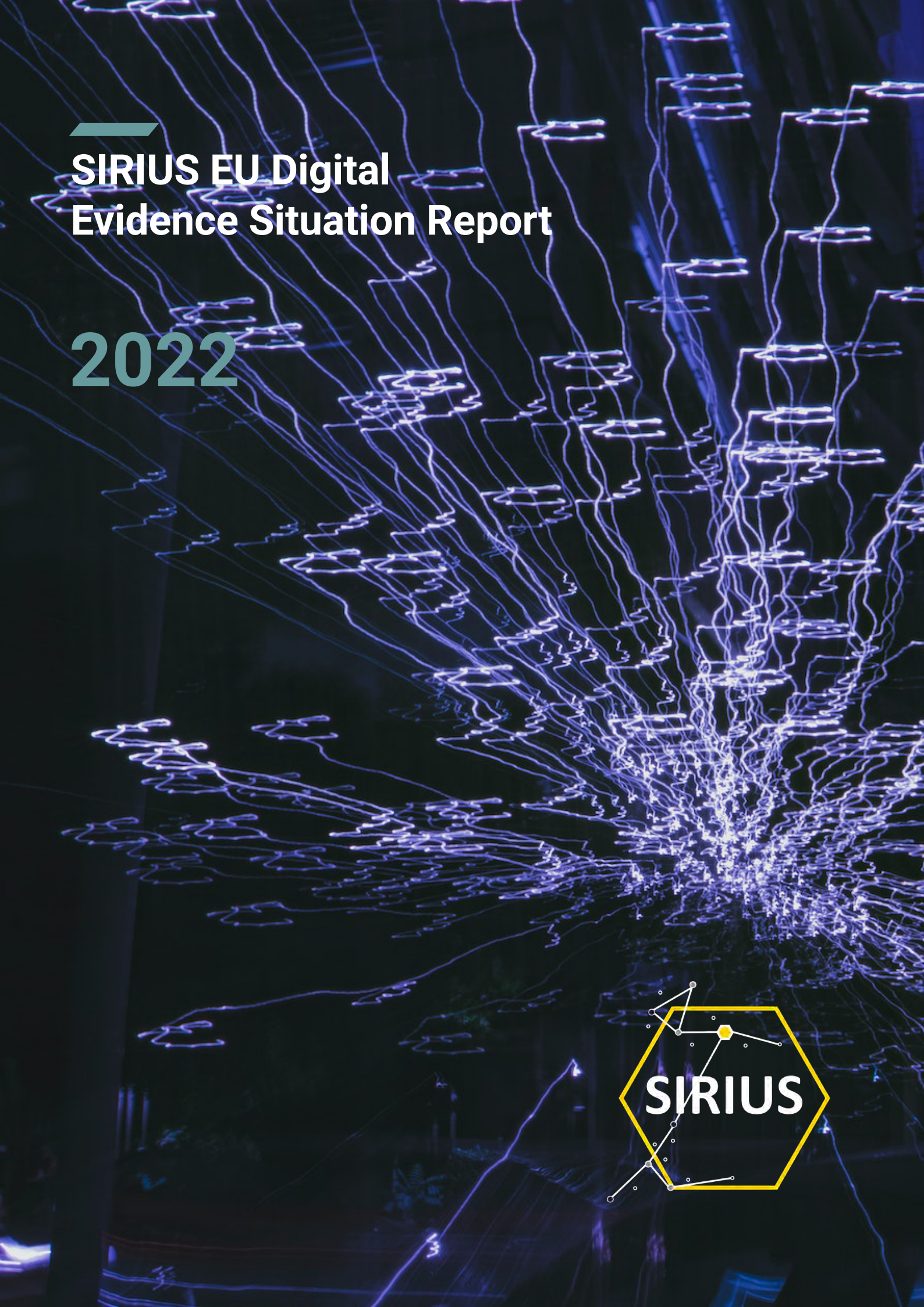
SIRIUS EU Digital Evidence Situation Report

2022



EUROPOL

EUROJUST
CRIMINAL JUSTICE ACROSS BORDERS 2002–2022

EUROPEAN JUDICIAL NETWORK
Connecting Justice

4TH ANNUAL SIRIUS EU DIGITAL EVIDENCE SITUATION REPORT

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

INDEX

INDEX 3

EXECUTIVE SUMMARY 6

KEY FINDINGS 8

INTRODUCTION 9

About the SIRIUS Project 9

Context 9

Methodology 10

PERSPECTIVE OF LAW ENFORCEMENT 13

A. Success cases 13

B. Engagement of EU law enforcement with foreign-based Online Service Providers 14

C. Submission of cross-border requests 16

D. Issues encountered by EU law enforcement 19

E. The relevance of Online Gaming Platforms in criminal investigations 20

F. The impact of the metaverse on electronic evidence 21

G. Feedback from LEAs about SIRIUS 22

H. Electronic evidence for law enforcement in non-EU countries 23

PERSPECTIVE OF JUDICIAL AUTHORITIES 26

A. Success cases 26

B. Cross-border requests for data disclosure 26

C. Challenges encountered by EU judicial authorities 44

D. Judicial cooperation 47

E. Implications of cost reimbursement 51

F. Data retention and data preservation 53

G. The long-lasting impact of the COVID-19 pandemic on the acquisition of electronic evidence 56

H. The European Judicial Network perspective: key elements for the MLA request for the electronic evidence in hate crimes 57

PERSPECTIVE OF ONLINE SERVICE PROVIDERS 60

A. Volume of data requests per country and per Online Service Provider 60

B. Volume of Emergency Disclosure Requests per country and per Online Service Provider 61

C. Success rate of EU cross-border requests for electronic evidence 62

D. The experience of Online Service Providers with Single Points of Contact 63

E. Reasons for refusal or delay in processing direct requests for voluntary cooperation issued by EU authorities 65

F. Existing and future challenges from the perspective of Online Service Providers 67

RECOMMENDATIONS 70

A. For EU Law Enforcement Agencies 70

B. For EU Judicial Authorities 70

C. For Online Service Providers 71

ENDNOTES 73

REFERENCES 74

ACRONYMS 74

Catherine De Bolle

EXECUTIVE DIRECTOR, EUROPOL

Europol, Eurojust and the European Judicial Network publish together the 2022 edition of the SIRIUS European Union Digital Evidence Situation Report. This report includes the results of SIRIUS' large-scale research delving into the complexity of cross-border investigations involving electronic evidence.

It provides valuable information from exclusive interviews and surveys conducted with Member States' competent authorities as well as Online Service Providers (OSPs) on their experiences accessing cross-border electronic data.

The report confirms that the need to access cross-border digital evidence continues to be on the rise. On a practical level, this translates into the exponential growth of data requests from EU competent authorities to OSPs in the context of criminal investigations. This in turn has resulted in SIRIUS becoming the leading source for support for EU law enforcement officers in matters related to electronic evidence. It is clear that while significant improvements have taken place over the last few years in this field, challenges remain.

Our work doesn't stop here. For our current success to have an even stronger hold in the future, it is imperative to observe, reflect and act on how transformative online technology (including the use of Artificial Intelligence, Augmented Reality and Virtual Reality), and ever changing legal landscapes will affect the manner in which Member States' handle electronic evidence. To do so, Europol will continue to work with its partners on EU and Member State levels as well as in the private sector to advance technological, legal and policy expertise among the law enforcement community.

Ladislav Hamran

PRESIDENT, EUROJUST

In an age in which our lives move increasingly online, SIRIUS has established itself as the EU's central knowledge hub on cross-border access to electronic evidence. Its work on bringing together judicial practitioners from EU Member States, prosecutors and judges from partner countries and private sector representatives lays the much-needed groundwork for strengthening the mutual trust international judicial and police cooperation so heavily relies on.

Eurojust proudly contributes to the project, in the knowledge that we share the goal of building bridges between jurisdictions. Among many other observations, this fourth Situation Report reflects a clear need for knitting a closer judicial fabric across borders. How can prosecutors and police authorities reach out to online service providers for evidence and information, and what can they expect? How can judicial authorities benefit more from the exchange platform SIRIUS has to offer?

To help answer these questions and many more, SIRIUS's work sits within Eurojust very naturally. As we navigate tomorrow's world of cross-border judicial cooperation, I have no doubt that SIRIUS will help chart our course. In addition to the trainings, guidelines and practical tools the project offers, its analytical work on trends in collecting e-evidence and on reconciling differing legislative frameworks will continue to inform policy makers and practitioners alike.

Didier Reynders

EU COMMISSIONER FOR JUSTICE

I'm delighted to welcome the annual SIRIUS EU Digital Evidence Situation report. This is an invaluable tool for anyone with an interest in the use of electronic evidence in criminal investigations, particularly policymakers. SIRIUS provides relevant and user-friendly, practical resources, such as specific guidelines, an up-to-date contact book listing over 1000 Online Service Providers (OSPs), and analyses of relevant policy developments of digital tools to assist national investigations. In 2021, there were significant improvements in competent authorities' access to electronic evidence stored by OSPs, especially in cross-border cases. This report finds a high level of awareness of existing processes among EU law-enforcement officers, leading to better quality requests to OSPs and higher use of online portals. This is excellent news in the fight against crime. Combatting crime in the 21st century requires the efficient use of all available technology.

EXECUTIVE SUMMARY

Online services are a cornerstone of everyday life for the majority of European Union (EU) citizens. Digital platforms also play a significant part in criminal activities and, therefore, it is not surprising that electronic datasets very often become crucial investigative leads. As a consequence, many criminal investigations in the EU quickly acquire an international dimension as soon as authorities need to make cross-border requests for data disclosure to Online Service Providers (OSPs) established in different countries. While policy developments to modernise applicable legal instruments are ongoing, authorities still rely on long judicial procedures or on the voluntary cooperation of OSPs to access such data. In this context, this report looks back at the situation of the use of digital data in criminal investigations in 2021, presenting comprehensive perspectives of international stakeholders.

From a law enforcement perspective, there is a growing concern that the rapid advancement of Artificial Intelligence (AI) and Virtual/Augmented Reality (VR, AR) technologies will require major transformations to effectively investigate crime. While acknowledging these future challenges, most EU law enforcement officers reported being satisfied with the engagement level with OSPs in 2021. At the same time, most of them agree that **non-content data continues to be more important than content data in the majority of cases, but not all.** The length of judicial processes and the lack of standardised policies of OSPs remain the main issues, while the relevance of Online Gaming Platforms (OGPs) is stable, with one quarter of EU law enforcement agencies seeking data from such companies last year.

From the perspective of judicial authorities, judicial cooperation instruments (Mutual Legal Assistance (MLA) and European Investigation Orders (EIOs)) are the main mechanisms for obtaining electronic evidence across borders. While one of the main issues faced by EU judiciary when obtaining electronic evidence across borders in 2021 is **the length of the MLA process**, the extracts of national legislation and the examples of practices shared by the surveyed EU judiciary demonstrate the efforts of the EU Member States to look for alternatives for obtaining electronic evidence from foreign-based OSPs. Even though the Second Additional Protocol to the Budapest Convention on Cybercrime has not yet come into force, this report demonstrates that several EU Member States have already implemented some of its measures in their domestic legislation. Another pressing and ever-recurring issue faced by EU judicial authorities trying to obtain data across border is t**he lack of a data retention framework**. In order for authorities to be able to obtain access to electronic data, such data must be available in the first place. The current legislative gap at the EU level on data retention in the frame of criminal proceedings leads to the loss of data. Therefore, EU judicial authorities are looking forward to EU-wide legislative efforts to regulate data retention for the purposes of

criminal procedures, which would enable them to more successfully fight crime.

Finally, from the perspective of the majority of the interviewed OSPs, there were significant improvements in the process of engaging with EU competent authorities in the context of criminal investigations in recent years. For instance, according to most OSPs, there is currently a high level of awareness among EU law enforcement officers regarding existing processes. This awareness leads to a better quality of requests as well as to a higher acceptance of the use of online portals. This is particularly true in law enforcement agencies that have established a Single Point of Contact (SPoC) approach, as these units act as quality filters for data requests under voluntary cooperation. Furthermore, **there was a 36% increase in the volume of requests to OSPs in 2021**, while the number of Emergency Disclosure Requests (EDRs) increased by 29%.

The last chapter of the report presents recommendations to improve the process of cross-border requests for electronic evidence in criminal investigations, with a focus on security and efficiency.

For EU Law Enforcement Agencies:

- Create or expand the capacity of units acting as SPoCs for cross-border data disclosure requests under voluntary cooperation;
- Include training on cross-border access to electronic evidence in routine training programmes for investigators and first-responders;
- Ensure the security of e-mail systems, including the obligatory use of strong passwords and two factor authentication to all law enforcement officers.

For EU Judicial Authorities:

- Strengthen capacity on different modalities and specific procedures for requesting and obtaining electronic data;
- Enhance mutual trust, exchange of expertise and best practices among EU judicial practitioners on cross-border access to electronic evidence.

For OSPs:

- Take measures to identify and prevent fake requests for data disclosure from unauthorised persons;
- Engage in international events organised by SIRIUS and share policy updates with the SIRIUS Team;
- When launching new products and services, especially in relation to AI, AR and VR, consider their impact on electronic evidence.

KEY FINDINGS

The SIRIUS platform remains the **highest ranked source of information** for law enforcement seeking assistance to prepare direct requests

Among law enforcement there is a **growing concern that rapid advancement of AI, VR and AR will require major transformations** in investigating crimes

A clear tendency emerged — the lack of an EU-wide data retention framework for the purpose of criminal investigations and prosecutions remains the core issue for EU judicial authorities when requesting digital data from other EU Member States

Constant training on the different modalities for requesting and obtaining cross-border data disclosure **is essential** for the EU judiciary to ensure proper awareness, knowledge and skills

Non-content data continues to be more important than content data in the majority of investigations in 2021

In 2021 there was an **overall 36% increase in the volume of requests to OSPs**, while the number of Emergency Disclosure Requests increased by 29%

INTRODUCTION

About the SIRIUS Project

The SIRIUS Project is the centre of reference for knowledge-sharing in the area of electronic evidence for EU law enforcement and judicial authorities. The main objective of the SIRIUS Project is to contribute to faster and more effective cross-border access to electronic evidence stored by OSPs in the context of criminal investigations. To that end, the project offers relevant and practical resources to competent authorities, ranging from specific guidelines, an up-to-date contact book with the contact details of over 1000 OSPs, and analyses of relevant policy developments to digital tools to assist in investigations. Furthermore, SIRIUS experts organise international in-person and virtual events, provide face-to-face training and awareness-raising sessions in EU Member States, and promote valuable opportunities for over 6000 practitioners to learn and share best practices with each other.

The project also has a stream of work to support interested OSPs in setting up or expanding their capacity to deal with requests for data from EU authorities and coordinates a network of SPoCs for matters related to the voluntary cooperation in 22 countries. The experts in the SIRIUS team maintain close cooperation with numerous OSPs worldwide through intensive outreach efforts, as well as collaborate with many international organisations working in the same field. The SIRIUS Project is led by Europol and Eurojust, in close partnership with the European Judicial Network (EJN). The project receives funding from the European Commission's Service for Foreign Policy Instruments since 2018 and its current cycle is set to continue until June 2024.

Context

As almost every criminal activity nowadays features an online component, digital data held by OSPs is essential to nearly all criminal investigations into any crime area. User data that is not publicly available, such as connection logs, IP addresses, contact details or payment data, may be key elements for competent authorities to investigate and prosecute criminal offences or save lives in imminent danger. Given the global and borderless nature of the internet, requesting such data from OSPs often involves the need to engage with legal entities based abroad. Consequently, domestic investigations acquire an international dimension, with national authorities facing the need to make international requests for data disclosure, even if all other circumstances of the investigation are domestic.

Formal legal requests for data may be submitted by the authorities of one country to the competent authorities where the relevant OSP is based, pursuing provisions established under bilateral or multilateral treaties. To obtain data via formal procedures, 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.

However, these mechanisms are often considered not to be adequately suited to obtaining digital evidence. Because of this, direct requests from competent authorities to foreign-based OSPs for the disclosure of non-content data under voluntary cooperation have become an alternative channel for access to relevant data in criminal investigations. The authorities of countries which have implemented Article 18 of the Budapest Convention on Cybercrime into their national legislation may opt to issue extraterritorial production orders for subscriber data addressed to OSPs not necessarily present, but offering their service within the territory of a country.

Furthermore, the invalidation of the Directive 2006/24/EC[1] (Data Retention Directive) and limiting the scope of the national data retention legal frameworks by Court of Justice of the European Union (CJEU), has left law enforcement and judicial authorities uncertain about the possibilities to obtain data from private companies.[2] As reiterated by the surveyed EU judiciary – the lack of an EU-wide data retention framework for the purpose of criminal investigations and prosecutions remains the key challenge when requesting digital data from other EU Member States.

From a policy perspective, two main developments which took place in 2021 are worth noting. First, the adoption of the Second Additional Protocol to the Cybercrime Convention (commonly known as Budapest Convention) in November 2021[3] – coinciding with the 20th anniversary of the adoption of the Budapest Convention. Among other measures, the Protocol sets out a much needed clear legal basis for the issuance of extraterritorial production orders (Articles 6 and 7) and procedures for expedited cooperation in emergency situations. The Protocol was opened for signatures in May 2022, and will come into force once it has been ratified by at least 5 States. Second, at the EU level, in November 2022 the co-legislators reached a provisional political agreement on the e-evidence package, hopefully leading to its formal adoption in the future.[4]

Methodology

This report has been developed on the basis of the information collected from publicly available sources, as well as from exclusive interviews and surveys conducted with competent authorities and OSPs, as described below.

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

The transparency reports analysed for the purpose of this report were: **Google, LinkedIn, Meta, Microsoft, Snap, TikTok and Twitter.** The numbers presented in this report for the years 2018 – 2020 differ from the results presented in previous reports, as Airbnb, Apple and Yahoo have been removed from the analysis, as they had not yet published their report for 2021 at the time this document has been drafted.

B. Online surveys with law enforcement

Europol conducted a survey amongst law enforcement agencies and collected 235 responses from representatives from all EU Member States, from April to June 2022.

For the first time, the same survey was open also to law enforcement authorities from non-EU Member States which have operational or working agreements with Europol. 32 responses were received from Albania, Bosnia and Herzegovina, Canada, Iceland, Japan, Montenegro, Norway, Serbia, Switzerland, United Kingdom (UK) and United States of America (US). 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.

C. Online surveys with judicial authorities

Eurojust has collected feedback from the judicial community of EU Member States, third countries with a Cooperation Agreement with Eurojust and one third country with which the SIRIUS Project has developed strong cooperation outside of the framework of official agreement. A survey was administrated from April to June 2022, reaching out to the judicial community on the SIRIUS Platform, as well as European Judicial Cybercrime Network (EJCN) and EJN contact points. In total, 53 in-depth responses were received reflecting the situation in 25 EU Member States[2], Georgia, Republic of Moldova, Switzerland and Japan. The compilation of this information forms the basis for the analysis and recommendations presented in this report.

This report also represents the up-to-date experience of judicial authorities in gathering electronic evidence, focusing particularly on the area of hate crimes and judicial cooperation with the US.[6] References to experiences from practitioners from EU, Switzerland, Japan and US as shared at the 58th Plenary meeting of the EJN under the French Presidency, and EU Member States' conclusions based on those discussions, are weaved into this report.

D. Interviews with OSPs

Europol and Eurojust interviewed representatives from Airbnb, Discord, GitHub, Google, Meta, Microsoft, Roblox, Snap, TikTok, Twitter, Uber, WhatsApp and Zoom between April and July 2022. The findings presented in this report should not be taken as the official formal position of any of the mentioned private entities.

The main topics discussed with these companies were:

- Main reasons for refusal or delay in processing requests for data from EU authorities in criminal investigations;
- SPoCs approach for cross-border data disclosure requests under voluntary cooperation;
- Need for Emergency Points of Contact in EU Member States for proactive reports;
- Impact of recent policy developments in the area of electronic evidence; and
- Future challenges in the area of cross-border data disclosure requests.


