a specific period of time. For instance, service providers will retain data for as long as necessary to provide their services and for legitimate business purposes, including invoicing, fraud prevention and enhancing users' safety and security. Service providers will also retain data in order to comply with any legal obligations applicable to them, such as tax and audit regulations.

Data retention for law enforcement purposes

Data retention obligations can also be legally imposed on service providers specifically for law enforcement purposes, i.e. in order to allow access to the retained data by competent authorities for the purpose of criminal investigations and proceedings.

The issue of data retention for law enforcement purposes in the EU has been extensively addressed by the Court of Justice of the European Union (CJEU) after the Data Retention Directive[43] was invalidated in 2014. Since then, the matter is regulated by national law, within the framework set by Article 15(1) of the E-Privacy Directive[44], as interpreted by the CJEU in light of relevant provisions of the Charter of Fundamental Rights of the European Union[45]. The CJEU has established a consistent jurisprudence on data retention for law enforcement purposes, outlining the permissible conditions for retention and access to such data under EU law[46].

At the time of writing, proceedings in two further cases of relevance to the conditions for access to retained data are pending before the CJEU.

The first case, Case C-178/22 *Procura della Repubblica presso il Tribunale di Bolzano*[47], derives from a request from the Public Prosecutor to access 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. Access to such data therefore appears to amount to a serious interference with the users' fundamental rights. According to the CJEU's jurisprudence, such access may be justified by the objective of preventing, investigating, detecting and prosecuting *serious* criminal offences (not criminal offences in general).

The Opinion of the Advocate General makes the following main points:

- EU Member States retain the power to define "criminal offences", including "serious criminal offences", within their national law, and to set penalties for engaging in such conduct;
- Access to sensitive data for prosecuting what has been determined by the national legislature to constitute a "serious offence" must still be reviewed beforehand by a court or independent administrative body, which must assess whether allowing such access constitutes a proportionate interference with fundamental rights, considering the public interest objective of combating crime in a particular case. In certain cases, access to such data may not be granted, even where the offence reaches the threshold of seriousness under national law; and
- Any such assessment must take into account and weigh all relevant rights and interests, including the damage caused to victims' rights and the rights of third parties[48].

The second case, Case C-470/21 *La Quadrature du Net and Others*[49], concerns the conditions for accessing civil identity data corresponding to IP addresses under EU law. The case has gone through initial proceedings, including an Opinion from the Advocate General, before being referred to the full Court at the request of the Grand Chamber[50]. As of the writing of this report, a further Advocate General Opinion is still pending and is expected to be delivered at the end of September 2023.

Although the CJEU has provided clear guidelines on the conditions for the retention of data for law enforcement purposes and for access to such data under EU law, the lack or limited scope of such data retention frameworks remains a persistent challenge. As noted in other parts of this report, this issue continues to pose difficulties for EU judicial authorities when seeking data from other jurisdictions, whether through voluntary cooperation or judicial assistance.

Recent legal developments will considerably expand the tools available to EU judicial authorities for cross-border data requests. However, in order to be able to obtain access

to electronic data, such data must be available in the first place. Therefore, there is still a strong demand for EU-wide legislative efforts to harmonise and regulate data retention specifically for law enforcement purposes. Such harmonisation, which could be done in the proposed e-Privacy Regulation[51] or another EU legislative instrument, would streamline the process and enhance cooperation among EU Member States in obtaining electronic data for investigative and prosecutorial needs.

New data retention obligations under the Digital Services Act

The DSA, an EU law that sets out updated and harmonised rules for providers of digital services, introduces a specific retention obligation for providers of online platforms which allow consumers to conclude distance contracts with traders (i.e. natural or legal persons, privately or publicly owned, who are acting for purposes relating to their trade, business, craft or profession).

Pursuant to Article 30 of the DSA, before allowing traders to use their platforms to promote messages on or offer products or services to consumers in the EU, platform providers designated as "very large online platform"[52] must collect a set of information (including but not limited to the name, address, telephone number and email address of the trader; a copy of the identification document of the trader or any other electronic identification; and the payment account details of the trader) that must be stored by the platform provider for the duration of the contractual relationship with the trader concerned and for a further 6 months after the end of the contractual relationship. The information can only be disclosed to third parties, including law enforcement and judicial authorities, when so required by the applicable law. Furthermore, certain information regarding traders (name, address, telephone number and email address; trade register information; self-certification) must be made publicly available on the relevant platform's online interface.

The European Judicial Network perspective: The practical application of EIO/MLA procedures to obtain encrypted information

Encryption is a genuine means to protect user privacy, communications and devices. However, criminal organisations have started exploiting this technology, enabling them to conceal illegal activities from authorities.

As an example of this, within the EU, the EncroChat toolprovided an encrypted telephone solution, which was widely used among criminal networks worldwide. In 2020, French and Dutch law enforcement and judicial authorities, with the assistance of Europol and Eurojust, managed to dismantle EncroChat[53]. Since then, a number of similar successful operations within and beyond the EU have followed, for instance, against SkyECC[54] and Anom[55].

The millions of messages exchanged between persons located in different countries have revealed the high degree of organisation of criminal groups and the seriousness of the crimes committed. In order to proceed with the related investigations, EU Member States and other countries have sent a high volume of EIOs and MLA requests which raised numerous judicial challenges.

In this light, EJN Contact Points within and beyond the EU, as well as partners, have reflected on the following issues related to obtaining encrypted information for the purpose of criminal investigations:

i. Type of measure

Countries initiating the investigation of criminal activities which concealed their communication by encrypted means have managed to obtain the evidence by infiltrating/intercepting the communications in accordance to the requirements of their respective legal systems. As the digital and encryption aspects presented some novelties to authorities, the EJN Contact Points discussed if the requests for evidence were understood as a request for interception or a request for documentation already existing in the EU Member States concerned.