"verifier":
"followers_
"friends_
"listed_
"favourites_
"statuses_
"created_at":
"utc_offset":

PERSPECTIVE OF LAW ENFORCEMENT

A. Success cases

EU law enforcement officers were invited to share examples of successful investigations involving the use of electronic evidence in 2021. Without disclosing any operational details, the testimonies below demonstrate how the availability of relevant user data in investigations or emergency situations is indispensable:

Terrorism

- *Last year, we dealt with a suspect terrorist who was sending threatening e-mail[s] and letters to local industries and businesses. One of the e-mails used by the organisation was a Gmail. So, being a SPoC and after performing forensic e-mail analysis, I submitted a legal request to Google and within a couple of hours I received all the data I needed to identify my suspect, like phone number, IP of registration and so on. We then performed a domicile search and found additional evidence.*
- *The administrator of multiple accounts on internet platforms radicalised people from [Region] and [Country]. He was identified using the data recovered via direct requests for voluntary cooperation to OSPs and was later arrested in [City]. He shared public calls for fighting, shared the insignia of terrorist organisations and quotes from the leaders of terrorist organisations.*

Sexual abuse

- *In the investigation of two crimes of sexual abuse through the internet, the IP connection information provided by Google and Instagram were essential for the identification of the perpetrator.*

Fraud

- *In a successful investigation related to fraudulent online investment platforms, the electronic evidence (BSI, billing information and admin connection logs) provided on a voluntary basis by the foreign hosting provider played a key role.*
- *I request data from companies all over the world on a daily basis. Recently, in cooperation with Coinbase, we were able to uncover a big fraud scheme, for example.*

Money laundering

- *Data from Binance has contributed towards a successful money laundering investigation.*

Sextortion

- *In a case concerning sextortion, direct requests for voluntary cooperation were sent to PayPal and Facebook in order to receive relevant data from specific users.*

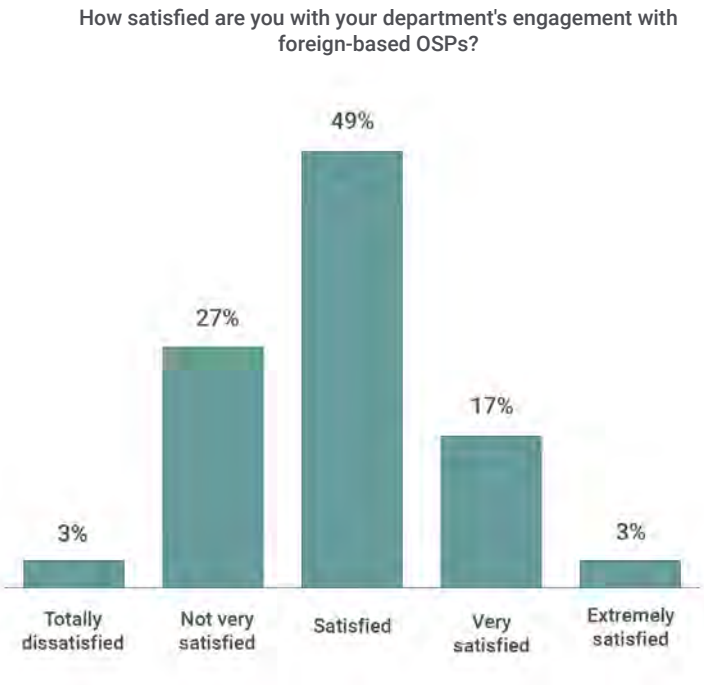
The data disclosed by these companies led to the detention of the offender and the identification of other victims as well.

Bomb threat

- *In connection with a bomb threat, we received a quick response from Google relating to a user of one Gmail account.*

Crime area not informed

- *Just about in all the cases I handle, obtaining electronic evidence is essential.*
- *In a violent crime case, we needed to identify a suspect. We had reason to believe he was the user of a specific Instagram account, which we found on the device from another suspect. Thanks to a direct request under voluntary cooperation, Meta provided us several months of IP log[s], with IPv4 and IPv6 and we could identify and locate the suspect.*



B. Engagement of EU law enforcement with foreign-based Online Service Providers

For EU law enforcement, the most common approach to accessing non-content data needed in criminal investigations is requesting it directly from foreign-based OSPs under voluntary cooperation.

The requesting authority must always comply with domestic regulations, while also observing the policies and requirements set by the OSPs themselves. For instance, OSPs may require the use of dedicated portals, or the submission of requests in specific templates or languages. They may also require information on the nature of the case, a clear reference to the national legal basis for the issuance of the request or the specification of narrow timeframes for the data sought.

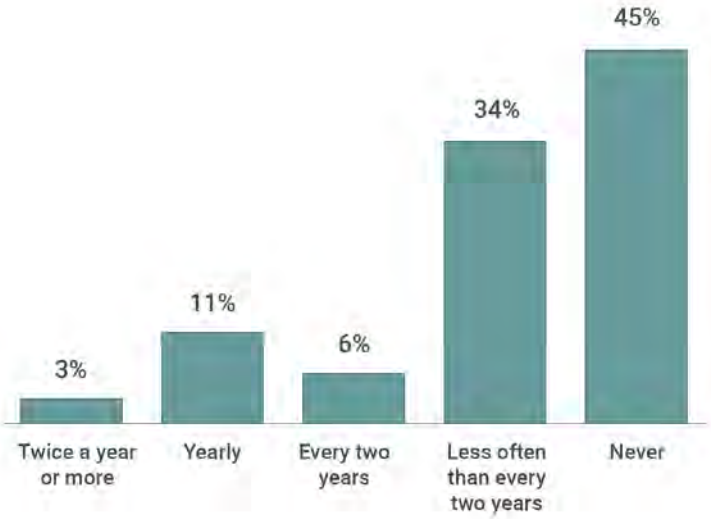
Despite the known challenges and limitations of existing processes, about 70% of EU law enforcement officers reported being satisfied with their department's engagement with OSPs in 2021. This represents an increase of almost 4% in relation to the previous year, indicating a positive trend in the engagement of EU law enforcement with OSPs in the context of criminal investigations.

A narrow majority of EU law enforcement officers have received training in matters related to cross-border access to electronic evidence to date. The percentage of untrained officers is still very high, considering that the importance of digital data in criminal investigations continues to increase. 45% of

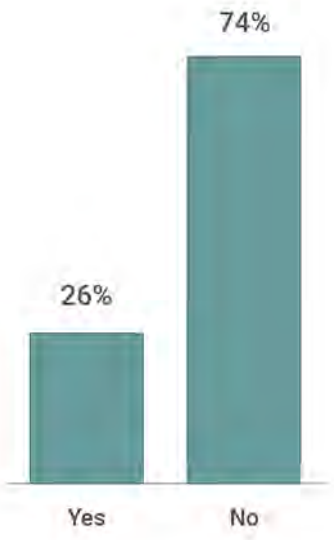
EU law enforcement officers reported that they never received any training regarding cross-border requests for electronic evidence.

26% of EU law enforcement officers have security limitations on their main work computer that block - partially or entirely - access to some online services, such as social media platforms. Officers report such limitations in 18 EU Member States (Austria, Belgium, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, Netherlands, Poland, Romania, Slovenia, Spain and Sweden). The blocking of websites leads to difficulties in investigating crime on online platforms and may also impede officers from accessing portals of OSPs, which are dedicated to the submission of requests for data. When relevant websites are blocked on their main work computer, officers need to use alternative work devices or work in contact with IT departments.

How often do you receive training regarding cross-border requests for electronic evidence?



Does your department block access to some online services - such as social media - on your main work computer?



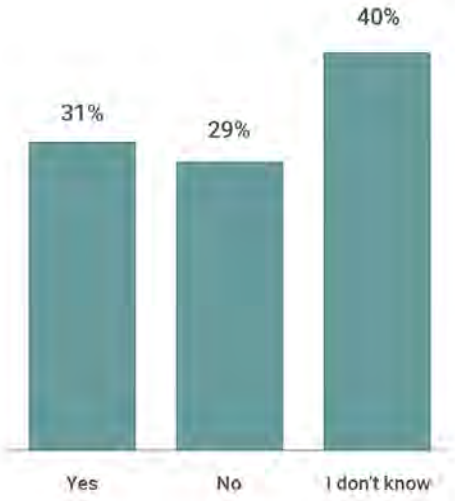
C. Submission of cross-border requests

Direct requests to foreign-based OSPs under voluntary cooperation continue to be widely used in the EU. 63% of officers indicated direct requests as the main approach during criminal investigations within their department in 2021. Judicial cooperation via MLA or EIO was indicated by 19% of respondents, while 8% indicated the use of EDRs as the main type of request for data in their investigations in the same period.

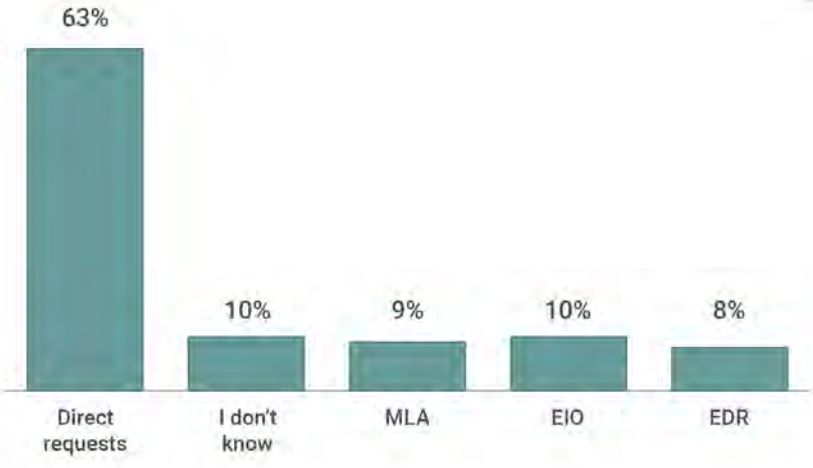
The use of the 24/7 Network established under the Budapest Convention increased by almost 7% from 2020 to 2021, with 31% of respondents indicating their department successfully submitted cross-border data disclosure requests via this channel. The lack of knowledge regarding the use of the 24/7 Network however still remains high at 40%.

In the majority of criminal investigations in the EU, non-content data is considered more important than content data. Officers indicated that connection logs, name and IP address used at registration are the three most important datasets in their investigations. Connection logs (list of date, time and IP address used to connect to a specific service) can lead to important information such as the use of the service and potentially indicative location, based on the IP address. Only 17% of officers indicated content data as the most important type of data in 2021, which is 3% less than in 2020.

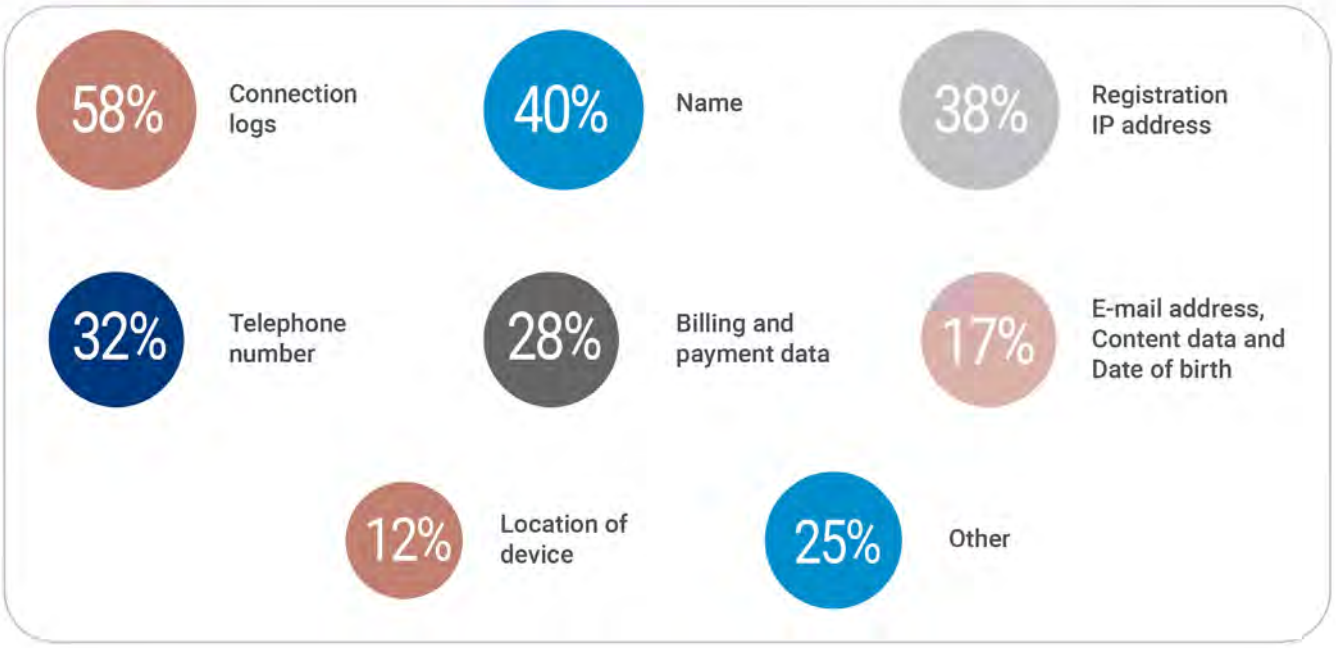
Has your department successfully submitted cross-border data disclosure requests via the 24/7 Network established under the Budapest Convention?



What type of request to OSPs was used the most in the criminal investigations you participated this year?

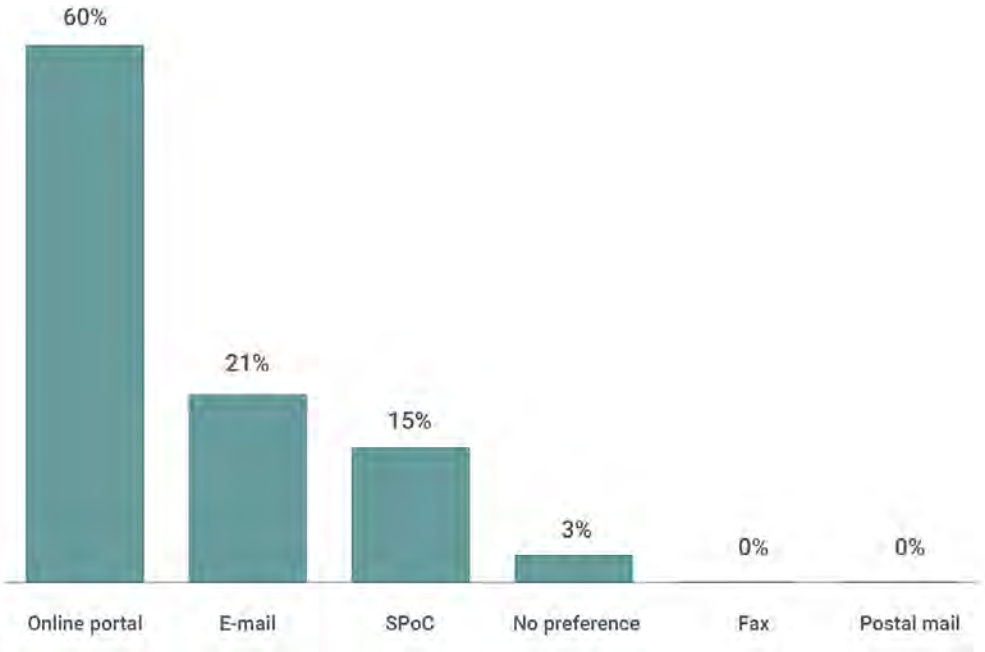


In the majority of the investigations, what are the most important types of data your department needed? (up to three choices allowed)

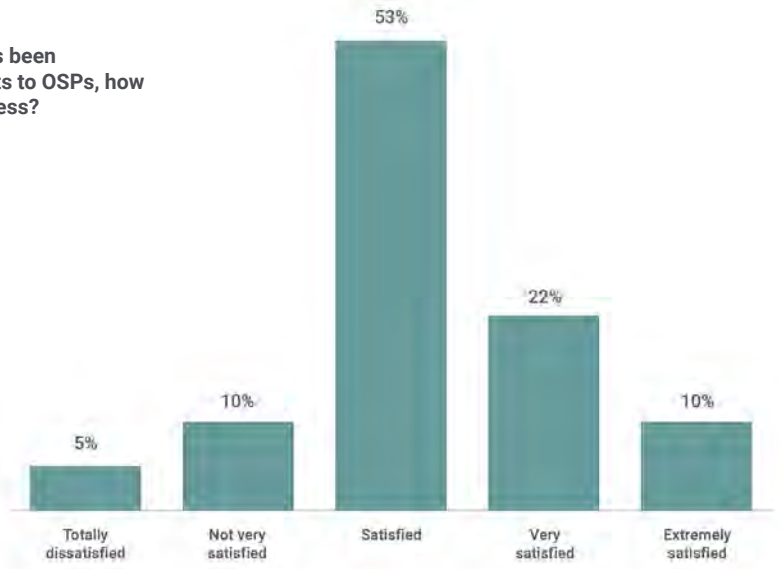


The use of online portals for the submission of direct requests for data disclosure to OSPs under voluntary cooperation remains the preferred channel, after an increase in popularity during the pandemic in 2020[7]. Such portals are available for several OSPs, including most of the large ones[8]. Their use is generally considered beneficial for streamlining the process, ensuring that all the required information is included, as well as for allowing the tracking of a request and submitting specific inquiries or additional information in relation to it. E-mail is the preferred channel for 21% of officers and SPoCs were indicated as the preferred channel by 15% of the respondents.

What is your preferred channel for submission of direct requests to OSPs?



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

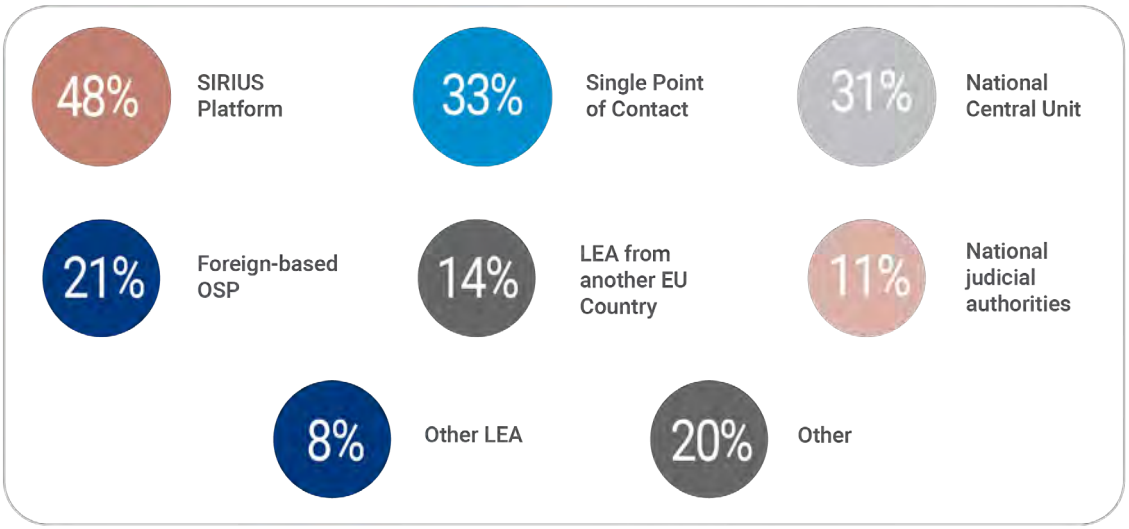


Among the officers that indicated that there is a unit acting as a SPoC within their agency, 85% indicated they are satisfied or more than satisfied with their processes to channel requests to OSPs in a centralised manner.

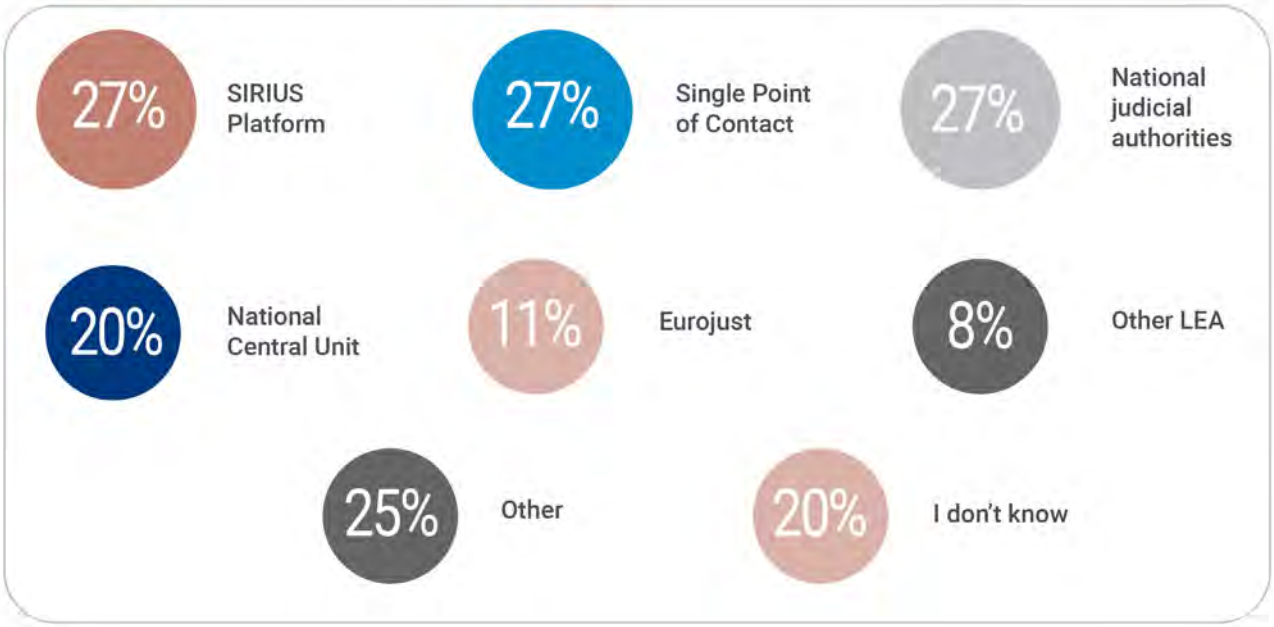
The SIRIUS Platform is the leading source of information for EU law enforcement officers who need assistance preparing direct requests to OSPs under voluntary cooperation, or to initiate MLA requests which are dealt with by the judicial authorities. SIRIUS is a restricted environment accessible only to law enforcement and judicial authorities, and enables access to knowledge-based resources on cross-border access to electronic evidence, as well as contact details of over 1000 OSPs worldwide. SPoCs were considered second-best by 33% of the respondents, and in third place Law Enforcement National Central Units, indicated by 31% of the respondents.

The SIRIUS Platform also appears as the leading source of information for EU law enforcement officers in matters related to MLA in 2021, tied with SPoCs and National Judicial Authorities.

In case your department needed assistance to prepare direct requests to OSPs, who did you consult? (up to three choices allowed)



In case your department needed assistance to prepare Mutual Legal Assistance requests, who did you consult? (up to three choices allowed)



D. Issues encountered by EU law enforcement

The main issues faced by EU law enforcement officers in the process of requesting access to cross-border electronic evidence are not new. The fact that the MLA process takes too long and the differences in the policies of OSPs with regard to responding to requests for information from authorities remain the two biggest issues for EU law enforcement officers, as indicated also in previous editions of this report. Other issues indicated by more than 30% of officers are the fact that OSPs usually provide only partial answers or take too long to reply. Moreover, 18% of respondents mentioned the short retention periods for digital data as their main issue, while 17% faced difficulties in locating the contact details of OSPs and 12% could not find OSPs' guidelines for law enforcement. Finally, 12% or less of law enforcement officers consider the following issues to be the main ones:

- Difficulties in identifying which set of data can be requested from companies;
- Requests are usually only accepted in English, not in their own language;
- Lack of technological resources to analyse responses from service providers;
- Companies' responses are not easy to analyse and understand;
- Companies change processes and response formats too often;
- Information is only available in English, not in their own language; and
- Companies' guidelines are too complicated or too long.

Only 3% of respondents replied that they encountered no problems in the process of requesting digital evidence from foreign-based OSPs in 2021.

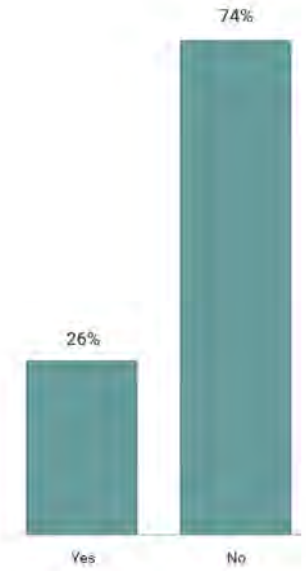
What are the main issues your department encountered in requests to foreign-based OSPs? (up to three choices allowed)

E. The relevance of Online Gaming Platforms in criminal investigations

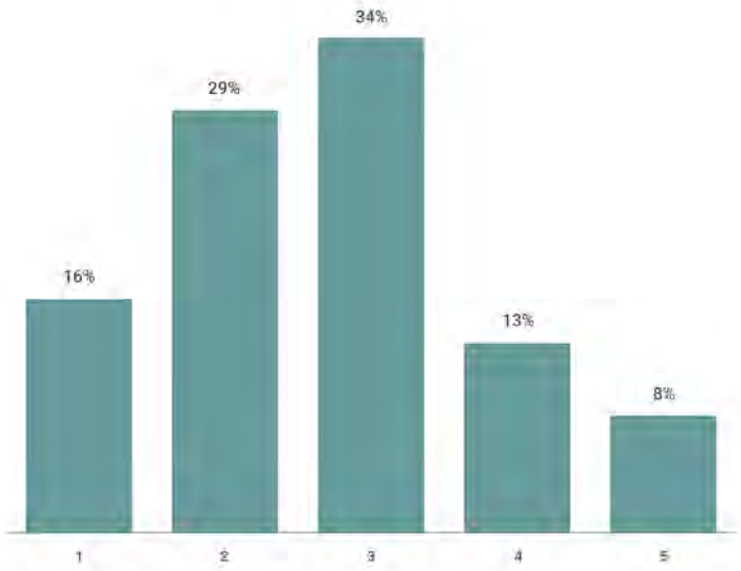
Engagement with OGPs for criminal investigations purposes remained mostly stable since the first study conducted in 2020. Around 25% of EU law enforcement officers mention that their department submitted requests for disclosure of electronic evidence to OGPs during the last three years. The stability in terms of engagement with OGPs is in contrast with an increase in criminal activity that exploits and abuses such platforms, for example in cases of online grooming, financial fraud or the dissemination of right-wing terrorist propaganda[9].

Among the law enforcement officers who replied that their department engaged with OGPs in 2021, only 21% attributed a high relevance of these services in criminal investigations. The apparent low relevance of OGPs in criminal investigations may be due to the type of services provided by these companies that only allow for limited interaction among users, usually in small groups. It is also possible that there is a low level of preparedness among law enforcement officers to investigate offences in OGPs and engage with the companies providing these services, given the high level of rapid innovation in this industry.

Did your department submit any requests for data disclosure to foreign-based online gaming companies?



What was the relevance of online gaming platforms in criminal investigations conducted by your department ? (1 – 'Not relevant at all' to 5 – 'Very relevant')



F. The impact of the *metaverse* on electronic evidence

Large global tech companies have recently announced investments in transformative online technology, including the use of AI, AR and VR. Many OSPs make reference to the future of tech as the creation of a metaverse, which may encompass virtually-enhanced physical and digital realities.

Law enforcement officers were invited to express their views on how future transformations in technology could affect their work in the area of electronic evidence. Officers' responses demonstrate there is growing concern that the rapid advancement of such technology will require deep transformations also among law enforcement to effectively investigate crime.

Below are some of the responses provided by EU law enforcement officers:

- *In my opinion future transformations [of technology] will lead to the emergence of new types of crime and this will lead to new types of electronic evidence.*
- *More criminal activity will be moved to these new technological areas where it might become unclear what data is gathered by the companies, how it is retained and how to obtain it.*
- *It could have a huge adverse effect. If law enforcement agencies do not keep up with advancing technology it will become very difficult to keep pace and make use of electronic evidence. In my personal opinion inadequate funding to keep pace with advancements in technology is causing issues in my agency.*
- *The use of AI is a real challenge for law enforcement. Law enforcement should invest in the training on the rapidly developing AI, otherwise a simple investigation on OSINT would become very*

difficult and maybe unreliable.

- *If we can't get data from the various OSPs (much) faster, we will continue to lag behind criminal organisations. Due to the very rapid changes in the computer world, it is difficult to keep up and we are getting pervasive individual specialisations that can hinder a unified approach.*
- *Changes in technology, especially with the use of AI, are causing an increased volume of reports on the part of providers. Law enforcement must meet this challenge by deploying technology and personnel.*

Europol's report "Policing in the metaverse: what law enforcement needs to know"[10] confirms these views, highlighting the main challenges and impacts for future investigations. For instance, the user experience in the metaverse is expected to be largely ephemeral like our interactions are in the physical world, meaning that in some cases there may be no data recorded. Moreover, the use of the metaverse is conceptually different than existing mainstream platforms, meaning that user behaviour could become more important than user generated content, posing considerable challenges for countering abuse.

G. Feedback from LEAs about SIRIUS

As indicated in Section C of this chapter, SIRIUS is a central reference point for knowledge-sharing in the area of electronic evidence for EU competent authorities. Law enforcement officers have spontaneously provided feedback on the SIRIUS Platform in their responses regarding their use of electronic evidence in criminal investigations in 2021.

Below is a compilation of some of the feedback we received:

- *SIRIUS helped me to search for current contacts of OSPs.*
- *I am following SIRIUS community on a weekly basis and sharing the information with my colleagues, even on our internal police portals. In case of Emergency Requests, it helped us a lot in the past to get to the right channel of the respective service provider.*
- *SIRIUS is just the go-to place for this kind of work. Without it I don't know where we would stand.*
- *I use the SIRIUS Platform every month to check the newest guidelines for our whole agency.*
- *The SIRIUS platform helped us to identify perpetrators of crimes and missing people. Thank you for your support.*
- *The use of the SIRIUS platform had let us know how to request some data and what kind of data for certain providers.*
- *SIRIUS really helped me to understand how to obtain electronic evidence. I have just graduated from the Police Academy and, like in any country, we did not learn many things about requesting data from outside the country. SIRIUS helped me to understand concepts like direct requests, type of data, mutual assistance, and in other words, helped me to do the job I am supposed to do and had almost no training in that sense.*
- *The SIRIUS Project is very helpful, especially for our emergency cases.*

H. Electronic evidence for law enforcement in non-EU countries

For the first time, law enforcement from non-EU countries, which have operational or working agreements with Europol, were invited to respond to the same survey used for authorities from EU Member States. SIRIUS received 32 responses from Albania, Bosnia and Herzegovina, Canada, Iceland, Japan, Montenegro, Norway, Serbia, Switzerland, UK and US.

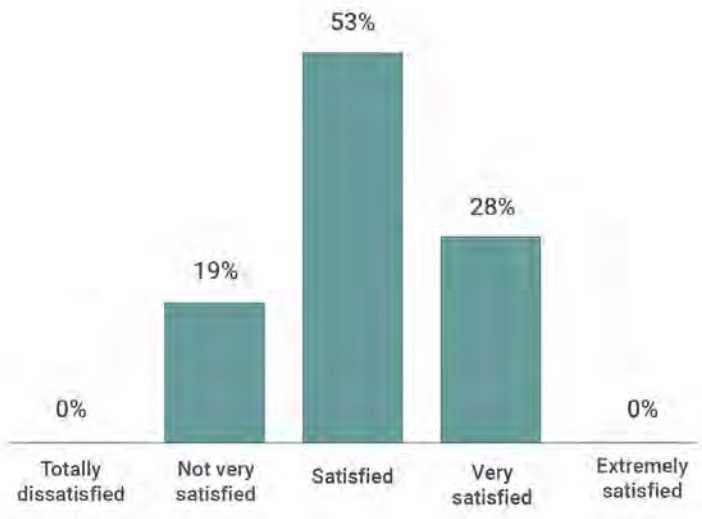
The percentage of officers from the above-mentioned countries that reported being satisfied or more than satisfied with their department's engagement with OSPs was 81%, which is 11% higher than among EU Member States.

In relation to training courses on cross-border requests for electronic evidence, there is a similar situation as in the EU, with almost half of all officers reporting never having received such training.

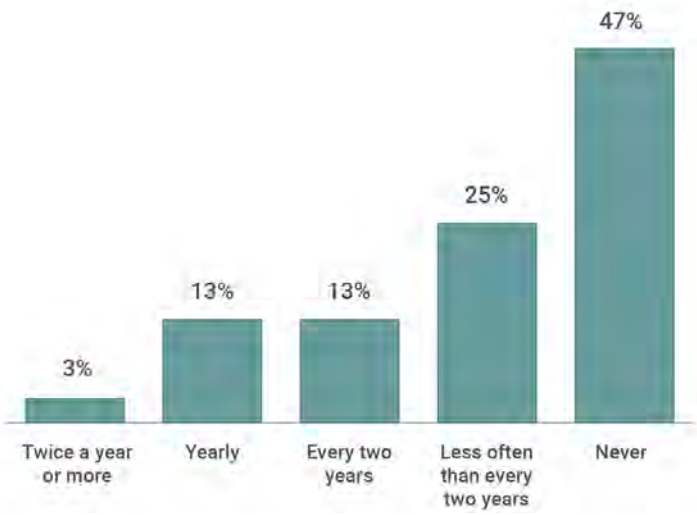
Likewise, the types of data needed in investigations in non-EU countries were also similar to the ones identified in the EU. Connection logs, IP address used at registration, telephone number and name are ranked in the top four, even though different weights are attributed to each of them. Moreover, 16% of officers from non-EU countries affirmed that content data is among the most important datasets in their investigations, which is also very similar to the results among EU law enforcement officers.

In the non-EU countries that responded to the SIRIUS survey, officers identified the same top three issues in their engagement with OSPs as in the EU. However, the fact that the MLA process takes too long seems to be an even bigger issue outside of the EU, where about 20% more officers indicated this as their main problem.

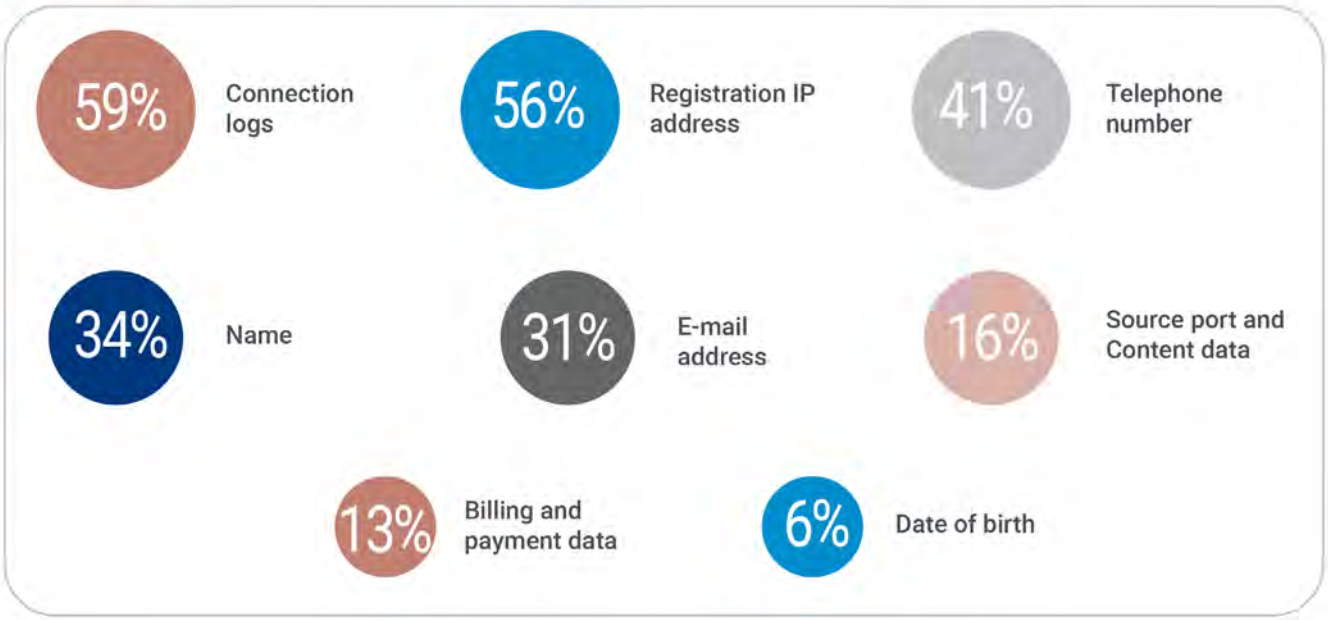
Non-EU Countries: How satisfied are you with your department's engagement with foreign-based OSPs?



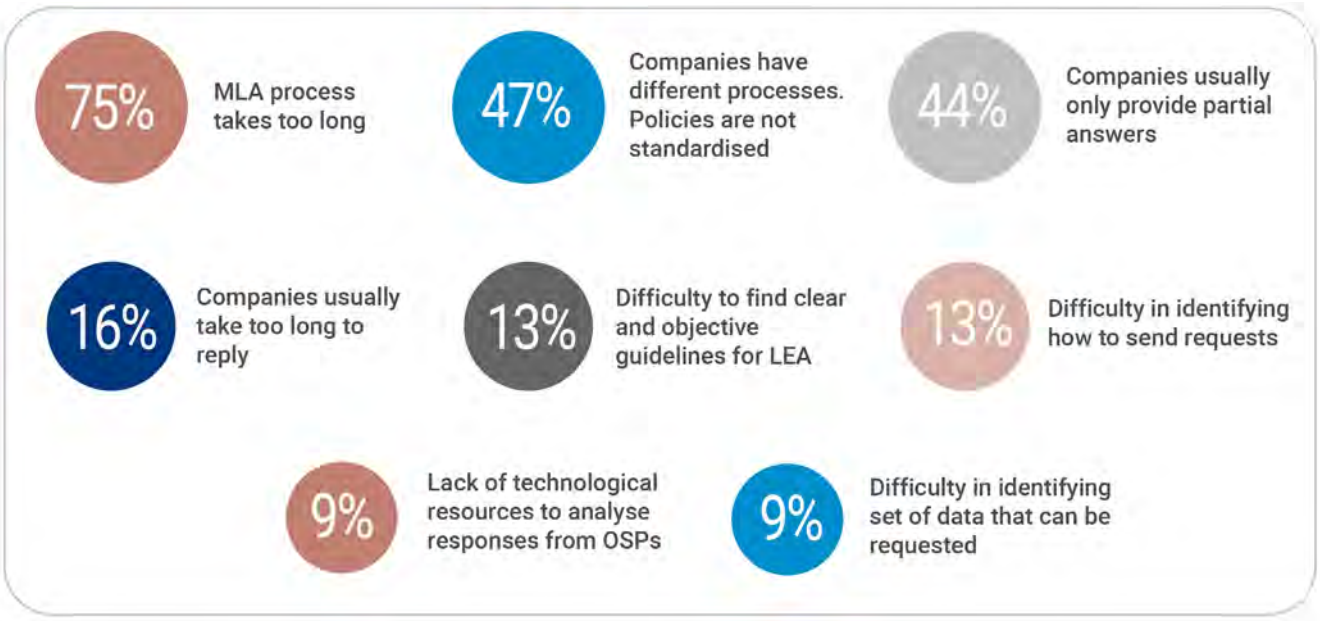
Non-EU Countries: How often do you receive training regarding cross-border requests for electronic evidence?



Non-EU Countries: In the majority of the investigations, what are the most important types of data your department needed? (up to three choices allowed)



Non-EU Countries: What are the main issues your department encountered in requests to foreign-based OSPs? (up to three choices allowed)



PERSPECTIVE OF JUDICIAL AUTHORITIES

A. Success cases

Despite the existing challenges and the continuously changing technological and legislative landscapes, the first-hand experiences collected from members of judiciary clearly show that **cooperation with private entities is vital**, both at the domestic and at the international level. The majority of the success cases mentioned by the respondents describe the cooperation with the private sector as **excellent, necessary, effective** and as an overall **positive experience**. Similarly, cooperation with colleagues across different jurisdictions is particularly relevant for effective data collection.

The role of Eurojust in facilitating the transmission of cross-border data was also mentioned by one respondent, as presented below:

- *In individual cases, the OSPs cooperate excellently and respond to requests at a short notice and without any problems. The information behaviour depends very much on the respective OSP (Germany).*
- *Colleagues in other jurisdictions are very polite, professional and easy to communicate with. Law enforcement officials do their best. However, the procedures are overly bureaucratic and do not do justice to the good work of police, prosecutors and judges (Ireland).*
- *Don't be afraid to write directly to OSP in USA, sometimes they provide necessary information without MLA (Lithuania).*
- *Companies are pragmatic and willing to find a compromise (Netherlands).*
- *In one case we have received data from France by way of Eurojust very quickly and with the use of platform for transmitting / downloading large files which was very effective (Slovenia).*
- *In the area of hate crimes, in Spain a protocol has been signed with the main ISPs, for withdrawal from the [Internet] of hate speech content constituting crime through a priority channel in which the computer crime unit acts as the direct communication channel to ISPs. Without being exactly the subject that we are dealing with, to our understanding it is a positive experience that can be transferred the scope of the delivery of certain kind of data (Spain).*

B. Cross-border requests for data disclosure

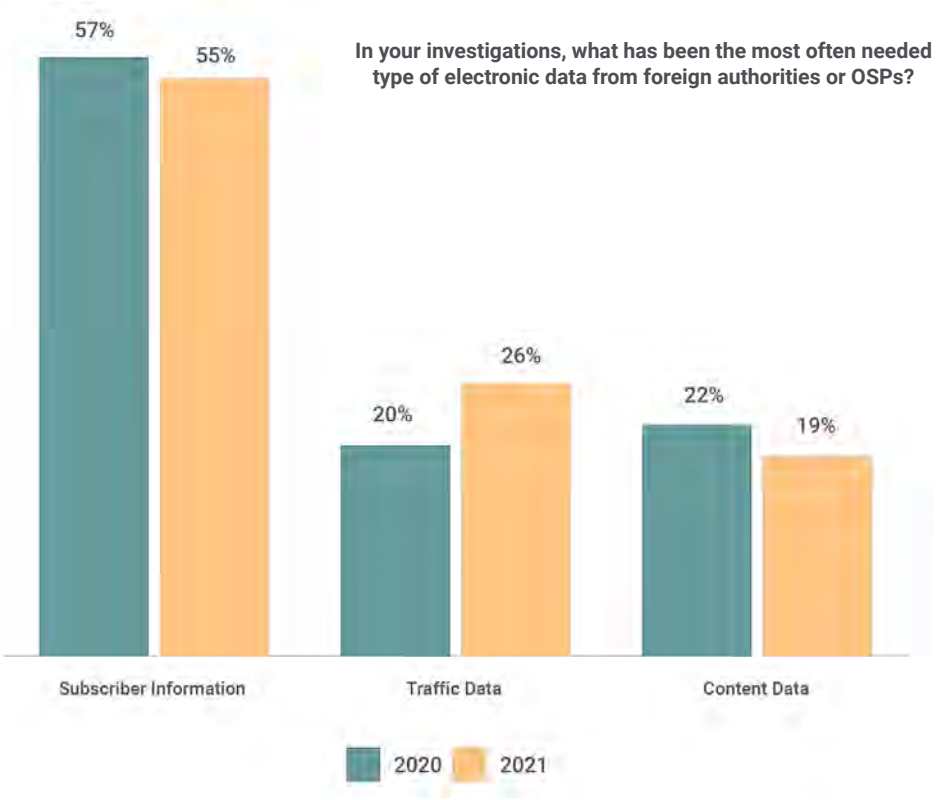
Cascading manner of requests

Electronic evidence is any information stored or transmitted in digital form, which may be used as evidence in criminal investigations or proceedings. In one way or another, such data relates to personal information related to a targeted individual. Therefore,

disclosure of such data is intrusive to an individual's personal life. Depending on the level of intrusiveness, the legal standards for accessing electronic data vary across jurisdictions.