In this respect, some practitioners explained that, collecting of the encrypted files presented challenges due to the mere nature of the encryption. However, some courts have established the practice that EIOs and MLAs can be used also for collecting also the encrypted information. The EJN Contact Points from different EU Member States and non-EU countries discussed that often practitioners fear that dealing with encrypted information requires other particular procedure. However, once it was understood that encryption was a method to secure digital data, they also learned about the process of gathering this information.The procedures for judicial cooperation were not more complex than in other situations. Therefore, training and understanding are essential for practitioners to enhance the knowledge of the concept of encrypted information and electronic evidence in general, for example:

- EU Member States are encouraged to organise meetings to promote discussions of the developments in cases involving encrypted communications; and
- Networks such as the EJN and the EJCN should continue strengthening the cooperation and creating opportunities for discussions to share experiences and find joint solutions to support judicial authorities.

Furthermore, defence lawyers have gathered expertise and efficient mechanisms to exchange information on know-how and case law involving investigations with encrypted communications. Therefore, judicial authorities should also benefit from a similar exchange of expertise as investigations involving novel technologies present them with similar questions in different jurisdictions.

As the initial measures involved the interception of encrypted communications, the EJN Contact Points discussed if additional assessments were required. In this regard, a number of the EJN Contact Points remarked that it was understood that another country had done the interception in accordance with their national legislation and procedural safeguards. Therefore, the country that intercepted the communications had already performed the initial assessment on the principles of necessity, legality and proportionality.

ii. Spontaneous exchange of information

As the evidence is retrieved by the country initiating the interception, the received information is often exchanged with the other countries. The initial collection of the encrypted communications is done as the country that initially intercepted the information believes that the content of information is unknown to the other country – hence no EIO/MLA would be expected from there– and would voluntarily assist another country in their investigations.

During the discussions, some EJN Contact Points explained that the spontaneous exchange of information had been done, for instance, through the following means:

- Spontaneous exchange of information on the basis of Article 7 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the EU;

- Spontaneous exchange of information on the basis of Article 26 of the Budapest Convention; and
- Applicable Europol Handling Codes in data processing/exchanging.

iii. Issuing authority

If the country that received the spontaneous information decides to proceed with the request, usually an EIO or MLA request would be sent to obtain as evidence in their criminal case the information that already has been intercepted by another country. However, in light of the latest decisions of the CJEU (for example, in the case C-724/19[56]) , some EJN Contact Points have expressed that regardless of the measure at hand, in their countries the EIOs would have to be issued by a court/judge.

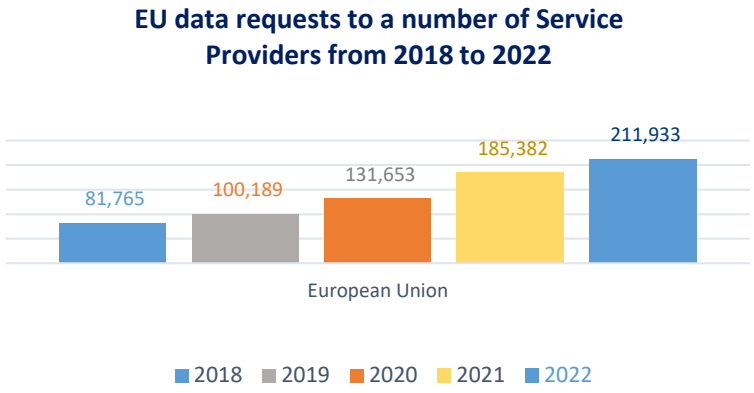
iv. Admissibility of the evidence

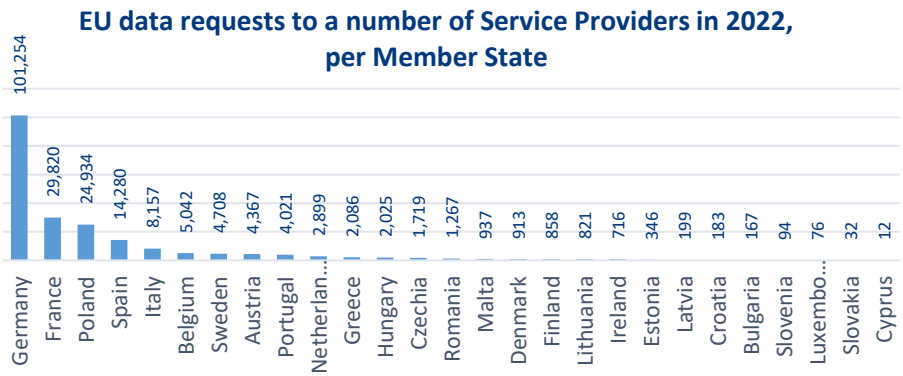
Practitioners from some EU Member States and non-EU countries have extensively shared that national courts have admitted information decrypted by the other country as evidence. Furthermore, prosecutors and courts have not only relied upon the information received but also presented corroborating evidence that strengthened or confirmed the facts presented in these files, for instance, for the identification of the accused.

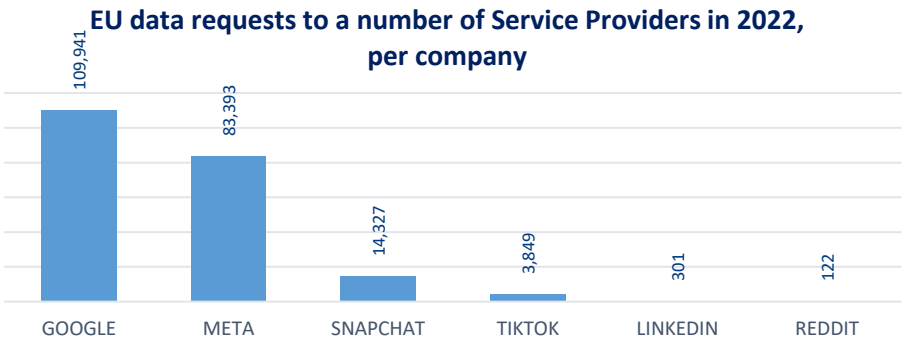
PERSPECTIVE OF SERVICE PROVIDERS

Volume of data requests per country and per Service Provider

The volume of data disclosure requests submitted by EU competent authorities to six service providers increased by 14% from 2021 to 2022. Last year, 211.933 requests were submitted to Google, LinkedIn, Meta, Reddit, Snapchat and TikTok. This is the result of the analysis of transparency reports published by the service providers themselves[57]. Germany submitted almost half of all requests in the EU in 2022(48%), followed by France (14 %). Among the service providers analysed, Google was the one that received most of the requests, followed by Meta.

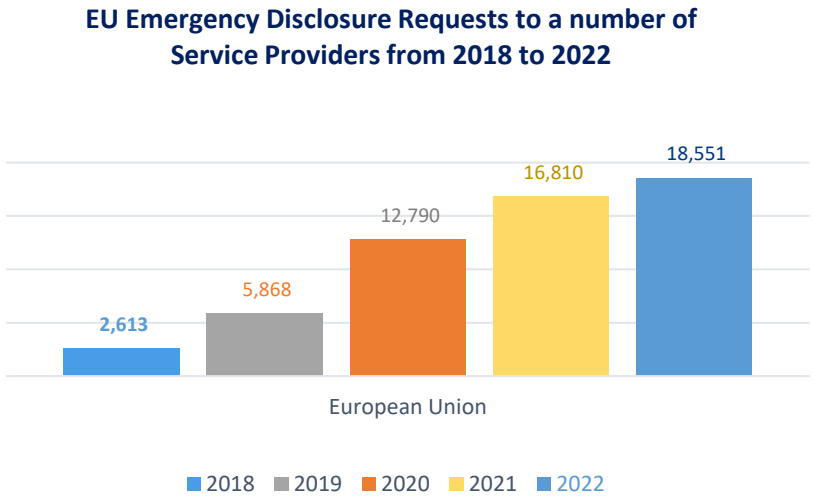


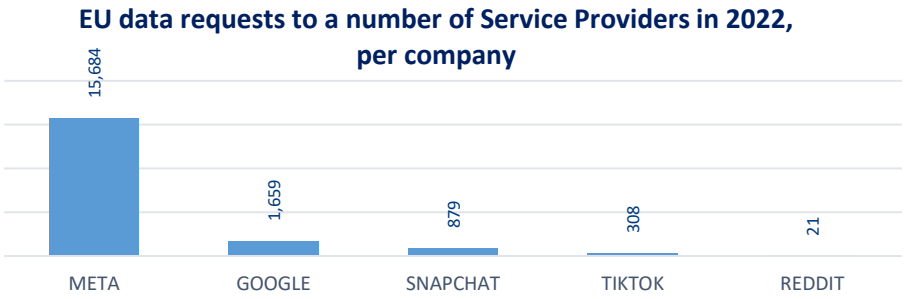




Volume of Emergency Disclosure Requests per country and per Service Provider

The concept of *emergency* is usually fulfilled when there is imminence of harm or serious physical injury to any person. Some service providers adopt a wider definition of emergency situations to include imminent and serious threat to the security of a State, the security of critical infrastructure or installation or crimes involving minors. From 2021 to 2022, the volume of Emergency Disclosure Requests issued by EU competent authorities increased by 10%, to 18.551, considering data from five service providers[58]. The majority of the requests were submitted by France to Meta (70% of all the Emergency Disclosure Requests in the EU in 2022).