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. This categorisation is based on an ascending level of privacy intrusion for the targeted individual[11] and refers to three categories of electronic data: subscriber information, traffic data and content data[12]. The compiled information and the first-hand experience of judicial authorities from the surveyed EU Member States and third countries indicate that requests for data disclosure take place in a cascading manner, starting from the least intrusive – namely requests for subscriber information[13], which is required in the majority of cases and often as a first step in criminal investigations involving electronic evidence – to requests for data requiring the highest level of procedural protection, namely content data, for which most often recourse to an MLA/EIO process would be required.

Subscriber information – such as name, address, e-mail or phone number of a subscriber – was the most sought after electronic data from foreign authorities or foreign-based OSPs in more than a half of the criminal investigations in 2021 (55%). The leading position of this data category remained unchanged compared to 2020 (57%[14]). However, a notable difference from the previous year is represented by the percentage of requests for traffic data (26%) which has slightly increased when compared to 2020 (20%). Furthermore, according to the responses obtained to this year's survey, requests for content data have decreased (19% compared to 22% in 2020).



The reasoning for building up their cases by using a cascading principle for needed data is well reflected in the input provided by some of the surveyed judicial authorities:

- *Traffic data or content data can only be obtained through an MLA Request, which is time-consuming and has little chance of success, so it is often not pursued (Germany).*
- *According to Greek legislation content data is protected by the law and access to it can be given only for serious criminal case after the decision of the judicial council (Greece).*

Voluntary cooperation with foreign-based OSPs

In the context of cross-border criminal investigations, EU law enforcement and judicial authorities can request and obtain disclosure of data held by OSPs established outside their jurisdiction in multiple ways. One specific channel builds on the regime of voluntary cooperation – directly addressing foreign-based OSPs. Direct requests under voluntary cooperation are entirely dependent on the willingness of OSPs to cooperate with authorities. The lack of enforceability of such requests can lead to struggles for authorities.

The data collected from the survey shows that the national legislation of slightly more than half of the EU Member States surveyed (14 out of 25) allows the gathering of electronic data via cross-border voluntary cooperation. However, a significant number of countries still do not foresee the possibility to directly address private entities situated abroad with data disclosure requests. The results are overall in line with previous year's data, although the percentages are closer.

Additional information as provided by some of the respondents is reported in Table 1.

Does your national legal framework allow electronic data to be gathered – outside the scope of the formal MLA procedure – via cross-border voluntary cooperation by directly addressing a private entity situated abroad?

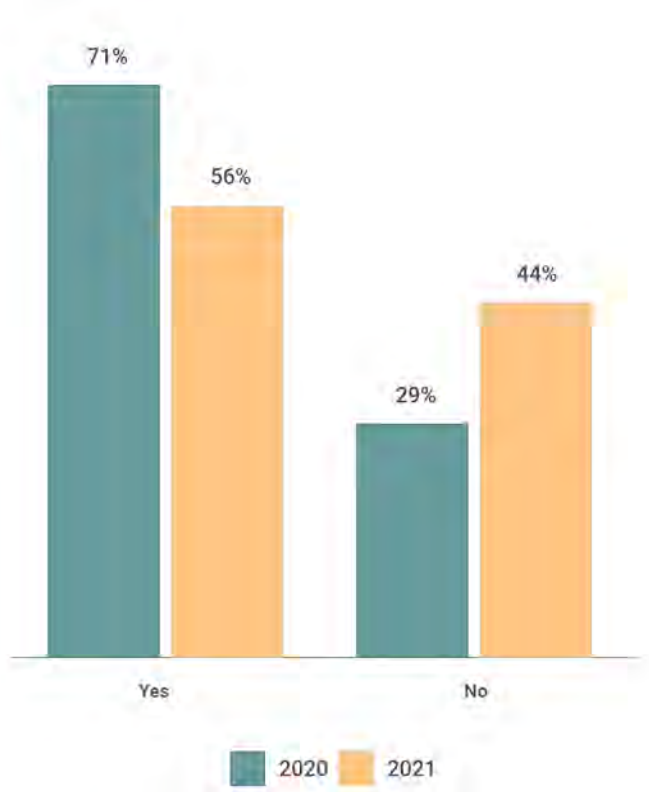


Table 1: EU Member States' legislation relating to voluntary cooperation mechanisms

Denmark	Yes, from US based entities - in accordance with US permission.
Estonia	According to the Code of Criminal Procedure there is no obligation to lodge an EIO or a MLAT in order to acquire evidence directly from OSPs situated on the territory of a foreign state.
Germany	On the basis of the European Mutual Legal Assistance Convention of 29.05.2000 and in the countries that have ratified the agreement.
Greece	Such a direct contact would violate the law on data protection.
Ireland	Not expressly. However, the admissibility of evidence obtained by cross-border voluntary cooperation, outside of the MLA provisions has not been tested by the Irish Courts which would make the decision based on the particular facts of the case, a determination as to whether any constitutional or legal rights were infringed to obtain the evidence and if so the application of a proportionality test to determine if the breach of rights is such as to outweigh the public interest in having the evidence admitted. The Court would also engage in an examination of the probity and authenticity of the evidence in question.
Lithuania	[Yes] but there is no specific legal provision in the national legal framework. The court is deciding in every specific case if certain data can be admitted as evidence.
Netherlands	The Dutch Penal Code does not provide for this legal figure, but we do see possibilities for making agreements with OSPs if, for example, the country where the OSP is based agrees or if the data is hosted on our territory. We ask other countries specifically to contact our legal authorities instead of directly addressing OSPs in the Netherlands.
Portugal	Article 14 of the Cybercrime Law transposed into the domestic law Article 18 of the Budapest Convention. Thus, it is permitted to address a foreign ISP requesting information - within the limits of Article 18, that is, limited to basic subscriber information, including the IP address used to establish a known and determined communication.
Slovak Republic	No, but it is also not forbidden and obtained information can be used for intelligence purposes.
Slovenia	Theoretically it would be possible to request BSI; however, according to the Slovenian legislation and case law a court order is required to obtain the BSI if OSP needs to process traffic data to get the BSI. Slovenian courts use MLA or EIO to issue their court orders to OSP in foreign countries, because the Constitution of the Republic of Slovenia prescribes court order when obtaining data, related to electronic communication (Article 37).
Spain	There is no legislative provision to that effect. In certain cases, data is being collected directly from ISPs in cases where the domestic legislation of the requested country so permits. In such cases, it is the nature of the data that determines whether or not judicial authorisation is required for this direct cooperation.
Sweden	Unregulated, used only towards US companies.

Regarding the practice in non-EU Member States, the judiciary of Georgia, Republic of Moldova and Switzerland indicated that the legal frameworks of their respective countries allow to gather electronic data outside of the scope of the formal judicial cooperation procedure.

Emergency disclosure requests

While the definition of an emergency situation varies from country to country, based on the answers received from EU judicial authorities, emergency disclosure procedures can apply, for example, in case of a terrorist threat or when a written order cannot be obtained in due time and a delay would endanger human life or health (see Table 2 below).

This year, judicial authorities were asked whether their national legal framework already foresees a specific mechanism to compel foreign-based OSPs providing services in their country to provide information in

emergency circumstances (for example, following the model of Article 3(2)(c) of the Second Additional Protocol to the Budapest Convention). The results show that in the majority of the EU Member States surveyed (20 out of 25), no such mechanism currently exists.

Additional information was provided by some of the respondents as further set out in Table 2.

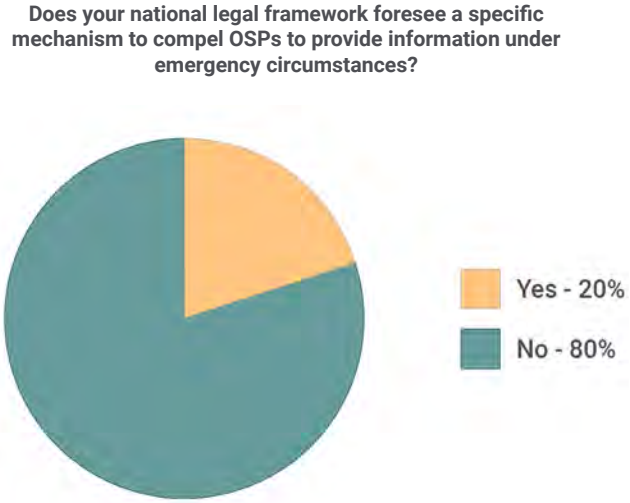


Table 2: EU Member States' legislation related to EDRs

Estonia	In an emergency situation the Code of Criminal Procedure allows the prosecutor to require the data without the court's permission. § 90-1. Requiring data from an electronic communications undertaking (6) In a situation of urgency where it is not possible to obtain, at the proper time, an authorisation of the pre-trial investigation judge or of the court, an enquiry mentioned in subsection 2 of this section may be made under an authorisation of the Prosecutor's Office which has been given in a form that is reproducible in writing and contains at least the particulars provided for by clauses 1 and 3 of subsection 4 of this section. In such a case, a reasoned application for allowing the enquiry must be filed with the court within the first business day following its making. The pre-trial investigation judge decides on allowing the enquiry by an order that may be made as a note on the application of the Prosecutor's Office. Electronic Communications Act § 112. Obligation to provide information (1) If an agency or authority specified in subsection 111-1 (11) of this Act submits a request, a communications undertaking is required to provide at the earliest opportunity, but not later than ten hours after receiving an urgent request or within ten working days after receipt of the request if the request is not urgent, if adherence to the specified terms is possible based on the substance of the request, the agency or authority with information concerning the data specified in subsections 111-1 (2) and (3) of this Act.
France	Yes, since 2015 terrorist attacks.
Greece	There is no provision in the Greek Law for such mechanism for emergencies. The main tool to this purpose is the issuance of an injunction, demanding from the OSP to display a document.
Netherlands	There is no specific mechanism but we are in good contact with the OSPs in the Netherlands and have possibilities via the [SPoC] to contact them.
Slovak Republic	This is a complicated issue to answer Yes/No. The police has some powers e.g. concerning the missing persons outside of criminal proceedings. In the criminal proceedings, there is a 24/7 mechanism of prosecutor/judge on duty that allows for an urgent reaction from the authorities. However, there is no legal obligation for OSPs to have 24/7 mechanism to respond. In other words the prosecutor may make a motion for a warrant and the judge may be available to issue it shortly. However, even if such warrant/order is issued in a short time, there is no guarantee to have it executed immediately by a provider (due to non-existence of 24/7 system at the level of providers).
Slovenia	There are provisions in the Criminal Procedure Act for exceptional situations when a written order cannot be obtained in due time and if a delay would endanger human life or health, the investigating judge may, on the oral motion of the state prosecutor, order the implementation of the measure referred to in paragraph one of this Article by an oral order imposed directly on the IT operator or information service provider. The investigating judge shall make an official note of the state prosecutor's oral motion. The written order must be issued within 12 hours of the issuing of the oral order. This applies to traffic data.
Spain	Although there is no standard requiring ISPs to provide this kind of information, there is agreements between the Police and ISPs, on the basis of which this information is provided without further requirements.

In addition to the legal frameworks within the EU, representatives of Georgia and Republic of Moldova stated that their national legal framework already includes a specific mechanism to compel foreign-based OSPs providing services in their country to disclose information in emergency circumstances. Whereas such mechanism is not currently available in Switzerland.

Production Orders – domestic measures with cross-border effects

The Budapest Convention provides an additional tool for obtaining subscriber information by directly addressing OSPs which considers the global reach of the services offered by OSPs: (extraterritorial) production orders pursuant to Article 18 of the Budapest Convention[15].

Pursuant to Article 18 of the Budapest Convention, competent authorities can request subscriber information from OSPs that are established outside their jurisdiction, provided that such OSPs are in possession or control over the data sought; and offer their services in the territory.

This measure is not without limitations. Even if production orders pursuant to Article 18 have extraterritorial effects, they remain a domestic measure and, as such, they need to respect the domestic legislation of both the issuing and the receiving State. Furthermore, Article 18 production orders are subject to legal safeguards (e.g. in relation to data protection, protection of human rights and proportionality).

With regard to the availability of the measure under the national legal framework of the surveyed countries, 63% of the respondents (15 out of the 24 EU Member States which were surveyed) reported that their domestic laws foresee the issuance of domestic production orders towards OSPs situated abroad, but offering their services in their territory, where such OSPs are in possession or control of the sought information. This is an increase from the previous year, when only 50% of the surveyed EU Member States indicated that this measure is available under their domestic legal framework.

Those who indicated that it is possible to issue domestic production orders addressed to foreign-based OSPs shared additional explanations and/or direct references to their national legislation, as further set out in Table 3.

Does your national legal framework foresee the issuance of domestic production orders towards OSPs situated abroad, but offering services in the territory of your country, which are in possession or control of the sought information?

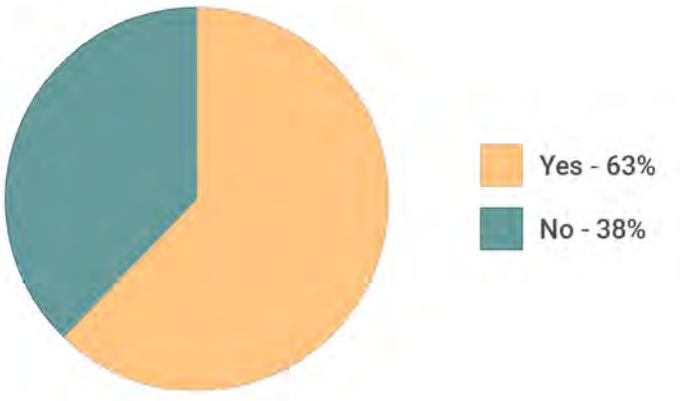


Table 3: EU Member States' legislation allowing the issuance of domestic production orders addressed to foreign-based OSPs

Estonia	The goal can be achieved on the basis of Code of Criminal Procedure § 215 and 90-1 (in the case of subscriber information). For acquiring traffic data, the special clauses from § 90-1 are applied: § 90-1. Requiring data from an electronic communications undertaking /.../ (2) On an application of the Prosecutor's Office and with the authorisation of the pre-trial investigation judge in pre-trial proceedings – or of the court in judicial proceedings – an investigative authority may make an enquiry to an electronic communications undertaking concerning data that are listed in subsections 2 and 3 of § 111-1 of the Electronic Communications Act and that are not mentioned in subsection 1 of this section. (3) An enquiry provided for by subsection 2 of this section may be made if the criminal offence is one listed in subsection 2 of § 126-2 of this Code and if it is ineluctably necessary for achieving the purpose of criminal proceedings. In relation to a criminal offence not mentioned in the list, such an enquiry is permitted if it is ineluctably necessary for achieving the purpose of criminal proceedings, justified by the gravity and nature of the offence and does not unjustifiably interfere with personal rights. (4) An authorisation for an enquiry concerning communication data states: 1) the data that are allowed to be collected by the enquiry; 2) the reason for collecting the data; 3) the period of time concerning which collection of the data is allowed. (5) An order of the pre-trial investigation judge – or a court order – that disposes of the application of the Prosecutor's Office may be made as a note on the application. /.../ For content data the provisions for search and [seizure] can be used: § 91. Search (1) The aim of a search is to find, in a building, a room, a vehicle or an enclosed area, an object to be confiscated or used as an item of physical evidence, or a document, thing or person needed for resolving the criminal case, or property to be attached in criminal proceedings, or a corpse, or to apprehend a person who has been declared a fugitive from justice. A search may be conducted provided there is a reasonable suspicion that what is searched for is located at the place to be searched. (2) Unless otherwise provided by this Code, a search may be conducted on an application of the Prosecutor's Office under a warrant from the pre-trial investigation judge or from the court. The order by which the pre-trial investigation judge or the court disposes of such an application may take the form of a note made on the application. (3) A search may be conducted based on a warrant from the Prosecutor's Office, except for a search at a notary's office or at the office of a law firm or at the premises of a person processing information for journalistic purposes, provided there is reason to believe that the suspect is using the premises or vehicle to be searched, or used those premises or that vehicle, at the time of the criminal event or during pre-trial proceedings, and the person is suspected of having committed a criminal offence mentioned in subsection 2 of § 1262 of this Code.
Greece	If a service is provided in the Greek territory by an individual or an entity, whose location is abroad, this service is regulated by the Greek law. This principle stems from article 6 of the Greek Penal Code.
Lithuania	According to the procedure established under Article 158 of the Code of Criminal Procedure.
Portugal	Article 14 of the Cybercrime Law (Law 109/2009, of 15 September) Injunction for providing data or granting access to data 1 - If during the proceedings it becomes necessary for the gathering of evidence in order to ascertain the truth, obtain certain and specific data stored in a given system, the judicial authority orders to the person who has the control or availability of those data to communicate these data or to allow the access to them, under penalty of punishment for disobedience. 2 - The order referred to in the preceding paragraph identifies the data in question. 3 - In compliance with the order described in paragraphs 1 and 2, whoever has the control or availability of such data transmits these data to the competent judicial authority or allows, under penalty of punishment for disobedience, the access to the computer system where they are stored. 4 - The provisions of this Article will apply to service providers, who may be ordered to report data on their customers or subscribers, which would include any information other than the traffic data or the content data, held by the service provider, in order to determine: a) the type of communication service used, the technical measures taken in this regard and the period of service; b) the identity, postal or geographic address and telephone number of the subscriber, and any other access number, the data for billing and payment available under a contract or service agreement, or

Portugal *(continued)*	c) any other information about the location of communication equipment, available under a contract or service agreement. 5 - The injunction contained in this article may not be directed to a suspect or a defendant in that case. 6 - The injunction described under this article is not applicable to obtain data from a computer system used within a legal profession, medical, banking, and journalists activities. 7 - The system of professional secrecy or official and State secrets under Article 182 of the Code of Criminal Procedure shall apply mutatis mutandis
Slovenia	Article 149č of Criminal Procedure Act (1) If there are grounds for the suspicion that a criminal offence prosecutable ex officio has been committed or is being prepared for which the perpetrator is prosecutable ex officio and if, for the purpose of detecting, preventing or proving this criminal offence or detecting the perpetrator, it is necessary to obtain the subscriber data on the owner or the user of a particular communication medium or information service, or on the existence and content of its contractual relationship with the IT operator or information service provider regarding the performance of communication activities or information services, the court, state prosecutor or the police may request in writing that the IT operator or information service provider transmit such information even without the consent of the data subject. The written request must include the legal instruction referred to in paragraph two of this Article and an indication of the competent court. In the written request, the state prosecutor or the police must specify in detail the categories of requested subscriber data. (2) The IT operator or information service provider may, for substantiated reasons and at its own expense, submit the requested information together with a copy of the written request to the competent court instead of to the police or the state prosecutor. Upon receipt, the court shall verify the legality of the categories of information stated in the request. If the request also contains information other than subscriber data referred to in paragraph one of this Article or information that may not be transmitted pursuant to paragraph four of this Article, the received information shall be destroyed; otherwise, it shall be forwarded to the state prosecutor or the police. In the event of destruction, the investigating judge shall make an official note thereof which shall be sent to the IT operator or information service provider, the head of the competent district state prosecutor's office or the state prosecutor, the ministry responsible for supervising police work and the police. (3) The IT operator or information service provider may not disclose to its user, subscriber or third parties that it has or will transmit certain information in accordance with this Article. Such information may not be disclosed for 24 months after the end of the month in which the data were transmitted. In the event that the IT operator or information service provider receives a court order within this period that refers to the information obtained upon the request referred to in this Article, the period of the prohibited disclosure of that request shall be extended until the expiry of the time limit that might be set in the order received. By an order, the investigating judge or court may set a different time limit, extend it by a maximum of 12 months, but not more than twice, shorten the time limit or remove the prohibition on disclosure. (4) Under this Article, it shall not be possible to request or obtain traffic data related to any identifiable communication, or data that must be obtained by processing data that can only be obtained pursuant to Articles 149b and 149c of this Act. Under this Article, it shall also not be possible to request or obtain data relating to the content of communication.
Spain	Article 588 ter j) of the Criminal Procedure Law regulates the collection of data stored by ISPs without distinguishing the place where it is located. That article provides electronic data held by service providers or persons facilitating communication in compliance with the legislation on retention of data relating to electronic communications, or on their own initiative for commercial reasons, or other type, and which are linked to communications processes, may only be assigned to incorporation into the proceedings with judicial authority. In turn, the Information Society Services Act, which establishes the legal regime for information society services and electronic contracting, as regards the obligations of service providers is applicable to foreign ISPs providing services in Spain by express provision of Art 2.2 of the Law itself.