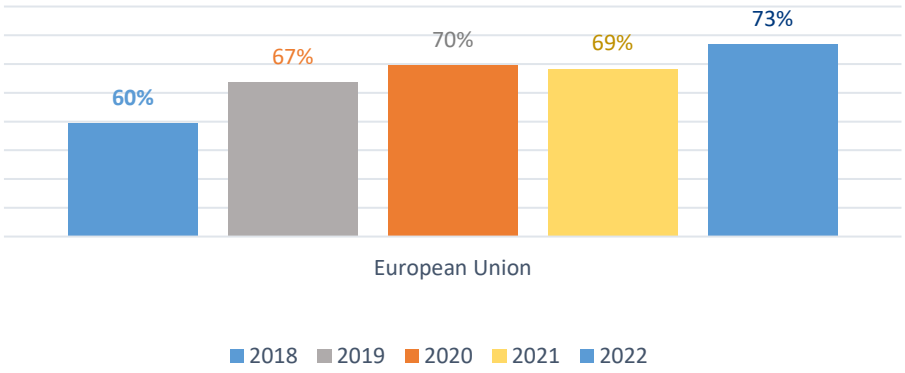


Success rate of EU cross-border requests for electronic evidence

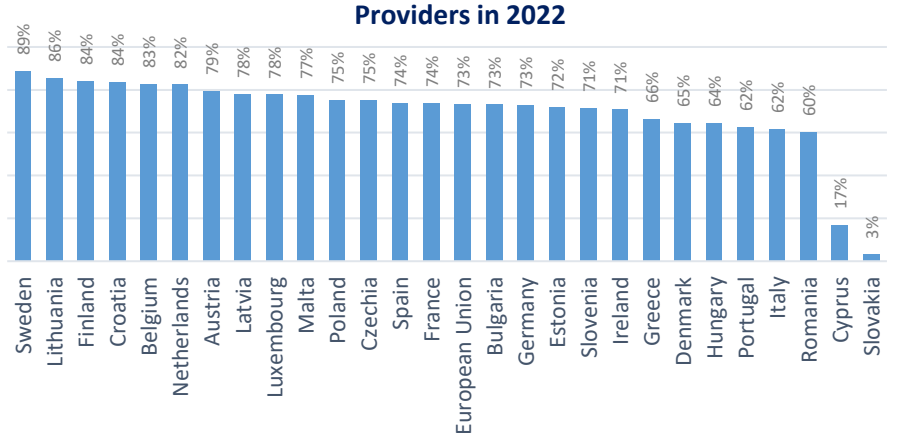
The average success rate of data disclosure requests submitted by EU competent authorities increased by 4% from 2021 to 2022, despite the considerable increase in volume in this period. The average EU success rate at 73% is the best result since the first edition of this report (created using data from 2018). There are 14 EU Member States that have a higher than average success rate. Sweden, Lithuania, Finland, Croatia, Belgium and Netherlands all have success rates above 80%. These results attest to the fact that EU competent authorities and service providers alike have more mature processes in place, and more experience in the field of cross-border access to electronic evidence.

Among the companies analysed, Google had the higher success rate (80%) and TikTok the lowest (51%). Moreover, EU Member States where SPoCs for direct requests under voluntary cooperation have been established have a higher success rate by 4% on average than those that do not have such units.

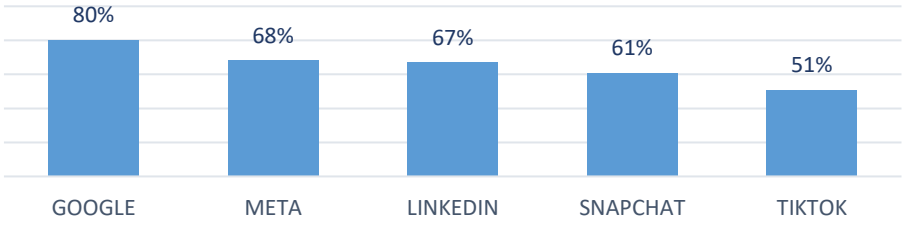
Average EU Success Rate of Requests to a number of Service Providers from 2018 to 2022

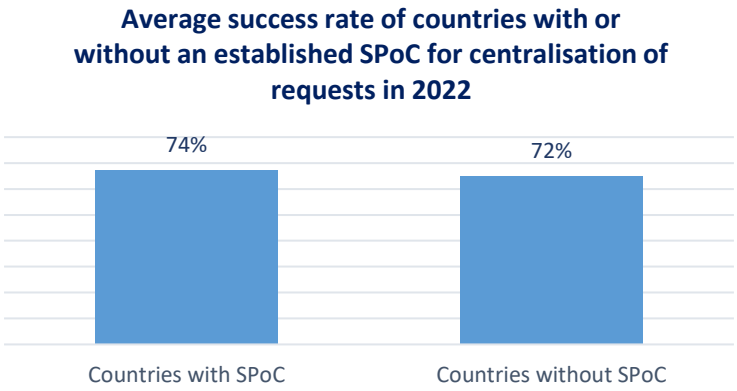


Success rate of EU data requests to a number of Service Providers in 2022



Average EU Success Rate of Requests to a number of Service Providers in 2022





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

The success rate of EU cross-border requests for electronic evidence is an important metric. Understanding the volume of requests rejected by service providers, and the reasons behind it may provide opportunities for improving the efficiency of the overall process. Competent authorities and service providers alike should strive for high success rates, which, in turn, would indicate an efficient use of resources. Thus, high success rates of data disclosure requests increase the speed with which criminal investigations can be conducted.

There are no official comprehensive statistics on the reasons why data disclosure requests are delayed or rejected by service providers. However, service providers indicated there were no major changes in 2022 in relation to what has been reported in previous years. The reasons for refusal or delay in processing direct requests for voluntary cooperation issued by EU authorities mentioned in 2022 are listed below. Many of these issues could be avoided by increasing awareness and ensuring capacity-building activities among requesters, by improving the clarity of the guidelines provided by service providers, and by increasing opportunities for direct engagement among service providers and competent authorities.

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

- Overly broad requests

Requests that fail to identify a targeted number of accounts in connection with the investigation or that cover an excessive amount of data about the specified users are often considered as overly broad. In these situations, authorities need to narrow down the request by specifying the service concerned – out of the many services offered by one entity – by defining a specific and narrow timeframe of relevance for the information sought, and/or by listing the exact datasets that are being requested. For instance, requests that refer to “all available data” concerning specific account(s) are generally considered to be overly broad.

- Procedural issues

Requests for disclosure of data are often delayed or rejected due to procedural issues such as missing dates, the fact that a wrong or no legal basis is mentioned, lack of signature or even because they are addressed to the wrong legal entity. Additionally, service providers could reject requests that were issued too long ago.

- Emergencies that do not meet the necessary criteria of imminent harm

Most service providers that accept direct requests for voluntary cooperation in emergency circumstances require authorities to demonstrate in the request the imminence of danger to the life of a person, and how the data sought may help. In practice, due to confidentiality concerns, extreme time pressure, or lack of preparedness, authorities may not provide complete details of the incident, which may lead service providers to request supplementary information or reject the request. Moreover, there can also be different interpretations of emergencies, or lack of understanding from untrained officials regarding the necessary thresholds.

- Linguistic barriers

Service providers report that some requests may be poorly written in English, or contain translation mistakes due to the use of automated online translation tools. Such situations may lead to delays as additional communication between service providers and authorities is required. In some cases, requests may need amendments or even to be re-issued and translated again.