From the perspective of the surveyed non-EU Member States, the responses indicate that only in Georgia it is possible to issue domestic production orders addressed to foreign-based OSPs, which offer their services in Georgia. There is no such possibility foreseen in the domestic legislation of the Republic of Moldova and Switzerland.

Future developments

The Second Additional Protocol to the Budapest Convention, which was opened for

signature by the Parties to the Convention in May 2022[16], provides, under Article 7, a legal basis for competent authorities in one Party to directly order a service provider in another Party to disclose subscriber information that is within its possession or control. This provision has a slightly wider scope of application when compared to Article 18 of the Budapest Convention by no longer requiring a territorial link with the Party issuing the production order, but only with any other Party to the Protocol. Therefore, once the Protocol comes into force and is implemented into the national legislation of its State Parties, competent authorities will have at their disposal an expanded legal basis for the issuance of extraterritorial production orders.

Furthermore, Article 6 of the Second Additional Protocol to the Budapest Convention on Cybercrime provides a legal basis for direct co-operation between competent authorities in one Party and entities providing domain name registration[17] services in another country for disclosure of domain name registration information in their possession or control. While the Protocol has to yet enter into force, according to the results of the survey, the possibility for authorities to directly cooperate with entities providing domain name registration already exists in 54% of the EU Members States surveyed (13 out of surveyed 24).

Several respondents provided additional explanations and/or and extracts of their national legislation, as further set out in Table 4 and Table 5.

Similarly, the survey shows that practices also vary among the third countries surveyed. For instance, in Georgia, pursuant to Article 138(1) of the Code of Criminal Procedure 2009 (international production orders) it is possible to request domain name registration from foreign-based OSPs; whereas in the Republic of Moldova and Switzerland such information can be requested only on the basis of MLA.

Does your national legal framework (for example, following the model of Article 6 of the Second Additional Protocol to the Budapest Cybercrime Convention) foresee the issuance of requests for domain name registration information to OSPs situated abroad?

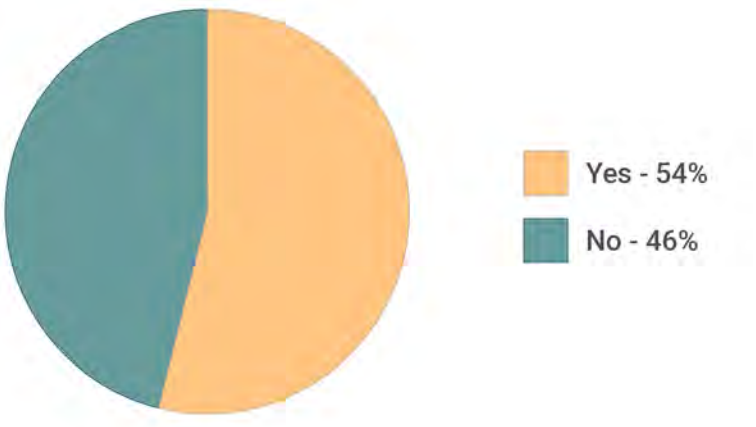


Table 4: EU Member States' legislation allowing the issuance of domestic production orders for domain name registration addressed to foreign-based OSPs

Hungary	Hungarian legislation (Crime Process Act XC of 2017) does not differ service providers in aspects of their location. Due to Budapest Cybercrime Convention's mentioned Protocol, investigation authorities can send their request directly to foreign providers for non-content e-data. But in practice the investigation authorities usually are afraid to send their request for non-content e-data to foreign service providers. Instead, they suggest EIO on platform of prosecution office or in better situation, send a data preservation request.
Latvia	Latvian Criminal Procedure Law Section 191. Storage of Data located in an Electronic Information System (1) The person directing the proceedings may assign, with a decision thereof, the owner, possessor or keeper of an electronic information system (that is, a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) to immediately ensure the storage, in an unchanged state, of the totality of the specific data (the retention of which is not specified by law) necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system. (2) The duty to store data may be specified for a term of up to thirty days, but such term may be extended, if necessary, by an investigating judge by a term of up to thirty days. Section 192. Disclosure and Issue of Data Stored in an Electronic Information System (2) During the pre-trial criminal proceedings the person directing the proceedings may request in writing, on the basis of a decision of an investigating judge or with the consent of a data subject, that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Section 191 of this Law. (3) In trying a criminal case, a judge or the court panel may request that a merchant of electronic communications discloses and issues the data to be stored in accordance with the procedures laid down in the Electronic Communications Law or that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Section 191 of this Law.
Portugal	Yes, by the framework of Law 32/2008, July 17th and Cybercrime Law 109/2009, September 15th.
Spain	Article 588 ter m) of the Criminal Procedure Act allows the Police and the Public Prosecutor's Office to obtain information on registration and payment data without the need for judicial authorisation. However, it is limited to data other than traffic data. The above-mentioned article provides as follows: Identification of owners or terminals or connectivity devices. When, in the exercise of their functions, the Public Prosecutor's Office or the Judicial Police need to know the holder of a telephone number or any other means of communication, or, on the contrary, need the telephone number or identity data of any means of communication, can go directly to service providers to telecommunications, access to a telecommunications network or information society services, which shall be obliged to comply with the request, with a warning about the commission of the crime of disobedience.

Table 5: EU Member States' legislation not allowing the issuance of domestic production orders for domain name registration addressed to foreign-based OSPs

Netherlands	The Dutch Criminal Code of Procedure currently does not provide a legal ground for direct production orders for domain name registration information in the possession or control of such information, MLA is required. The Dutch legal framework does not allow for voluntary requests that lack a legal basis in the Dutch Code on Criminal Procedure.
Slovak Republic	No specific provisions that would provide concrete legal basis for issuing a request to an entity providing domain name registration services in the territory of another Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name.

Domestic legal framework in relation to direct requests to OSPs

In order to also assess the perspective of OSPs, judicial authorities were asked whether their respective national legal framework allows companies to respond to direct requests for data from foreign-based authorities. The results from the survey reveal that the legislation in the majority of the EU Member States does not allow domestic OSPs to respond to such requests (17 out of 24 surveyed). However, some legal ambiguity in the national legal frameworks (e.g. based on case law) remains, as indicated by 17% of the EU Member States.

Some respondents provided additional explanations as further set out in Table 6 and Table 7.

Does your national legal framework allow domestic OSPs to directly respond to requests from the public authorities situated in other jurisdictions ?

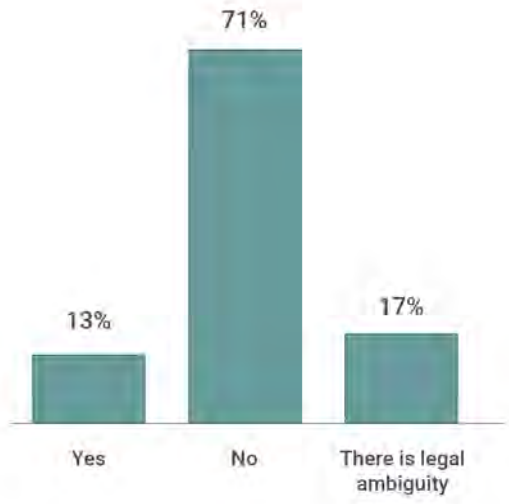


Table 6: EU Member States which allow domestic OSPs to respond to direct requests for data from foreign authorities

Denmark	Since there is no specific national framework regarding this, OSPs in our country can chose to respond to requests from foreign authorities, provided that the response is in accordance with the rules and regulations of GDPR.
Greece	If the OSPs have the consent of the nominees, they can transmit the information to others. Any such order, even if it comes from a non-domestic judicial authority, is enforced by or through domestic authorities.
Ireland	There is no specific legal provision for this exchange. It is a matter for the OSP. Otherwise an MLAT request is required for a domestic order to issue on behalf of the requesting authority. Although there are no specific legislative provisions in that regard, it is possible for OSPs to share information or respond directly to legal requests. It depends on who owns the data, the nature of the data, the purpose of the request, the user terms and conditions of the OSP, the extent of the duty of care owed by the OSP to the owner of the data / user etc. This is a very nuanced question, for example a request for information about a legal person may be treated differently than a request for information about a natural person particularly where the offence under investigation is a serious offence relating to the right to bodily integrity of a victim or the safety and security of the State.
Netherlands	The Netherlands have endorsed the Guidance Note for article 18 of the Cybercrime Convention.
Slovenia	According to Art. 68.a of Cooperation in Criminal Matters with the Member States of the European Union Act (ZSKZDČEU-1) an EIO is needed for transfer of evidence. Therefore a request has to be assessed by competent State Prosecutor or Judge.

Table 7: EU Member States which do not allow domestic OSPs to respond to direct requests for data from foreign authorities

Estonia	A domestic OSP is not allowed to directly respond to requests from the public authorities situated in other jurisdictions. The statement relies on the following legal norms from the Code of Criminal Procedure: § 433. General principles (1) International co-operation in criminal procedure comprises extradition of persons to foreign states, mutual assistance between states in criminal matters, execution of the judgments of foreign courts, taking over and transfer of criminal proceedings commenced, co-operation with the International Criminal Court and Eurojust and extradition to member states of the European Union. [RT I 2008, 19, 132 - entry into force 23.05.2008] (2) International co-operation in criminal procedure shall be effected pursuant to the provisions of this Chapter unless otherwise prescribed by the international agreements of the Republic of Estonia, the European Union legislation or the generally recognised principles of international law. [RT I 2008, 19, 132 - entry into force 23.05.2008] § 434. Requesting state and requested state (1) A state which submits a request for international co-operation in criminal procedure to another state is the requesting state. (2) A state to which a requesting state has submitted a request for international co-operation in criminal procedure is the requested state. § 463. Compliance with requests for assistance received from foreign states (1) Requests for assistance are complied with pursuant to this Code. At the request of a foreign state, a request may be complied with pursuant to procedural provisions different from the provisions of this Code unless this is contrary to the principles of Estonian law. § 489-46. Recognition and execution of European Investigation Orders (1) The Prosecutor's Office is competent to recognise a European Investigation Order transmitted to Estonia, to conduct proceedings concerning the EIO and to ensure its execution. The Prosecutor's Office may require an investigative authority to execute the EIO or refer it for execution to another competent judicial authority. [RT I, 19.03.2019, 3 – entry into force 01.07.2019]

In addition to the EU judiciary's input, the judiciary of Japan, the Republic of Moldova and Switzerland also indicated that according to their domestic legislation, OSPs situated in these countries are not allowed to respond to direct requests from foreign authorities and thus, an MLA request is required to obtain electronic evidence from such OSPs.

Admissibility as evidence of data collected via direct requests for voluntary cooperation

In addition to whether electronic data can be directly obtained from foreign-based OSPs, another important question to be considered is whether such data can be admissible as evidence in court in accordance with the applicable national legal framework.

Regarding the admissibility of data collected via direct requests for voluntary cooperation as evidence, the answers received show that in the vast majority (74%) of the EU Member States surveyed (17 out of 23), data gathered via cross-border voluntary cooperation can be admitted as evidence in court. These results are almost identical to results received in the previous year.

For some of the countries where such data can be admitted as evidence in court, further explanations were provided as set out in Table 8.

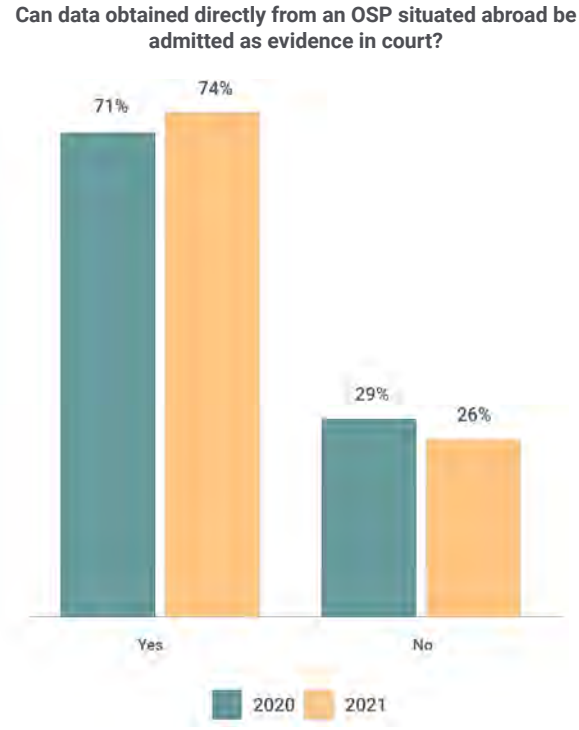


Table 8: Admissibility as evidence of data gathered via direct requests for voluntary cooperation

Denmark	In Danish law, there is a so-called free assessment of evidence.
Estonia	Directly gathered evidence are admissible pursuant to Code of Criminal Procedure §-s 215, 90-1 or 91 (depending on evidence sought to be gathered) and § 65. § 65. Evidence obtained on a ship during voyage and in a foreign state (1) Evidence taken in a foreign state according to the legislation of such a state may be used in criminal proceedings in Estonia unless the procedural operations performed in order to obtain the evidence are contrary to the principles of Estonian criminal procedure, having regard to the special rule provided by subsection 2 of this section. Case law regarding the provision states that the phrase, [“] the principles of Estonian criminal procedure" does not entail every possible procedural norm. It must be understood in the light of constitutional provisions (foremost §-s 22 - 24) and the general principles regarding gathering evidence (Code of Criminal Procedure § 64) (The Supreme Court's Judgement dated 18.11.2009 no 3-1-1-84-09, point 10.1). § 64. General conditions for the collection of evidence (1) Evidence is collected in a manner which does not offend the honour and dignity of those participating in its collection, does not endanger the life or health of such participants and does not cause unjustified pecuniary harm. It is prohibited to collect evidence by torturing a person or by subjecting them to violence in any other way, or by using means which affects their faculty of memory, or by treating them in a manner that degrades human dignity. (3) If technical equipment is to be used to take the evidence, this is notified in advance to the participants in the corresponding procedural operation and the purpose of using the equipment is explained to them. 4 […] (5) Where this is needed, participants of a procedural operation are cautioned that, under § 214 of this Code, disclosure of information relating to pre-trial proceedings is not allowed. (6) The taking of evidence by covert operations is regulated by Chapter 31 of this Code.
France	If it is provided by the defendant or the victim.
Germany	There are no special rules for electronic data collected directly from OSPs abroad. The same rules apply as for domestic data collection.
Greece	If the access to the data is not prohibited by the law.

Ireland	Possibly, provided the investigator can prove probity and authenticity. Under the Wilmington principle it is necessary to prove the chain of evidence. The evidential burden rests with the prosecution. The method of proving electronic evidence also depends on whether the evidence is classified as "real evidence" i.e. evidence which is produced by a machine without human intervention or "hearsay evidence" i.e. evidence produced by a person inputting data into a machine. If the evidence is classified as real evidence, the prosecution will be required to prove the chain of evidence, the probity and authenticity of the evidence. If the evidence is classified as hearsay evidence, the prosecution will be required to bring the evidence within one of the common law or statutory exceptions to the rule against hearsay. There are too many to list. Commonly used statutory exceptions may be found in the Criminal Evidence Act 1992 and the Bankers Books Evidence Acts. An example of a common law exception is res gestae evidence (i.e. evidence which forms part of the commission of a crime) or declarations to prove falsity.
Lithuania	Under our national law, the court shall decide in each case that the data provided is admissible as evidence. Article 20 of Code of Criminal Procedure of the Republic of Lithuania Evidence 1. Evidence in a criminal procedure shall be material obtained in the manner prescribed by law. 2. Admissibility of the material obtained shall be determined in every case by the judge who is seized of the case. 3. Only such material which proves or disproves at least one circumstance relevant for a fair disposition of the case may be regarded as evidence. 4. Evidence may be only such material which is obtained by lawful means and may be validated by the proceedings laid down in this Code. 5. Judges shall assess the evidence according to their inner conviction based on a scrupulous and objective review of all the circumstances of the case in accordance with the law.
Portugal	According to the Portuguese legal framework, it is allowed to obtain evidence in any circumstance, unless it is forbidden by law. Thus if it is permitted to request directly information to a Service Provider, the information that the provider may sent will be accepted as evidence.
Spain	There is no specific legal provision but in principle there is no legal obstacle to its admission as evidence without prejudice to the fact that the procedure of obtaining it can be challenged giving rise to the judicial assessment of its validity or not.

A similar tendency towards the admissibility as evidence of data collected via direct requests for voluntary cooperation was observed in the responses of the Georgian, Moldovan and Swiss judiciary, where representatives of all three countries expressed that such data may be deemed admissible as evidence in their respective courts.

Regarding the responses which indicated that such evidence is not admissible in their country, additional remarks were received from the judicial authorities of the following EU Member States, as presented in Table 9.

Table 9: Admissibility as evidence of data gathered via direct requests for voluntary cooperation

Czech Republic	[No], unless it is verified by foreign judicial authority.
Malta	[No], only if obtained via an EIO or Letters Rogatory.

Direct access to electronic data

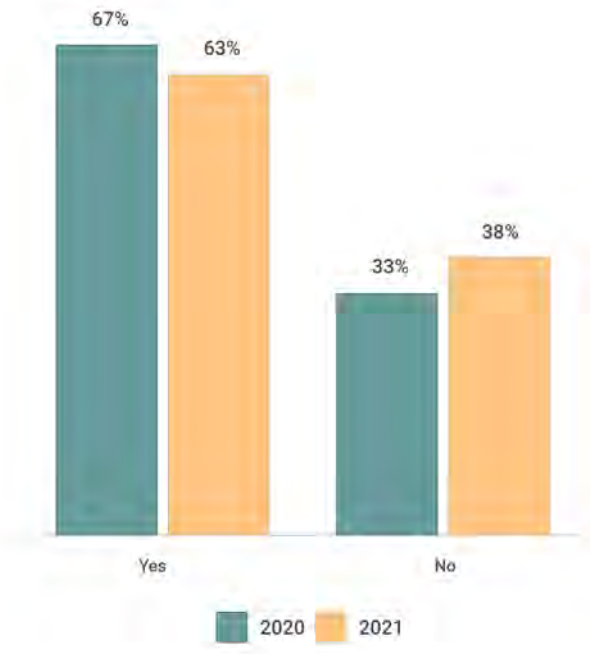
Another modality for cross-border access to electronic data, in addition to direct requests for voluntary cooperation, domestic production orders and judicial assistance, is direct access. Direct access to data may be obtained pursuant to coercive measures taken in accordance with national procedural laws (e.g. search and seizure) or when the parties of the investigation – for example a victim, a witness or a suspect, which are holders of the targeted data – voluntarily

provide the information (e.g. by handing over the requested piece of information or password or by downloading the entire database and handing it over to the authorities).

The Budapest Convention provides in its Article 32[18] a specific modality for direct access to data stored abroad. This provision compounds three key aspects:

- **The cross-border aspect**: investigative authorities can directly access data stored in another country;
- **The automatic recognition**: data gathered on this basis can be admissible as evidence in court without the need to go through a judicial assistance process (EIO/MLA); and
- **The consent**: the consent of the person who has the lawful authority to disclose the data is required.

Does your national legal framework (e.g. on the basis of the Article 32(b) of the Budapest Cybercrime Convention) allow cross-border direct access to electronic information ?



With regard to the availability of this measure in their respective national legal frameworks, the majority of the EU Member States surveyed (15 out of 24) reported it as being incorporated into their national legislation. These results are similar with those received in the previous year.

Some respondents, whose national legal framework permits cross-border direct access to data with the consent of the data subject, provided additional information as further set out in Table 10.

Similarly, respondents whose national legal framework does not allow cross-border direct access to data as envisaged in Article 32 of the Budapest Convention provided additional explanations included in Table 11.

In addition, regarding the responses from the third countries surveyed, Georgia and Switzerland stated that the measure provided for in Article 32(b) of the Budapest Convention is incorporated into their domestic legal framework. However, such legal measure is not available in the Moldovan national legislation.