- Incorrect identifiers or non-existing target

Different platforms use different account identifiers for their users' accounts, which can lead to misunderstandings in formulating data disclosure requests. For instance, many online services, such as social media platforms, allow users to change their display name at any time, and do not prevent different users from having the same username. Therefore, authorities must ensure they provide *unique* identifiers particular to the specific platform targeted, so as to allow the service provider to locate the specific account of interest. Commonly accepted identifiers are e-mail addresses, phone numbers with country code or platform-specific unique usernames/profile URL. Furthermore, a mistake as simple a typo in the identifiers may also lead the service provider to believe the targeted account does not exist.

- Jurisdictional challenges

Some service providers only accept direct requests under voluntary cooperation for data pertaining to users who are located in the same jurisdiction as the requesting authority. Because it is not always possible to determine the jurisdiction of a user, some service providers consider the EU as one jurisdiction, while others may restrict the responses within each country. Therefore, requests for data stored in a different jurisdiction may lead to delays or rejection of requests.

- Dual criminality requirement

As service providers must respect the domestic legislation of the country that they are based in, they may refuse to disclose data for the investigation of specific crimes which are not punishable under the domestic criminal law system of that country. For example, the dual criminality requirement could lead to the rejection of requests related to hate speech crimes, depending on the jurisdictions involved.

- Requirement for MLA process

Some service providers apply different policies to different countries, even within the EU. For instance, some service providers accept direct requests under voluntary cooperation only from specific EU Member States. Requests submitted by other EU Member States to these service providers are automatically rejected, and authorities are advised to follow an MLA process. For example, this is the case of Snapchat and Yahoo, which only accept direct requests from a very limited number of EU Member States, without any publicly available indication of the reason for such differences in policies.

Most service providers apply a common policy for data requests from competent authorities across the EU. However, some requests might still be rejected with an indication to follow an MLA process when the data requested is content data.

- Lack of information regarding the link between the crime under investigation and the data sought

Service providers assess the necessity and proportionality of direct requests under voluntary cooperation based on the information provided by competent authorities. Some requests may be rejected when it is not clear how the data sought could assist the investigation, or when there is no clear link between the case under investigation, the user and the platform addressed.

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

When service providers require additional information to process a request, they generally reach out to the competent authority via the same channel used for the submission of the request. In such situations, authorities may mistakenly understand that the service provider is being uncooperative and pursue different investigative approaches, or they may not be in a position to provide the requested information. The lack of response from authorities frequently leads to the rejection of requests.

- Misunderstanding on the datasets available

Data disclosure requests are rejected when the data requested is not collected by the service provider, or is only collected with end-to-end encryption. Large service providers which offer numerous products and services may be more affected by this issue, as there may be more misunderstandings in relation to the data they collect from users.

Existing challenges: the perspective of service providers

Law enforcement response teams dealing with data disclosure requests from competent authorities face numerous challenges in their day-to-day work. They often work under the pressure of an ever-increasing volume of requests, as well as in a constantly evolving legal landscape in many countries where their companies operate. For example, some of the service providers reported that each request they receive represents a considerable workload to staff, which is not always clear to requesters. During the interviews with service providers conducted to collect data for this report, they also mentioned other specific challenges which are listed below.

- Dealing with a large number of one-time requesters requires more resources

Service providers report that law enforcement officers who have never sent requests to them in the past (what some providers call "one-time requesters") often need to be contacted individually to clarify the requirements of the request or the circumstances of the case. This may have a considerable impact on service providers, considering the large volume of requests they receive. As a matter of fact, the need to contact one-time requesters to clarify policies and requirements is one of the biggest challenges for many service providers, as many officers have little or no formal training in electronic evidence matters.

- Monitoring frequent changes of applicable policies at the national level around the world

Law enforcement response teams are in charge of responding to data disclosure requests from competent authorities in many or all the countries where a service provider operates. Because of this, staff members need to be trained in specific legal aspects of each country, and sometimes consider regional differences within the same country. Monitoring worldwide policy changes at local level, and their impact to processes was reported as a challenge by some service providers, as it requires constant monitoring and adaptation.

- Authentication of incoming requests

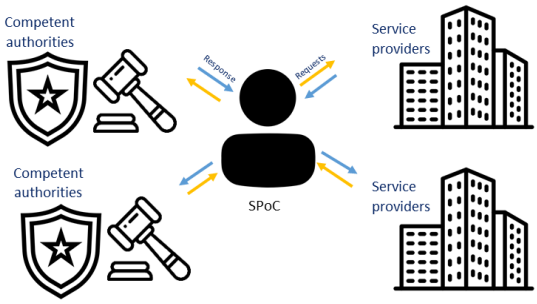
Service providers report that authenticating incoming requests is challenging. Many of them use a list of vetted e-mail domains of EU authorities provided to them by the SIRIUS Project. However, service providers do not rely solely on the e-mail domain of the requester, as they also consider different aspects of the request to ensure it was issued by a competent authority. In some cases, law enforcement response teams may try to confirm the authenticity of requests by calling law enforcement agencies, or previously established SPoCs.

To mitigate these challenges, some service providers mentioned two measures. First, the creation of dedicated online portals for law enforcement requests, which guide requesters in providing all the required information, facilitate authentication, and make the overall process more effective. Second, the establishment of processes with SPoCs also largely contributes to improvements in all the areas mentioned, since it ensures a more streamlined communication and improved processes, as further explored in the next section.

The experience of service providers with Single Points of Contact

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

Single Points of Contact (SPoCs) for electronic evidence requests



As in previous years, all service providers that have engaged with SPoCs in 2022 report more positive experiences with these units, in comparison with agencies without SPoCs. Some service providers confirmed that the success rate of requests is considerably higher in countries where SPoCs have been established, compared to those which do not have them in place.