Table 10: EU Member States where cross-border direct access to data with the consent of the data subject is allowed

Estonia	The Code of Criminal Procedure (CCP) does not contain specific provisions for the particular procedural act, however the same goal can be achieved as a result of co-interpreting the provisions mentioned under the answer no 3 (foremost CCP § 215 accompanied by a clear consent of a data subject) and adding the following norms: The Constitution of Republic of Estonia § 3. State power shall be exercised solely on the basis of the Constitution and laws that are in conformity therewith. Generally recognised principles and rules of international law are an inseparable part of the Estonian legal system. CCP § 2 point 2 § 2. Sources of criminal procedural law The sources of criminal procedural law are: 1) the Constitution of the Republic of Estonia; 2) the generally recognised principles and provisions of international law and international agreements binding on Estonia; 3) this Code and other legislation which provides for criminal procedure; 4) decisions of the Supreme Court in the issues which are not regulated by other sources of criminal procedural law but which arise in the application of law. The referred norms allow to directly rely on the Budapest Cybercrime Convention article 32 (b). The Supreme Court of Estonia has issued several decisions regarding the meaning of a voluntary consent to disclose data. The latest one was made in the context of disclosing a patient's health records. The Court relied on the General Data Protection Regulation and ruled that a consent that cancels the effect of confidentiality must be defined on a case by case basis and include information - who are recipients of such information and to what extent data is going to be disclosed to such recipients. The patient's consent must be voluntary, defined, informed and clear for a data subject. These elements must be explained to a patient in simple and understandable manner (The Supreme Court's decision 01.04.2022, no 1-20-5071, point 24).
Latvia	Latvian Criminal Procedure Law. Section 190. Submission of Objects and Documents Requested by the Person Directing the Proceedings (1) The person directing the proceedings, without conducting the removal provided for in Section 186 of this Law, is entitled to request from natural or legal persons, in writing, objects, documents and information regarding the facts that are significant to criminal proceedings, including in the form of electronic information and document that is processed, stored or transmitted using electronic information systems.
Lithuania	The legal basis for application is Article 155 of the Criminal Procedure Code.
Netherlands	Cross-border direct access is possible from a device in the Netherlands if: - either we order to search that device or the defendant gives permission to search the device and - if during that search a server abroad is entered and we know in which country that server is based with permission of that competent authority, and in the case we don't know where the server is based and we cannot get the requested permission from the foreign authority, we can proceed with the search.
Slovak Republic	The T-CY provided a Guidance Note on this issue, therefore within its limits and restrictions explained in the Guidance Note Article 32b is applicable.
Slovenia	Article 219a (1) A search of electronic and related devices, and electronic data storage devices (electronic devices), including network-connected and accessible information systems where data is stored, may be carried out for the purpose of obtaining information in electronic form if reasonable grounds for suspicion exist that a criminal offence has been committed and if it is likely that the electronic device contains electronic information: - on the basis of which the suspect or the accused person may be identified, uncovered or apprehended, or the traces of the criminal offence that are important for criminal proceedings may be uncovered, or - which may be used as evidence in criminal proceedings. (2) The search shall be carried out with the prior written consent of the owner and the users of the electronic device known by and accessible to the police who have reasonable expectations of privacy (user) concerning such a device, or pursuant to a reasoned written warrant of the court issued upon a motion of the state prosecutor. When the search is carried out pursuant to a court warrant, a copy of such warrant shall be served on the owner or user of the electronic device which is to be searched before the beginning of the search. The search of an electronic device seized from an attorney, a candidate attorney or a trainee attorney may only be carried out pursuant to a court search warrant, reasoned in accordance with paragraph six of Article 220.

Spain	Spanish legislation provides for the possibility of accessing information contained in other systems, accessible from a device subject to registration that is located in national territory without distinguishing according to the place where the information is housed, in art. 588 ss. c) 4 [of the Criminal Procedure Code]. Where the searcher, or has access to, the information system or a part thereof, in accordance with the provisions of this Chapter, has reasonable grounds to consider that the data sought is stored in a different computer system, or part of it, may expand the search, provided that the data is legally accessible through or available to the initial system. This extension of the registration must be authorised by the judge, unless it has already been done in the initial authorisation. In cases of urgency, the Judicial Police or the Prosecutor may execute it, immediately informing the judge and, in any case, within a maximum period of 24 hours, of the proceedings carried out, the manner in which they have been carried out and their outcome. The competent judge shall, also in a reasoned manner, revoke or confirm such measure within a maximum of seventy-two hours of the interception order.

Table 11: EU Member States where cross-border direct access to data is not allowed

Ireland	Not specifically, but cross border access to electronic evidence can be obtained under the provisions of the Mutual Legal Assistance Act 2008 and MLATs.
Portugal	The article 15º/5 of The Portuguese Cybercrime Law doesn´t allow cross-border direct access to electronic information and we need international judicial cooperation to obtain evidences abroad in public or private providers. If we need a kind of electronic searches, the Prosecutors must ask permission to the investigative judge and in 15 days bring a copy of the evidences obtained and submit them to judicial control.

Other aspects of extraterritorial jurisdiction

The vast majority of the respondents from EU Member States (22 out of 24) as well as third countries (Republic of Moldova and Switzerland) indicated that there are no other aspects of extraterritorial jurisdiction relating to the acquisition of electronic evidence covered by their respective national legislation or case law (other than Articles 18[19] and 32[20] of the Budapest Convention, Articles 6[21] and 7[22] of the Second Additional Protocol to the Budapest Convention, and Article 31[23] of Directive 2014/41/EU of the European Parliament and of the Council regarding the European Investigation Order in criminal matters (EIO Directive)).

The countries which stated that such additional extraterritorial aspects do exist provided additional explanations and/or examples of their national legislation, as further set out in Table 12.

Are there any other aspects of extra-territorial jurisdiction in relation to acquisition of electronic evidence covered by your national legislation and/or case law?

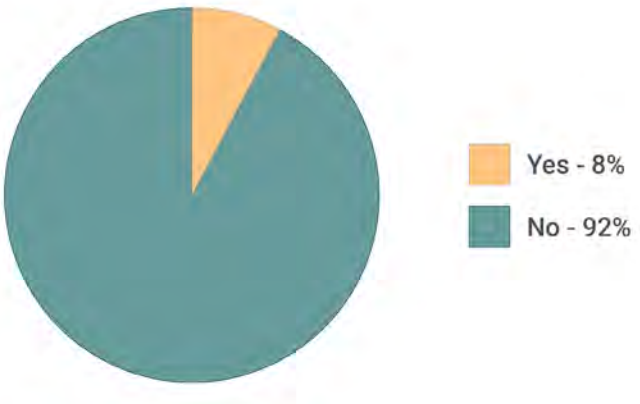


Table 12: Additional aspects of extraterritorial jurisdiction

Netherlands	Article 557 of the proposed Dutch "Innovatiewet Strafvordering" introduces the power to open an extended (network) search from a location other than the location where a device has been seized. This does not involve preservation or production orders, but unilateral searches that may also extend [outside of] The Netherlands.
Portugal	Article 15 of the Cybercrime Law allows authorities to conduct computer searches. This provision follows Article 19 of the Budapest Convention. Thus, it also allows the extension of the search in case the authorities discover that the evidence is in another system that may be lawfully accessed from the first. In Article 19 of the Budapest Convention this possibility is limited to computer systems that are located within the territory of the investigating country. In the Portuguese laws this limit does not exist: that is, the search can be extended to computer systems wherever they are located, including in another country.
Spain	The Criminal Procedure Act, in art. 588 septies a). 3. by regulating the technological research measure of remote registration, but requires that the device be located in national territory, allows access through the same to information hosted in outsourced systems with specific judicial authorisation to do so, without distinguishing according to the territory where the information is hosted. This paragraph states: Where the agents carrying out the remote search have reasons to believe that the data sought are stored on a different computer system, or on a part of it, they will make this fact known to the judge, who may authorise an extension to the terms of the search.

Agreements on public-private partnerships

Cooperation with the private sector is vital in combating crime. The private sector holds much of the evidence required for investigations and prosecutions and public-private partnerships can, among other things, be intended to strengthen and facilitate cooperation in criminal matters – for example with telecommunication or other businesses – which can have implications for access to electronic evidence.

For the purposes of the present report, judicial authorities were asked if in their respective countries any public-private partnerships and/or memoranda of understanding were in place with the industry. Similarly to the situation presented in last year's report, the answers received indicate that in the majority of the EU Member States surveyed (14 out of 25), such agreements are not in place. However, the latest data show an increase on the number of partnership put in place.

Additional explanations were provided by several of the respondents, as further set out in Table 13.

Are there any public-private partnerships/memoranda of understanding in place with the industry intended to strengthen and facilitate either strategic or operational cooperation in criminal matters ?

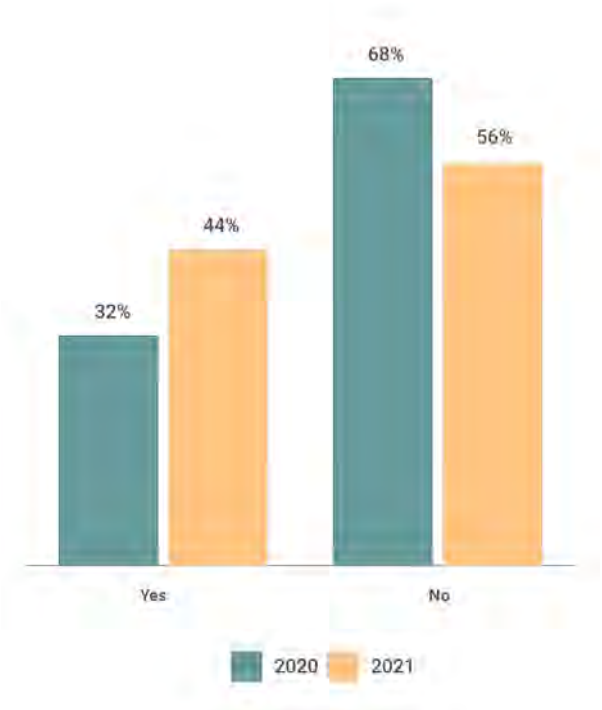


Table 13: Examples of public-private partnerships/memoranda of understanding aimed at facilitating cooperation with the private sector in criminal matters

Denmark	There is some cooperation with e.g. telecommunication companies.
France	Most of the time with the police and gendarmerie forces. Since [M]arch 2022 in relation with the Cyber Campus located in Paris.
Lithuania	Law enforcement has some agreements with several private companies.
Netherlands	Based on Article 26 of the GDRP (the Electronic Crimes Task Force) and possibly in the future regarding the exchange of cyber threat intelligence.
Portugal	Under the general powers of the Prosecution Service, a Protocol was signed with the major telecom and Internet providers. This protocol created easy channels to send requests (from the prosecutors to the ISPs) and introduced a template to draft requests. The result was a[n] easier and quicker process of requesting basic subscriber information and also the identification of the user of [an] IP Address.
Slovak Republic	Not at the level of the prosecution service. However, there is a mechanism for discussing the issues with the private sector - National expert group against cybercrime - that is composed of both public and private sectors.
Sweden	Possibly at the level of law enforcement with telecommunication service providers.

As far as third countries are concerned, such cooperation agreements are reported to be in place in the Republic of Moldova and Georgia. Regarding the latter, a memorandum of understanding between Georgian major telecommunication providers and investigating authorities was signed in 2009. Regarding Switzerland, it has been reported that no agreements with the private sector are in place; there is also no information about such practice in Japan.

C. Challenges encountered by EU judicial authorities

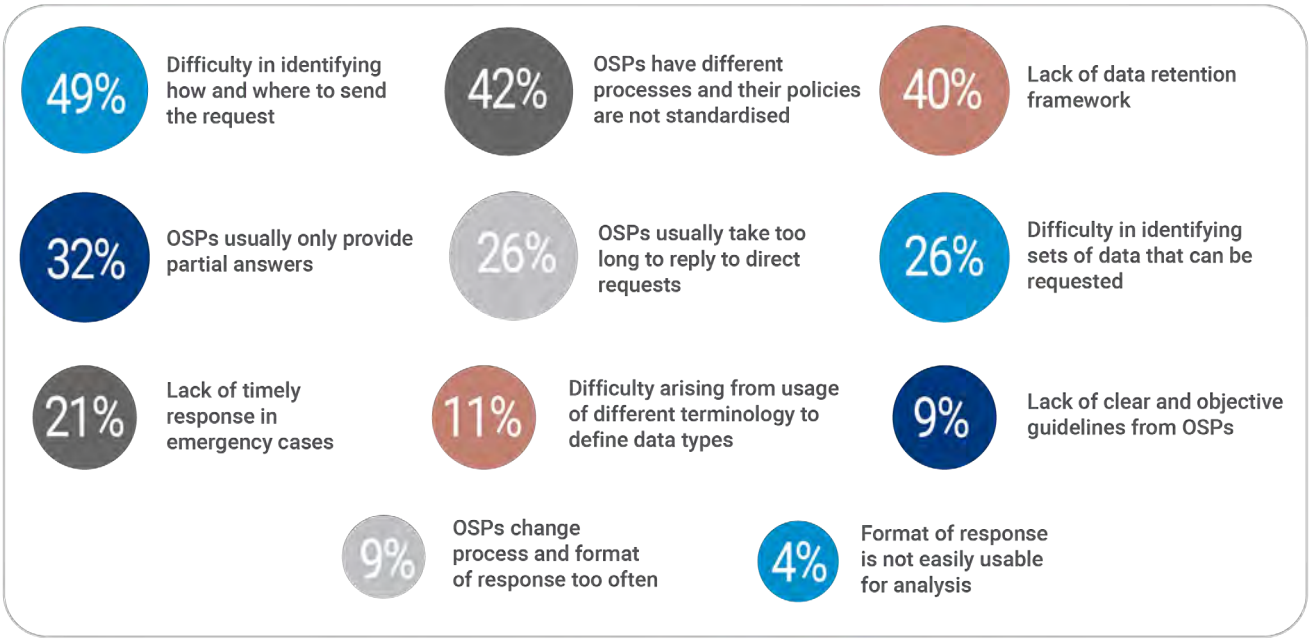
Challenges related to reaching OSPs based in foreign jurisdictions

The surveyed judicial authorities were requested to identify the three most challenging aspects faced when contacting foreign OSPs with requests for electronic evidence under voluntary cooperation. In 2021, the predominant issue, pinpointed by 49% of the respondents, was the difficulty in identifying how and where to send the request. This can refer, for instance, to the impossibility to identify the location where an OSP is established or which is the legal entity responsible for cooperation with public authorities.

The second main issue identified is the fact that companies have very different processes (42%). Data retention related issues (identified as the main problem in investigations carried out in 2020 -57%) were identified as the third most prominent problem in investigations carried out in 2021 (40%). Other issues identified are the fact that companies usually only provide partial answers (32%) and that they take excessive time to respond (26%).

Overall, the main challenges faced by public authorities in reaching out to OSPs as indicated in the previous reports remain unchanged.

In your personal experience, what have been in 2021 the three main problems when contacting OSPs located in another jurisdiction?



Additional problems reported with a lower prevalence were:

- Difficulties in identifying sets of data that could be requested from companies: 26%
- Lack of timely responses in emergency cases: 21%
- Difficulties arising from the different terminology used by the different service providers and the law enforcement authorities defining the data types: 11%
- Difficulties in understanding or finding clear and objective guidelines provided by the company: 9%
- Companies change processes and response formats too often: 9%
- Other: 8%
- Format of the response is not easy to use for analysis (for example, non-editable PDF format): 4%

Some of the respondents provided specific reflections on the challenges they encountered when directly contacting foreign-based OSPs, see Table 14.

The respondents from Switzerland and the Republic of Moldova have identified as main issues the fact that companies have very different processes (a problem also identified by the EU Member States surveyed), the fact that their policies are not standardised and that they change processes and response formats too often. Additional reflections were provided by the Republic of Moldova while Georgia referred to other issues faced, see Table 15.

Table 14: Issues faced by judicial authorities from EU Member States in directly interacting with OSPs in 2021

Austria	Long response times; lack of available data due to missing data retention regulation.
Croatia	Lack of knowledge of legal framework in other countries; too long procedure; partial obtained information or evidence.
Germany	The OSPs abroad either do not answer at all, only partially or too late.
Estonia	Not all OSP reply to direct requests and thus require an EIO or a MLAT. Direct cooperation between different OSPs varies in speed, meaning that some of them answer quickly and some of them take too long. Also the responses vary in quality, however that happens also in MLA and EIO procedures. Practice is unstable and varies between different OSPs located in different countries. The same OSP could agree to execute a request from police and next time could require a MLAT instead of a direct request.
France	Replies are too often incomplete.
Greece	Response time is too long and there are often incomplete replies; different terminology. Long procedures, difficulties in coming in contact with OSPs, the plethora of applicable law to the case that are involved in.
Hungary	- Slow answer - Objections to jurisdictions - data saving/preservation
Ireland	1. Increase in the incidents of cyber offending and resulting increase in requests for disclosure not being met by decreased staffing levels. 2. Wanting everything online which presents difficulty when it comes to serving and executing court orders. 3. Unwillingness to interact directly with LEA citing COVID as the reason.
	There is not enough direct interaction. There is an over-reliance on the MLAT processes. Consideration of the right to privacy is not nuanced enough in the context of the cybercrime and electronic evidence. All criminal investigations necessarily involve a compromise of the right to privacy of the accused and often the victim. The decision in the case of Graham Dwyer lacks nuance. Data cannot be obtained and analysed for the purposes of a criminal investigation if it is not retained. [T]he capacity of OSPs to obtain evidence from pseudo-anonymised and [anonymised] data retained for marketing purposes has not been given due consideration. The reality that OSPs retain vast amounts of personal data for the purposes of marketing and "surveillance capitalism" has not been given due consideration in proportionality tests. Furthermore, there has not been sufficient consideration of the pros and cons of allowing users to remain anonymous in the virtual world.
Lithuania	Response time, reluctance to cooperate, lack of staff in OSPs.
Malta	Lack of data retained on Internet Traffic Data, lack of uniformity in data presentation by the OSP, all the local OPS have different formats, lack of retention of Engineering Data retained by OSP.
Netherlands	Practical difficulties of identifying the enforcing jurisdiction, especially if it concerns resellers abroad. Timeliness and diversity of procedures, which not always match what is allowed under the Dutch Code of Criminal Procedure (e.g. copies of warrants etc.).
Portugal	Delays in the execution of requests due to reduced capacity. Increase in cases connected to cybercrime. Difficulty in identifying set of data that could be requested.
Slovak Republic	Our national legislation (absence of regulation) is the biggest problem in direct interaction with OSPs.
Slovenia	There is no common legal framework on EU level to regulate process to obtain electronic evidence and grant its admissibility at court proceedings. Different EU states have different procedures, data retention periods and admissibility standards which makes cross-border cooperation very difficult.
Spain	Delay in responding to requests for data delivery, lack of knowledge of where the data is stored, disappearance of the data, determined by the lack of data retention legislation and the delay in responding to the requests made.

Table 15: Issues faced by judicial authorities from third countries in directly interacting with OSPs in 2021

Georgia	For Georgia one OSP does not disclose any data unless it is an emergency. Some of the above issues are at varied and tolerable levels so that none has created any significant difficulties.
Republic of Moldova	Negative response and usually requests of MLAT through official national authorities of the requested party, and lack of mechanism to comply.

Recurring issues

Comparing the information included in the SIRIUS EU Digital Evidence Situation Reports of the recent years[24], a clear tendency is emerging.

While carrying different weights, the recurring issues polling higher in recent years refer to:

- The lack of a data retention regime;
- The difficulties in identifying correct methods and channels for the submission of requests;
- The perceived lack of timely responses from OSPs to direct requests;
- The diversity in policies in place among OSPs; and
- The lack of timely responses in emergency cases.

At the receiving end of the requesting process there are OSPs, which are also facing specific issues. One of these issues concerns fake data disclosure requests received by OSPs and the preventative measures that they may introduce establishing more scrutinised screening and vetting procedures, which could lead to delays in responding to *prima facie* questionable or suspicious requests (e.g. first request of a law enforcement agency).

D. Judicial cooperation

The MLA process towards competent authorities in the US

Considering the large number of OSPs based in the US, judicial authorities were asked to identify the main problems encountered with the MLA process towards competent authorities there. The vast majority (89%) of respondents reported the long time needed for MLA procedures as the most challenging issue encountered in 2021. The same issue had been identified as the most prominent one in previous years, demonstrating that this is a recurring and long-standing challenge for EU authorities.