More specifically, service providers reported the following advantages of SPoCs:

- SPoCs act as an important filter, ensuring high quality standards of the data disclosure requests before they are even submitted to the service provider. For example, because of previous experiences, SPoCs are aware of the correct legal entity to address in a request, which data needs to be included and which datasets can be provided;
- The engagement with SPoCs facilitates direct communication between service providers and law enforcement, leading to fast identification of possible issues in the existing process and of solutions that benefit both sides;
- The establishment of procedures with SPoCs brings consistency to the overall process, facilitating the processing of data disclosure requests;
- SPoCs have a good level of English and technical background which facilitates the communication between the involved parties;
- SPoCs are better placed to ensure all officers within a law enforcement agency have access to policy updates and changes to the service, whenever needed.

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

EU Electronic Evidence legislative package

The EU Electronic Evidence legislative package will change how EU competent authorities can request access to data in the context of criminal investigations. As

previously mentioned in the Context section, the new policies will enter into force only in 2026, but most service providers interviewed for this report have already started to consider how they will impact their processes in the future.

The perceptions and the concerns of service providers around the upcoming EU Electronic Evidence legislative package vary a lot. The majority of those interviewed have welcomed the new legislative package, while still expressing concerns over the challenges of its application, as further detailed below.

Most service providers welcome the new rules for:

- Bringing more legal certainty to the process of data disclosure in criminal investigations, eliminating or reducing the burden service providers currently face in assessing the lawfulness of each request against a complex legal landscape, composed of numerous applicable national laws, as well as international instruments; and

- Setting out the applicable legal basis and standardising the format of data disclosure and preservation orders.

Conversely, service providers have also expressed several concerns over the upcoming legislative package and its implementation, some of which are listed below.

- A large multi-stakeholder effort is necessary in order to prepare for the implementation of the EU Electronic Evidence legislative package, but so far little effort has been put in by stakeholders. Some service providers call for systematic and regular engagement among public and private parties, which should allocate dedicated staff to ensure alignment on practical aspects of the new policy;

- Complying with the deadlines for responding to European Production Orders in *non*-emergencies could be challenging, because it is not possible for service providers to estimate the volume of orders that they will receive (and, in turn, prepare accordingly);

- The decentralised system for secure digital communication and data exchange between competent authorities and service providers is a topic of concern. Service providers operating globally mention that the fragmentation of channels for requests from competent authorities, in different countries, poses practical challenges that can impact efficiency;

- Competent authorities should provide continuous and high-quality training to officials, to ensure that European Production Orders take into consideration the specificities of each service provider. For instance, many requests are rejected because the requested data is not collected by the service provider in question, or the wrong account identifier is provided. To ensure the new regulation is successful, competent authorities must keep up-to-date with the products, services and policies of service providers;

- The volume of requests submitted under voluntary cooperation today is disproportionately higher than requests via judicial cooperation for many service providers. The new EU Electronic Evidence Regulation requires that a judge, a court, an investigating judge or – in some limited instances – a public prosecutor issues *or validates* European Production Orders[59]. Therefore, judicial authorities could be faced with a large increase in workload, requiring considerable allocation of resources in EU Member States where they are not

already involved in all requests issued by law enforcement. Lack of preparations from judicial authorities to cope with increased volumes could lead to bottlenecks in the process.

Service providers were asked whether they will continue to accept direct requests under voluntary cooperation, once the new EU Electronic Evidence Regulation will come into force in mid-2026. The responses on this matter varied widely:

- Some providers indicated that it is too early to take a decision on the future of direct requests under voluntary cooperation;
- Some providers indicated that they plan to completely stop accepting direct requests under voluntary cooperation as soon as the new regulation will be applicable;
- Some providers indicated that even if they will stop accepting direct requests under voluntary cooperation, they would consider complying with such requests in emergency cases with imminent threat to life, in order to ensure the fastest process possible;
- Some providers indicated that they plan to continue accepting direct requests under voluntary cooperation, because this might continue to be a more effective process, considering the high volume of criminal investigations that require electronic data disclosure.

During this year's interviews, several service providers have praised the SIRIUS Project for promoting knowledge-sharing at EU level, fostering multi-stakeholder engagement, creating crucial networking opportunities and monitoring the state of play regarding cross-border access to electronic evidence as presented in this public report. Some service providers have suggested that the SIRIUS Project may have an important role in the EU in the years to come. For example:

- SIRIUS could promote recurrent workshops and multi-stakeholder engagement on dedicated practical aspects of the implementation of upcoming policies;
- SIRIUS can play an important role to ensure a centralised repository of up-to-date information in relation to the specificities of each service provider, such as the account identifiers of each service, correct legal entities and datasets that can be requested;
- SIRIUS could continue to monitor the state of play regarding cross-border access to electronic evidence, in order to identify potential areas of improvement, and offer valuable data to stakeholders;
- SIRIUS could provide practical guidance in electronic evidence matters to providers which offer online services in the EU Single Market.

RECOMMENDATIONS

For EU Law Enforcement Agencies

Initiate preparations for the implementation of the EU Electronic Evidence legislative package

Law enforcement agencies should designate teams to assess what impact the EU Electronic Evidence legislative package will have on their activities in the field of electronic evidence. They should also actively engage with domestic judicial authorities, relevant service providers and authorities in other EU Member States to establish processes and procedures. Active participation in future SIRIUS events is encouraged to help facilitate coordination and preparedness.

The EU Electronic Evidence legislative package may have significant effects on law enforcement agencies especially, considering that service providers could stop accepting direct requests under voluntary cooperation. Once the new rules are in place, increased coordination with domestic judicial authorities will be required for the issuance of European Production Orders and European Preservation Orders.

Adapting current internal processes to the new legislation will generate a more effective result if conducted in a coordinated manner. SIRIUS' established role as a centre of reference in the EU could facilitate this process by enabling information-sharing on bilateral and multilateral levels.

Include training on cross-border access to electronic evidence in routine training programmes for investigators and first responders

Ensuring law enforcement officers are prepared to request and analyse electronic evidence is crucial for effective criminal investigations. It is recommended that training activities on cross-border access to electronic evidence are included in routine training programmes for investigators and first responders.

In addition to evolving legislation, EU investigators and law enforcement at large will be confronted with new challenges stemming from the evolving technological field, as this report shows. Ensuring technical preparedness, aligned with legal requirements, could increase efficiency in the entire cycle that connects the investigation and prosecution of crime.

Ensure active engagement of SPoCs in the SIRIUS SPoC Network

The SIRIUS SPoC Network is composed of all SPoCs established in the EU, offering its members a restricted online platform for secure communication and the dissemination of resources. Members may also participate in restricted online and in person events organised by the SIRIUS Team focused on improving coordination and the dissemination of knowledge, experiences and lessons learned.

It is recommended that SPoCs are established in all law enforcement agencies. Law enforcement agencies working on the establishment of SPoCs are encouraged to contact the SIRIUS Team at Europol to join the SIRIUS SPoC Network as observers.

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

For EU Judicial Authorities

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

Continuous training on available legal instruments and specific procedures for requesting the preservation and production of electronic evidence across borders is essential. This will ensure that EU judicial practitioners have the required knowledge and skills to acquire electronic evidence by using the most appropriate solutions that match the specific needs of a case.

In this respect, EU judicial authorities are encouraged to use the support and resources offered by EU actors active in the field of judicial cooperation, including Eurojust, the US-EU MLA Expert group, the EJN and its website, the EJCN, the European Judicial Training Network (EJTN) and the SIRIUS project.

Judicial authorities can contact the SIRIUS Team at Eurojust via e-mail at sirius.eurojust@eurojust.europa.eu.

Prepare judicial authorities for the use of new instruments under the upcoming legislative changes related to the cross-border gathering of electronic evidence

Ongoing legal developments, such as the EU Electronic Evidence legislative package, the Second Additional Protocol, CLOUD ACT executive agreements and the UN Convention on Cybercrime, will bring ground-breaking changes in the process of cross-border gathering of electronic evidence.

To be properly prepared for the imminent changes to the legislative framework for the acquisition of electronic evidence across borders, EU judicial authorities are encouraged to use the resources, as well as the training and awareness-raising sessions developed and offered by the SIRIUS project.

Judicial authorities can contact the SIRIUS Team at Eurojust via e-mail at sirius.eurojust@eurojust.europa.eu.

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

Recognising the challenges faced by EU judicial practitioners when gathering electronic evidence across borders, it is of paramount importance to strengthen mutual trust among judicial authorities in the EU. Another aim is to foster knowledge sharing and the exchange of best practices on accessing electronic evidence from different jurisdictions.

In this regard, EU judicial authorities are encouraged to actively engage with members of the judicial community via the dedicated forum on the SIRIUS platform.

For Service Providers

Initiate preparations for compliance with the EU Electronic Evidence legislative package

First, service providers that offer services in the EU, but do not have a legal establishment in one of the EU Member States, should carefully consider the obligations that will stem from the Electronic Evidence Directive.

Second, service providers should carefully consider how the Electronic Evidence Regulation will impact their existing processes and resources. For example, many service providers reported the need for additional human resources and technical solutions to allow them to comply with the deadlines for responses to European Production Orders set out in the Electronic Evidence Regulation.

An early engagement with the SIRIUS Project seems beneficial in both cases. The expertise developed within the project would support a wide range of service providers – long established ones, small and medium enterprises but also those service providers that are entering the EU market. From different standpoints, they will all be required to familiarise themselves with the applicable legislation in the field of cooperation with EU authorities.

Engage in international events organised by SIRIUS and share policy updates with the SIRIUS Team

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

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

END NOTES

[1] 27 EU Member States, as well as countries with an operational agreement with Europol and/or an international or cooperation agreement with Eurojust.

[2] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.191.01.0118.01.ENG&toc=OJ%3AL%3A2023%3A191%3ATOC.

[3] Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.191.01.0181.01.ENG&toc=OJ%3AL%3A2023%3A191%3ATOC .

[4]https://www.europarl.europa.eu/news/en/press-room/20230609IPR96203/electronic-evidence-new-rules-to-speed-up-cross-border-criminal-investigations and https://www.consilium.europa.eu/en/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/.

[5] The Electronic Evidence Regulation (2023/1543) shall apply from 18 August 2026 while in the case of the Electronic Evidence Directive, EU Member States shall adopt the necessary measures to comply with it by 18 February 2026

[6] See supra note 2.

[7] See supra note 3.

[8] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT .

[9] Voluntary cooperation is currently common practice for many service providers in the EU. Moreover, direct cooperation with service providers in other jurisdictions to obtain subscriber information will also be possible for example in accordance with Article 7 of the *Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and disclosure of Electronic Evidence*, once the instrument comes into force in countries that ratify it.

[10]https://www.coe.int/en/web/cybercrime/-/japan-becomes-2nd-state-to-ratify-the-second-additional-protocol-to-the-convention-on-cybercrime#:~:text=Today%2C%2010%20August%202023%2C%20Japan,Europe%2C%20deposited%20the%20instrument%20of .

[11] https://www.coe.int/en/web/cybercrime/second-additional-protocol and https://www.coe.int/en/web/cybercrime/-/t-cy-confirms-broad-scope-of-powers-for-the-collection-of-electronic-evidence-and-international-cooperation%C2%A0.