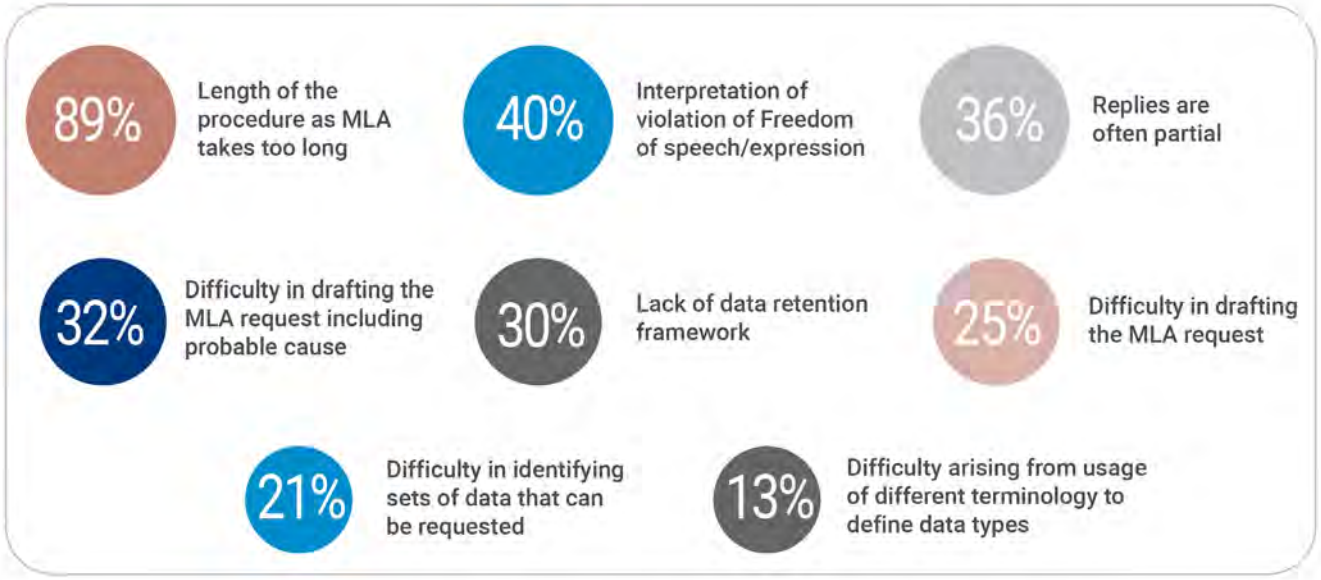
Following this main procedural issue, the "Interpretation of a violation of Freedom of speech/expression (First Amendment of the Constitution of the US)", was identified as the second biggest issue by the EU judicial authorities surveyed (40%), followed by the fact that the replies received are often partial (36%). Another challenging aspect are the difficulties in drafting the MLA requests, including meeting the probable cause standard, identified as one of the main issues by 32% of the respondents.

Additional challenges reported with a lower prevalence are:

- Lack of a data retention framework: 30%
- Difficulties in drafting MLA request: 25%
- Difficulties in identifying the set of data that could be requested: 21%
- Difficulties arising from the different terminology used by the different service providers and the law enforcement authorities defining the data types: 13%
- Other: 2%

The three third countries surveyed also all identified the length of the MLA process

What are the three main problems in the formal MLA process addressing the competent authorities of the US?



among the main issues encountered when trying to obtain data from the US through judicial channels. Other issues identified were difficulties in drafting the MLA request, difficulties arising from the different terminology used by the different service providers and the law enforcement authorities defining the data types and the fact that replies are often partial.

In addition to the issues mentioned above, obtaining electronic evidence from the US in the hate crimes has been challenging due to substantial reasons. However, the EJN Contact Points have shared the experience that allows to summarise which elements are needed in these type of MLA request for the successful outcome of cooperation.

Recurring issues

Comparing the information included in previous SIRIUS EU Digital Evidence Situation Reports, a clear tendency is emerging. While carrying different weights, the recurring issues polling higher in recent years refer to:

- The length of the MLA process;
- The interpretation of a violation of freedom of speech/expression;
- The difficulties in drafting the MLA request, including probable cause; and
- The fact that replies are often partial.

The MLA process towards competent authorities in third countries other than the US

Judicial authorities were also asked to identify the main problems encountered with the MLA process towards competent authorities in third countries, other than the US. In this respect, the length of the MLA process was reported as the most challenging issue encountered in investigations in 2021 by the respondents from the EU Members States

surveyed (79%). Following this challenge, the short data retention periods were indicated as another major problem by 42% of the respondents from EU Members States, while 36% referred to the lack of timely responses in urgent cases and the fact that the replies received are often partial as the main issues encountered.

Additional challenges reported with a lower prevalence are:

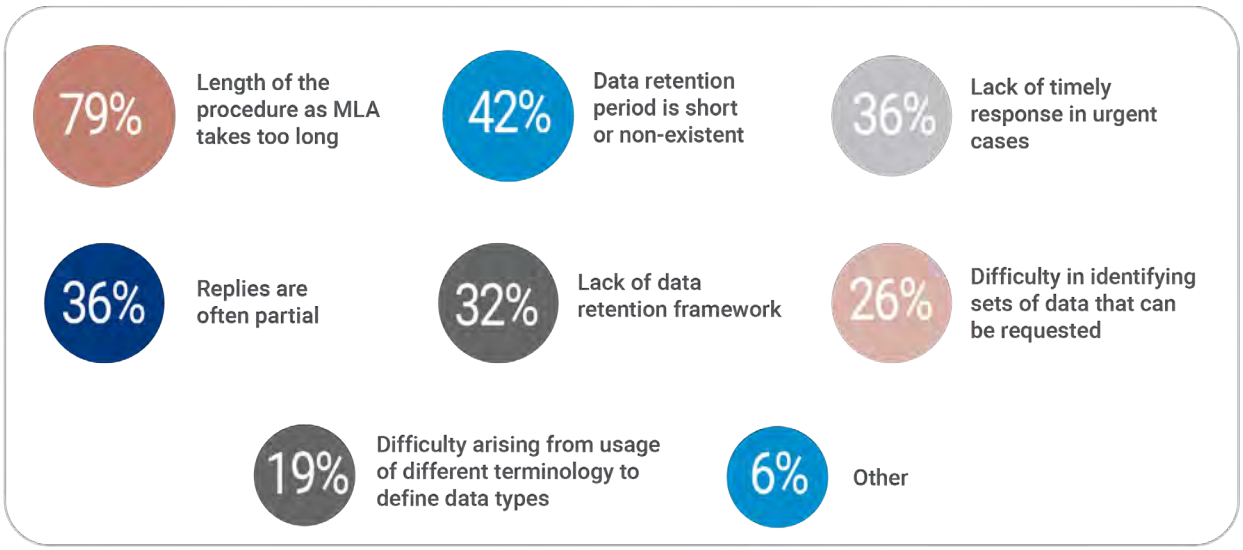
- Lack of data retention framework: 32%
- Difficulties in identifying the set of data that could be requested: 26%
- Difficulties arising from the different terminology used by the different service providers and the law enforcement authorities defining the data types: 19%
- Other: 6%

Further detailed information was reported by respondents from the following countries:

Slovak Republic	Not established direct contacts at the level of central judicial authorities to consult the issues directly.
Spain	Difficulties in identifying the PAHO that stores the data and standard procedures to address them.
Switzerland	No legal basis (no multilateral convention or bilateral agreement).

All the third countries surveyed also identified the length of the MLA process among the main issues encountered when trying to obtain data from third countries other than the US through judicial channels. Other issues identified were related to the lack of a data retention framework, the lack of timely responses in urgent cases, and the fact that replies are often partial.

What are the three main problems of the MLA process towards third states (i.e. non-EU Member States) other than the US?



The EIO/MLA process towards competent authorities in other EU Member States

As a number of OSPs are also based within the EU, judicial authorities were asked to identify the main problems with the EIO/MLA process towards other EU Member States[25].

In this respect, the majority of the respondents from EU Member States identified the lack of a data retention legal framework as the main issue, followed by the length of the procedure, namely the fact that the deadlines for recognising and executing EIOs are not respected (45%), the length of the EIO procedure (42%) as well as the length of the MLA process (38%). The difficulty in identifying the set of data that could be requested was selected as the fourth most prominent issue (30%).

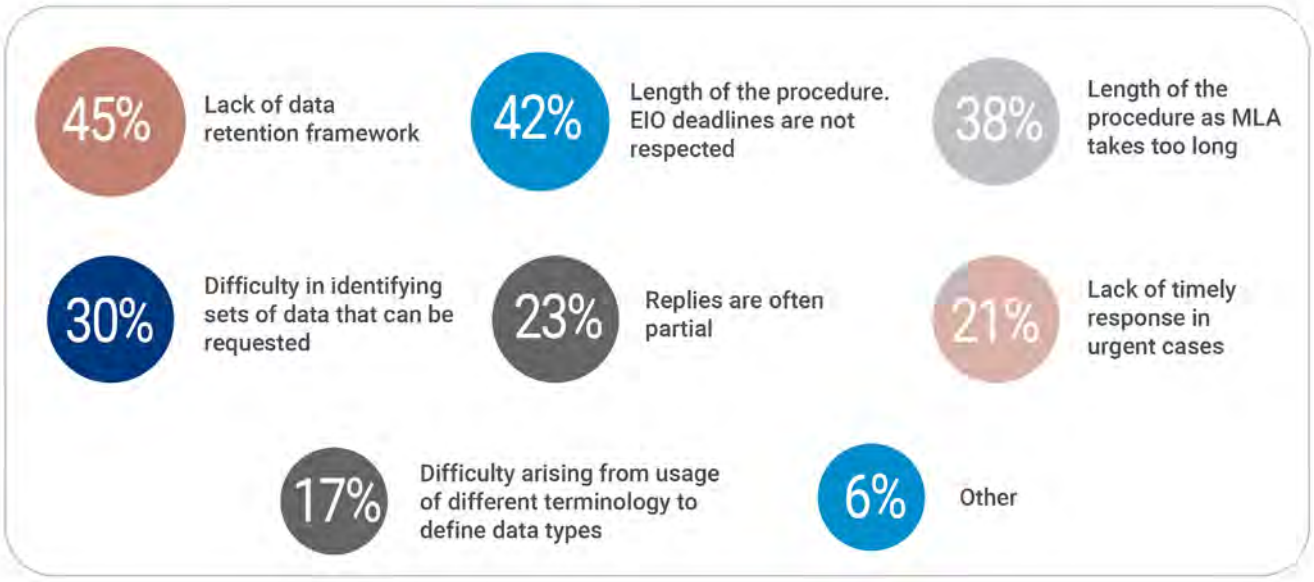
Additional challenges reported with a lower prevalence are:

- Replies are often partial: 23%
- Lack of timely response for urgent cases (such as when there is a risk of destruction/deletion of evidence, detention of a suspect, etc.): 21%
- Difficulties arising from the different terminology used by the different service providers and the law enforcement authorities defining the data types: 17%
- Other: 6%

Further detailed information was reported by respondents from the following countries:

Ireland	Ireland does not subscribe to the EIO process.
Slovak Republic	In general the issue of hosting providers, not precise WHOIS information that may mislead the authorities with targeting their requests to the proper MS, non-application of the Budapest Convention by one MS.

What are the three main problems with EIO/MLA requests towards EU Member States?



Recurring issues

Comparing the information included in previous SIRIUS EU Digital Evidence Situation Reports, it is evident that the recurring issues polling higher in recent years refer to:

- The lack of a data retention regime;
- The length of the MLA process; and
- The fact that EIO deadlines for recognition and execution are not respected.

E. Implications of cost reimbursement

The high demand for electronic data in criminal investigations and prosecutions can cause additional costs for OSPs and/or national authorities requesting access to data. Currently, the reimbursement of costs associated with complying with such requests appears not to have a significant impact on access to electronic data, however, it does have the potential to influence the data acquisition process to a greater extent in the future. In this regard, a tendency to abstain from introducing cost reimbursement policies for providing information upon request to public authorities is observed among the well-established big tech companies. This can be explained by the reputational value of cooperating with authorities and the relatively low financial costs involved in responding to requests when compared to the overall turnaround of such businesses. On the other hand, smaller companies seem inclined to reserve their right to seek cost reimbursement if faced with a high number of requests or when dealing with requests which require extensive use of resources.[26]

For instance, US federal law (18 U.S.C. §2706), relied upon by the major US-based OSPs in their respective policies[27], allows domestic OSPs to charge governmental authorities for their compliance with production orders.

A number of EU Member States also have similar legislation in this respect as provided in Table 16.

Table 16: EU Member States legislation on cost reimbursement

Austria	Austrian Code of Criminal Procedure, Article 111: (3) Persons not suspect of the offence shall, upon their request, be reimbursed for the reasonable and customary costs necessarily incurred by separating documents or other objects relevant to the evidence from others or in delivering copies.
Belgium	Belgian Royal Decree of 9 January 2003, Article 10: Costs related to investment, operation and maintenance of the technical means used by the operators of tele-communications networks and the [OSPs] for the execution of this Decree should be borne by those operators and providers. Costs related to investment, operation and maintenance of the technical means used by the judicial authorities for the execution of this Decree should be borne by the Ministry of Justice. The only compensation which operators of tele-communications networks and [OSPs] obtain in exchange for their cooperation in accordance with Articles 3, 4 and 5 of this Decree is set out in the Annex to this Royal Decree. The operator of tele-communications networks or [OSPs] who observes an accumulation of requests from judicial authorities giving rise to a considerable difference between its actual costs and the costs that are foreseen to be reimbursed under this Royal Decree, may contact the NTSU-CTIF service to determine the best way to avoid or limit such a difference.

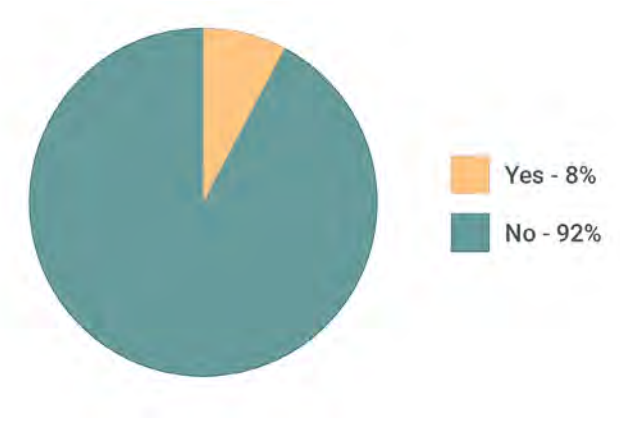
Germany	German Judicial Remuneration and Compensation Act (Justizvergütungs- und Entschädigungsgesetz - JVEG) Section 23: (1) Insofar as orders for the interception of telecommunications are implemented or information is provided by those who provide telecommunications services or are involved therein (telecommunication companies), for which special compensation is specified in Annex 3 to this Act, the compensation shall be calculated exclusively in accordance with this Annex.
Netherlands	Dutch Telecommunications Act, Article 13.6: 2. Providers of public telecommunications networks and publicly available telecommunications services shall be entitled to a payment from the State treasury for the administration costs and personnel costs that they incur arising directly from their complying with a special order or consent pursuant to the Intelligence and Security Services Act 2017 within the meaning of Article 13.2(1) and (2) or Article 13.2a, or a demand or request within the meaning of Article 13.2a, Article 13.2b, or Article 13.4(1), (2), or (3)." Dutch Ministerial Order on the reimbursement of costs of interception and provision of data, Article 3: 1 If the commissioning party [the authority that has given the provider an order or request or made to carry out a wiretapping or provide information] is of the opinion that the declared costs are billable costs [the administrative and personnel costs incurred by a provider which result directly from the carrying out of tapping or information provision activities, as specified in the Annex to this Order], the compensation will be set at the amount declared by the provider, insofar as the declared costs can reasonably be considered necessary.
Portugal	Portuguese Regulation of Judicial Costs, Article 16: 1 – The costs comprise the following types of charges: […] d) Payments due or paid to any entities for the production or delivery of documents, provision of services or similar acts, requested by the judge on request or ex officio, except in the case of certificates extracted ex officio by the court; […].
Slovak Republic	Telecommunications Act of the Slovak Republic, Section 63: (6) […] State authority that was provided with the data shall bear the costs of the medium/data storage that was needed so that the data could be provided.
Sweden	Swedish Post and Telecom Authority, Section 3: Upon disclosure of stored information, the person liable for storage shall be compensated on the basis of one of the following categories. Category 1: disclosure of stored data relating to a certain geographically delimited area [...] Category 2: other disclosures of stored data.

The feedback received from judicial authorities on the matter shows that the majority of the EU Member States surveyed do not have a cost reimbursement system in place (16 out of 25).

In addition, the results of the survey also confirm that only 8% of respondents encountered the situation where an OSP requested reimbursement of the costs associated with responding to requests for data; a vast majority of the respondents, including those from the EU Members States which do have a cost reimbursement system in place, indicated that they have never received such a claim for compensation.

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

In relation to your requests toward foreign authorities/OSPs in 2021, have you encountered the situation where the OSP requested reimbursement of the costs associated?



F. Data retention and data preservation

Developments concerning data retention in the EU

Data retention for law enforcement purposes constitutes the continued storage of non-content data by an OSP for a specific period of time due to regulatory requirements. Data retention is a proactive continuing process, which takes place in the absence of a specific request and without any connection to imminent or ongoing investigations.

Since the Court of Justice of the European Union (CJEU) invalidated the Data Retention Directive[28] in 2014, EU Member States either maintained, repealed, amended or are revising their national laws regarding retention of and access to data for law enforcement purposes.[29] Taking into account the recent rulings of the CJEU, the tendency observed in the jurisprudential developments concerning data retention in the EU is pointing towards targeted retention of data.

In 2022, the CJEU issued two judgments concerning data retention for the purpose of criminal investigations and prosecutions, namely in Case C-140/20 – *Commissioner of the Garda Síochána and Others*[30] (5 April 2022), referred to it by the Supreme Court of Ireland, and in Joined Cases C 793/19 SpaceNet and C 794/19 Telekom Deutschland (20 September 2022)[31], referred by the Federal Administrative Court of Germany.

In its recent judgments, the CJEU followed the direction set out in its previous rulings, including *Privacy International*[32], *La Quadrature du Net and Others*[33] and *Prokuratuur*[34], which concern conditions of retention and access to data related to electronic communications and data retention for the purpose of criminal investigations and prosecutions.[35]

Accordingly, the CJEU confirmed that EU law does not allow, as a preventative measure, general and indiscriminate retention of traffic and location data relating to electronic communications, for the purposes of combating serious crime and preventing serious threats to public security. By contrast, some legislative measures that provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, are allowed under certain conditions:

- *The general and indiscriminate retention of traffic and location data* for a period that is limited in time to what is strictly necessary but which may be extended, in situations where the EU Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable;
- *The targeted retention of traffic and location*

data which is limited, according to the categories of persons concerned or using a geographical criterion (e.g. the average crime rate in a particular geographical area) for a period that is limited in time to what is strictly necessary, but which may be extended;

- *The general and indiscriminate retention of IP addresses* assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary, but which may be extended;
- *The general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems* (it is noted that this measure is not dependent on the seriousness of a crime and thus is applicable for the purposes of combating any type of crime (crime in general)); and
- *The expedited retention (quick freeze) of traffic and location data* which is in the possession of electronic communications' service providers for a specified period of time.

In addition, the CJEU ruled that, in order to ensure full compliance with strict conditions of access to personal data such as traffic and location data, access by the competent national authorities to the retained data must be subject to a prior review carried out either by a court or by an independent administrative body.

Moreover, the national legislation must ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

The absence or limited scope of the data retention frameworks for the purpose of criminal investigations and prosecutions proved to be one of the most pressing and ever-recurring issues faced by EU judicial authorities when requesting digital data from other EU Member States. The current legislative gap at the EU level on data retention in the frame of criminal proceedings leads to the loss of data. Therefore, the EU judicial authorities are looking forward to EU-wide legislative efforts to regulate data retention for the purposes of criminal procedures.

Data preservation in EU Member States

Data preservation is a targeted law enforcement measure aiming to conserve and maintain the safety and integrity of any type of data (non-content as well as content data) which may have an evidentiary value in the context of a specific criminal investigation. As opposed to data retention, data preservation is a reactive process and can only be applied from the moment a criminal investigation has been initiated and a preservation order has been issued.

The effective safeguards for the persons concerned must be ensured by the applicable substantive and procedural rules, providing that data is preserved by the competent law enforcement or judicial authorities for the sole purpose of criminal investigation.

In this respect, the vast majority of EU

Member States surveyed (22 out of 24) indicated that they have a regime for data preservation in place in relation to data held by OSPs, while just a small minority indicated not having such a regime in place. Similar data were collected in the previous' report.

The majority of the EU Member States which indicated that they have a data preservation regime in place provided additional explanations and/or extracts of their national legislation, as further set out in Table 17.

Is there a data preservation regime in place in your country in relation to data held by the OSPs?