[12] https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en.

[13] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065

[14] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

[15] DSA, Article 10

[16] https://unric.org/en/a-un-treaty-on-cybercrime-en-route/.

[17] Austria, Belgium, Bulgaria, Croatia, Czechia, Denmark, Estonia, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

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

[19] Responses may have been edited for additional clarity, or translated from different EU languages into English.

[20] SIRIUS EU Digital Evidence Situation Report 2022, 4th Annual Report, 22 December 2022

[21] Responses may have been edited for additional clarity, or translated from different EU languages into English.

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

[23] Responses may have been edited for additional clarity, or translated from different EU languages into English.

[24] See supra note 13.

[25] See DSA, Article 10.

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[27] As indicated during the interviews conducted by the SIRIUS Project team with service providers in 2023.

[28] For the purposes of this report and the underlying survey, the data categorisation applied is the one set out in the Budapest Convention on Cybercrime (Budapest Convention) and its Explanatory Report as well as the EU Electronic Evidence legislative package. Definitions are available for each category of data in the Budapest Convention and its Explanatory Report: subscriber information (Article 18(3) of the Budapest Convention), traffic data (Article 1(d) of the Budapest Convention) and content data (Explanatory Report, para. 209), as well as the Electronic Evidence Regulation, Article 3.

[29] All data referring to 2020 has been rounded up or down to allow immediate comparison with data gathered as of 2021.

[30] For more information regarding the implementation of Article 32 into the national legislation of EU Member States, see the topic-specific factsheet prepared within the framework of the SIRIUS Project, available at: https://www.eurojust.europa.eu/publication/trans-border-access-stored-computer-data-under-article-32-budapest-convention.

[31] The answers received from one EU Member State have been excluded, as they were inconclusive
[32] The answers received from one EU Member State have been excluded, as they were inconclusive
[33] The answers received from one EU Member State have been excluded, as they were inconclusive
[34] For the purposes of this report, data retention refers to the continued storage of data by a service provider due to regulatory requirements, in the absence of a specific request from authorities in relation to specific criminal investigations or proceedings, as also defined in the SIRIUS EU Digital Evidence Situation Report 2022, 4th Annual Report, 22 December 2022, p. 53. See also section d. Data retention.

[35] 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; and SIRIUS EU Digital Evidence Situation Report 2020, 2nd Annual Report, 1 December 2020.

[36] Electronic Evidence Regulation, Article 3(18)

[37] Second Additional Protocol, Article 3(2)(c).

[38] For more information regarding the implementation of Article 18 into the national legislation of EU Member States, see the topic-specific factsheet prepared within the framework of the SIRIUS project, available at: https://www.eurojust.europa.eu/publication/production-orders-under-article-18-budapest-convention-cybercrime-and-extraterritorial.

[39] The answers received from one EU Member State have been excluded, as they were inconclusive.
[40] Article 18 of the Budapest Convention and Article 7 of the Second Additional Protocol.

[41] In the case of European Production Orders to obtain subscriber data or to obtain data requested for the sole purpose of identifying the user, see Electronic Evidence Regulation, Article 4(1)(a)-(b).

[42] Within the EU, an MLA process must be followed when requesting data from Denmark and Ireland.

[43] 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.

[44] 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.

[45] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[46] 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

[47] Available at: https://curia.europa.eu/juris/documents.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=C-178%252F22&for=&jge=&dates=&language=en&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&avg=&lgrec=en&page=1&lg=&cid=2837985.

[48] Opinion of the Advocate General, paras. 21-31, 40, 42. Full text of the opinion is available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=274432&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2837985

[49] Available at: https://curia.europa.eu/juris/documents.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=C-470%252F21&for=&jge=&dates=&language=en&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&avg=&lgrec=en&page=1&lg=&cid=2845080.

[50] See Order of the Court, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=272062&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=2845080 (only in French).

[51] See Proposal for an e-Privacy Regulation, available at: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation. The proposal published on 10 January 2017 does not include any specific provisions in the field of data retention, however proposals have been made for the inclusion of an explicit provision on data retention in Article 7(4). At the time of writing, the negotiations are on standby.

[52] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

[53] https://www.eurojust.europa.eu/news/dismantling-encrypted-criminal-encrochat-communications-6-500-arrests-900-eur-seized

[54] https://www.eurojust.europa.eu/news/new-major-interventions-block-encrypted-communications-criminal-networks

[55] https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

[56] Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=251302&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=33220

[57] Airbnb, Apple, Microsoft, Yahoo and X (formerly known as Twitter) have been removed from the analysis in comparison with previous editions of this report, because their transparency reports for the full year of 2022 had not been published as of 9 October 2023, when the draft of this document has been finalised.

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

[59] Electronic Evidence Regulation, Article 4.

REFERENCES

All links were accessed in September 2023.

- 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://www.redditinc.com/policies/transparency?_ga=2.6477810.1955032930.1679335409-1865029628.1677515303
- Snap Transparency Report, https://www.snap.com/en-US/privacy/transparency
- TikTok Information Request Report, https://www.tiktok.com/transparency/en/information-requests-2022-2/

ACRONYMS

AI	Artificial Intelligence
AR	Augmented Reality
CJEU	Court of Justice of the European Union
DSA	Digital Services Act
EDR	Emergency Disclosure Request
EIO	European Investigation Order
EJCN	European Judicial Cooperation Network
EJN	European Judicial Network
EU	European Union
GDPR	General Data Protection Regulation
IP	Internet Protocol
MLA	Mutual Legal Assistance
OSINT	Open Source Intelligence
SP	Service provider
SPoC(s)	Single Point(s) of Contact
UK	United Kingdom of Great Britain and Northern Ireland
UN	United Nations
US	United States of America