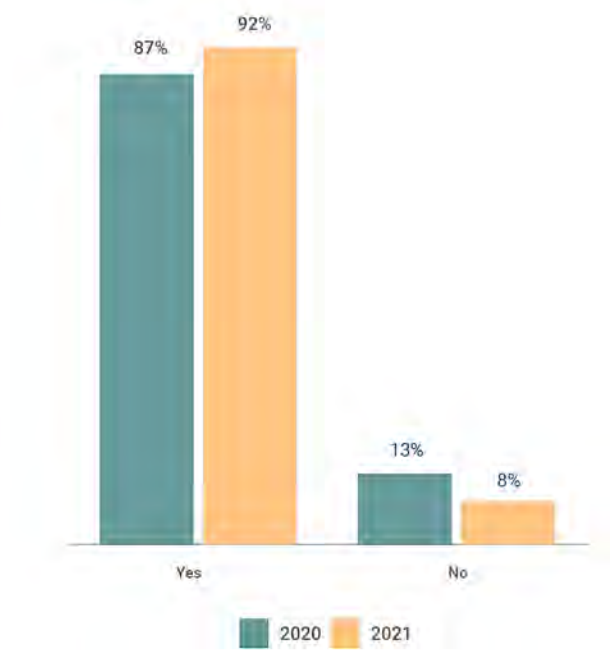


Table 17: EU Member States with a data preservation regime in place

Czech Republic	90 Days, could be extended.
Latvia	Every available data connected to a user.
Luxembourg	Any data available may be preserved upon request by the state prosecutor. Article 48-25 of the "Code de procédure pénale" (https://legilux.public.lu/eli/etat/leg/code/procedure_penale/20211226), states that: "When there is reason to believe that data stored, processed or transmitted in an automated data processing or transmission system, which are useful for the determination of the truth, are likely to be lost or altered, the State Prosecutor or the investigating judge to whom the matter is referred may have such data promptly and immediately preserved for a period not exceeding 90 days."
Netherlands	Article 126ni Penal Procedure Code.
Portugal	The Portuguese law transposed into the domestic legal framework the full provision of Articles 16 and 29 of the Budapest Convention. Thus, it is possible to preserve all types of data.
Slovak Republic	[T]here is a provision of Section 91 of the Code of Criminal Procedure available: Section 91 Preservation, Disclosure and Withdrawal of Computer Data (1) If the preservation of the stored computer data is necessary for the clarification of the facts necessary for the criminal proceedings, including transactional data that is stored through a computer system, the presiding judge and, before the commencement of the criminal proceedings or in the preliminary hearing, the prosecutor, may issue an order that must be justified even by the merits, to the person who possesses or controls such data, or the provider of such services to a) preserve such data and maintain the integrity thereof, b) allow the production or keeping of a copy of such data, c) disable access to such data, d) remove such data from the computer system, e) release such data for the purposes of the criminal proceedings. (2) In the order under Subsection 1 Paragraphs a) or c), a period during which the data preservation shall be performed must be determined. This period may be up to 90 days, and if its re-preservation is necessary, a new order must be issued. (3) If the preservation of the computer data, including the transactional data for the purpose of the criminal proceedings is no longer necessary, the presiding judge and, before the commencement of the criminal proceedings or in the preliminary hearing, the prosecutor, shall issue an order for the revocation of the preservation of such data without undue delay.

Slovak Republic *(continued)*	4) The order under Subsections 1 through 3 shall be served to the person who possesses or controls such data, or to the provider of such services, and they may be imposed an obligation to maintain the confidentiality of the measures specified in the order. 5) The person who possesses or controls the computer data shall release such data or the provider of services shall issue the information regarding the services that are in their possession or under their control to those who issued the order under Subsection 1 or to the person referred to in the order under Subsection 1. 6) If the person who possesses or controls computer data fails to release such data on the basis of an order referred to in paragraph 1, such data may be taken by the authority that issued an order under paragraph 1 or by a person specified in an order under paragraph 1.
Slovenia	Article 149e Criminal Procedure Code: (1) If there are grounds for suspicion that a criminal offence prosecutable ex officio has been committed, is being committed, is being prepared or organised, and if, for the purpose of detecting, preventing or proving this criminal offence or detecting the perpetrator, it is necessary to obtain data stored in electronic form that must be obtained under a court order in accordance with this or some other Act, but such data are likely to be deleted or altered by the time the order is delivered, the state prosecutor or the police may request that the holder, user or IT operator or the information service provider save the information without undue delay until the court order is received, but for not more than thirty days after the delivery of the request. The state prosecutor or the police may extend the time limit by a maximum of thirty days by an additional request. If a court order is not served on the holder, user, IT operator or information service provider within the period set for saving the data, such saving of data shall be cancelled. This can be requested for traffic, content data, location data. The saving of traffic data or information on the content of communication by the IT operator or information service provider may be requested only for the purpose of uncovering, preventing or proving the most serious criminal offences that are listed in [the Criminal Procedure Act], or for the purpose of uncovering the perpetrator of such criminal offence.
Spain	Article 588g of the Criminal Prosecution Act, which implements art. 16 of the Budapest Convention, provides: Order of preservation of data. The Public Prosecutor's Office, or the Judicial Police, may require any natural or legal person to preserve and protect specific data or information contained in a computer storage system to which it has access until the relevant judicial authorisation for its assignment is obtained; in accordance with the provisions of the preceding articles. The data will be kept for a maximum of ninety days, which may only be extended once until the allocation is ordered or one hundred and eighty days have elapsed. The requested party shall be obliged to cooperate and keep secret the performance of this legal measure and shall be subject to the liability described in paragraph 3 of Article 588b e.
Sweden	A public prosecutor can issue a preservation order for up to 90 days. It can be prolonged for up to 90 days if needed. It is the same term for all data categories.

G. The long-lasting impact of the COVID-19 pandemic on the acquisition of electronic evidence

The outbreak of the COVID-19 pandemic in 2020 has changed the working conditions of judicial authorities, in some cases permanently. Last year, judicial authorities were asked to indicate both positive and negative effects of the pandemic and related measures which they experienced in their daily work during 2020. This year, the most common effects previously identified were listed to the respondents in order to identify which ones were still applicable in 2021.

The majority of the respondents from the EU Members States surveyed (60%) stated that they have witnessed an increase of cases related to cybercrime. At the same time, the pandemic has also led to some positive outcomes, derived from the increased digitalisation of work, such as the use of video conferencing tools and faster communication via electronic channels.

Which of the following aspects, caused by the COVID-19 pandemic, were still applicable in relation to the acquisition of electronic evidence in 2021?

H. The European Judicial Network perspective: key elements for the MLA request for the electronic evidence in hate crimes

Difficulties in obtaining electronic evidence are particularly apparent in the fight against hate crimes committed online. The identification of perpetrators often relies on cooperation with foreign authorities, including the US. During the 58th Plenary meeting of the EJN, EU Member States indicated that the execution of MLA requests in the US in hate crime cases is often refused due to the concept of freedom of expression enshrined in the First Amendment of the Constitution of the US[36]. Judicial cooperation in connection with these types of crimes can require the need to establish probable cause of a crime in the text of the MLA request, when seeking certain types of evidence. When it comes to cooperation inside the EU, the current legal framework provides relatively smoother ways to obtain electronic evidence, in terms of both time, and the absence of the First Amendment considerations that may apply to requests to the United States.

Hate crimes are usually committed by publishing posts with offensive content on online platforms. Therefore, for the investigation of such crimes, it is important to have information about the account(s) used for publishing such posts. Depending on where it is stored, this information is generally obtained via MLA requests.

In general, for the successful outcome of an MLA request, it should be as complete as possible, being in line not only with the law of the requesting state, but also the in line with requirements of the state that is going to execute it.

Due to the unique nature of hate crimes, MLA requests for electronic evidence, especially from the US, should be prepared with particular attention. Even though the US may not be able to fully execute certain requests because of the First Amendment, there are cases in which the US can provide assistance because the speech in question is not protected by the First Amendment. Although these are not guarantees that any given request for assistance will be granted,

below are some tips, based on EU Member State practitioner experiences, in making MLA requests to the US in hate crime cases:

1. A description of the author of the publication

The MLA request should contain a description of the alleged perpetrator, and any background information relating to the perpetrator that may provide context for the hate crime publication, including previous incidents and/or convictions.

2. The audience

Based on the experience of EU Member State practitioners, the addressees and/or readers of the publication may potentially be considered when deciding whether a request can be executed, in combination with other factors such as the threat of violence as described directly below.

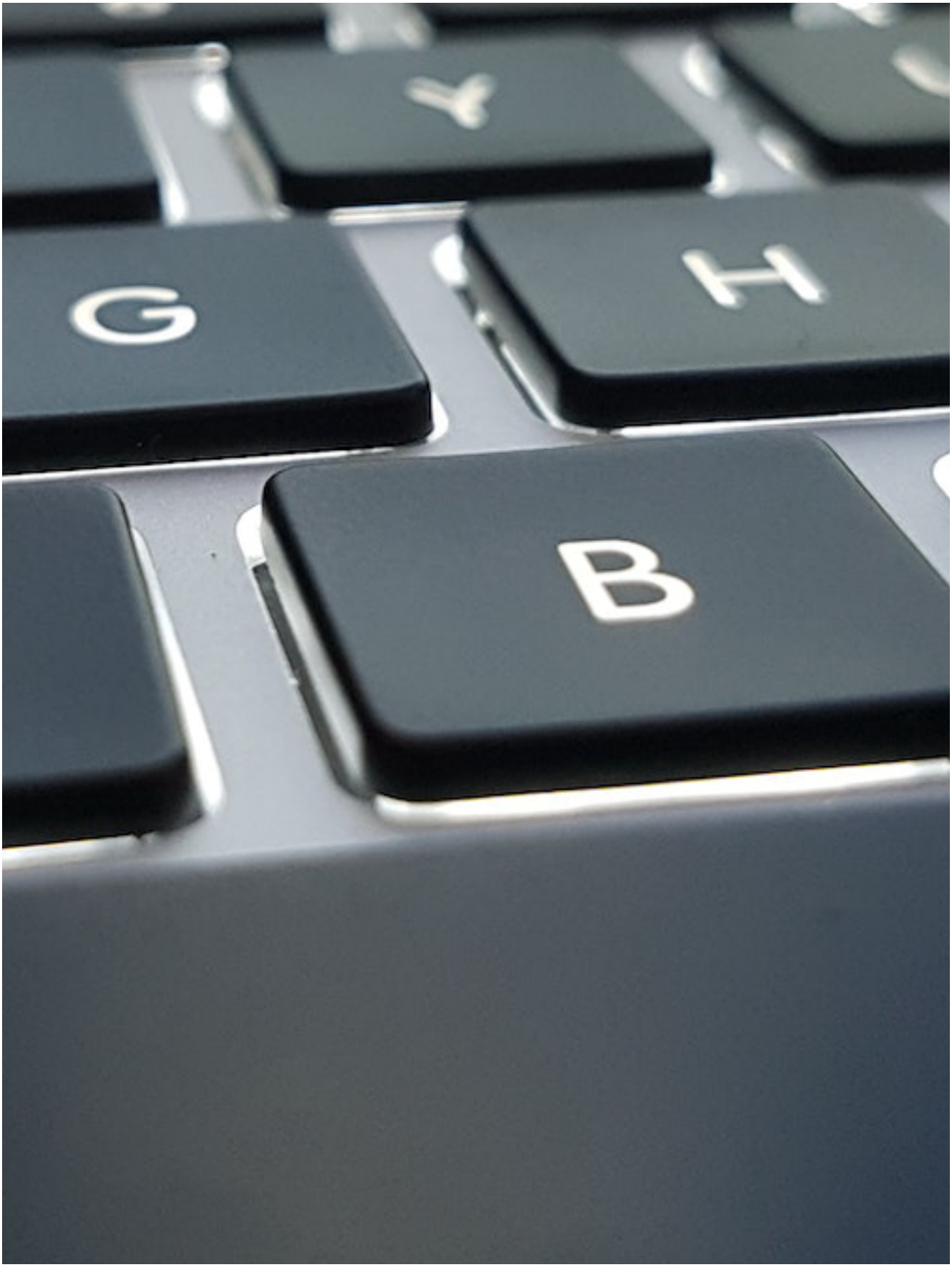
3. Threat of violence

Based on the experience of practitioners, MLA requests are more likely to be executed if they refer to an offensive publication that, in addition, contains elements of threat, e.g.:

- Incitement to commit criminal acts, including to cause physical harm to an individual or to a group of people; or
- Soliciting somebody to commit a crime; and
- The threats are considered real (a serious expression of an intent to commit an act of unlawful violence) by a potential victim, or by other members of the audience.

4. Links between targeted account(s) and alleged perpetrator(s)

To meet the requirements of probable cause, an MLA request, inter alia, should contain a description of the link between the account(s) where the post was published, and the alleged perpetrator(s).

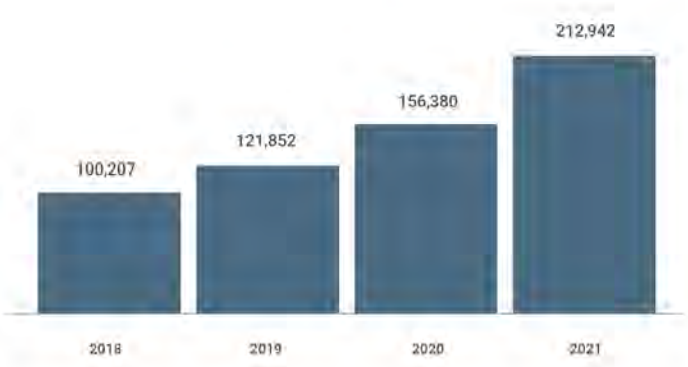

Y
G
H
B

PERSPECTIVE OF ONLINE SERVICE PROVIDERS

A. Volume of data requests per country and per Online Service Provider

Many OSPs publish annual Transparency Reports describing the volume of requests for user data that they received. These reports offer a valuable source of information to understand the situation of the use of electronic evidence in the EU.

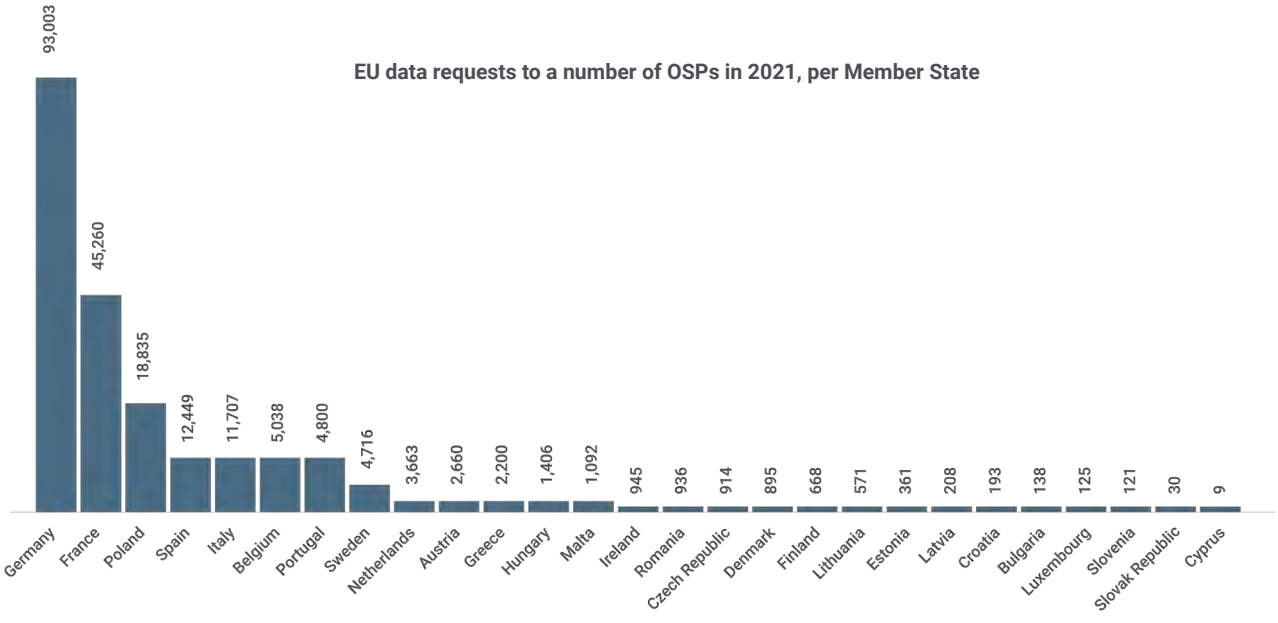
EU data requests to a number of OSPs from 2018 to 2021



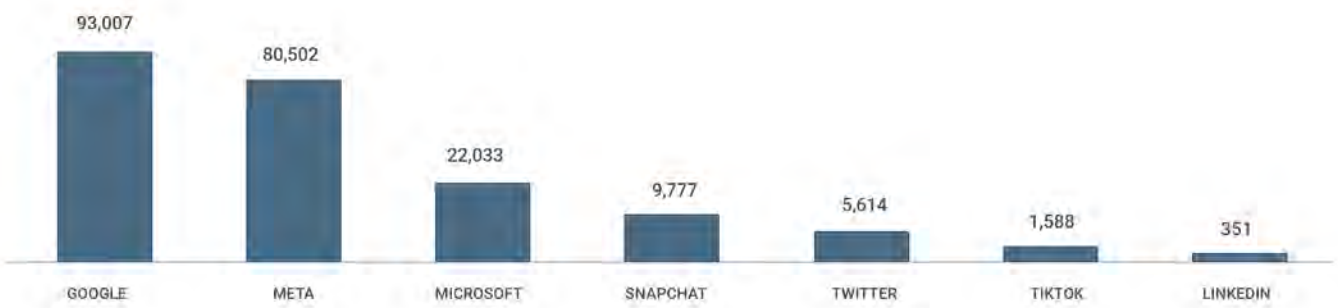
For instance, data from seven OSPs show there was an increase of 36% in the volume of requests from EU competent authorities for the disclosure of user data in the context of criminal investigations from 2020 to 2021. This is the highest increase in volume observed since 2018, when the first SIRIUS EU Digital Evidence Situation Report was published, indicating there is an exponential growth in the importance of electronic evidence.

Germany and France account for 65% of all the EU requests to the seven OSPs analysed in 2021. Among these OSPs, 81% of the EU requests were submitted to Google and Meta.

EU data requests to a number of OSPs in 2021, per Member State



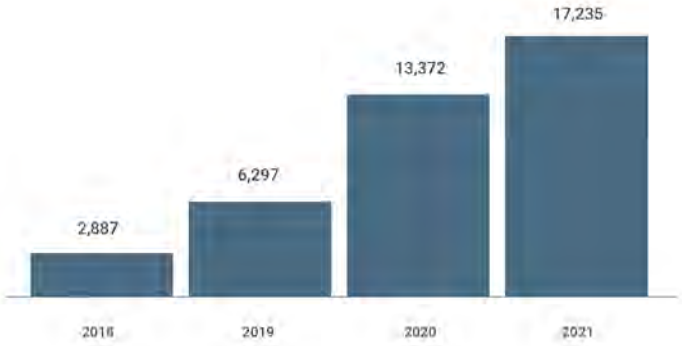
EU data requests to a number of OSPs in 2021, per company



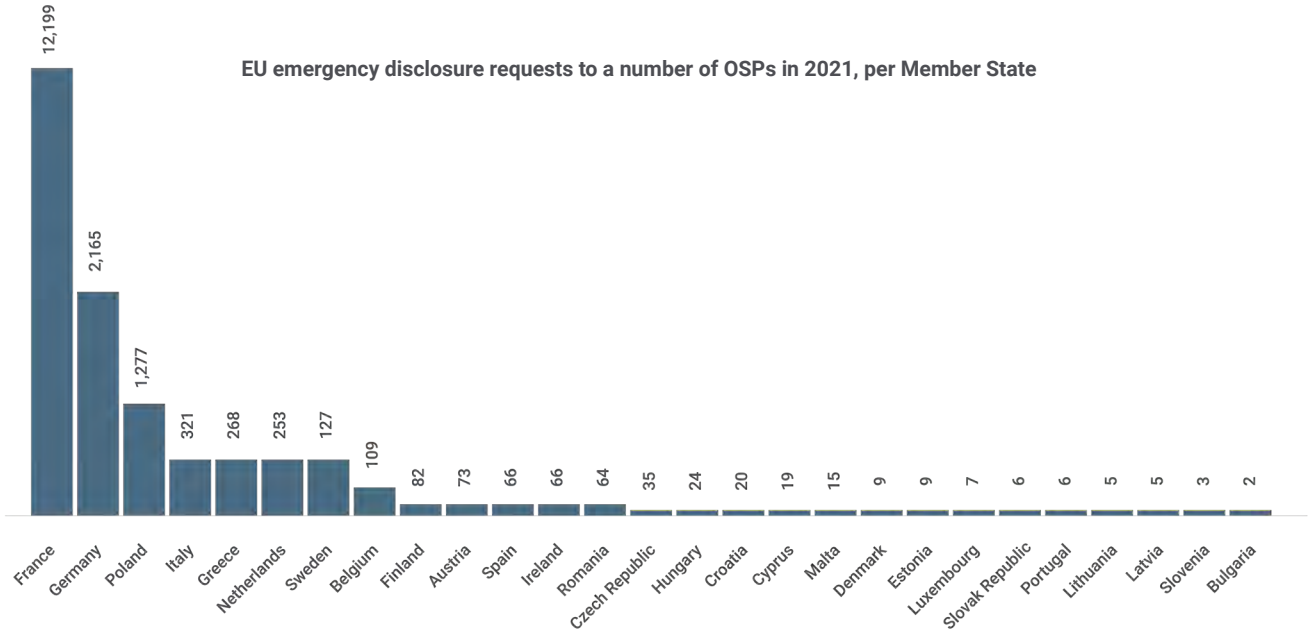
B. Volume of Emergency Disclosure Requests per country and per Online Service Provider

The volume of EDRs to OSPs increased 29% from 2020 to 2021[37]. The total of EU EDRs was strongly influenced by the requests from France, which account for 71% of all the requests in emergencies, being the vast majority of them to Meta.

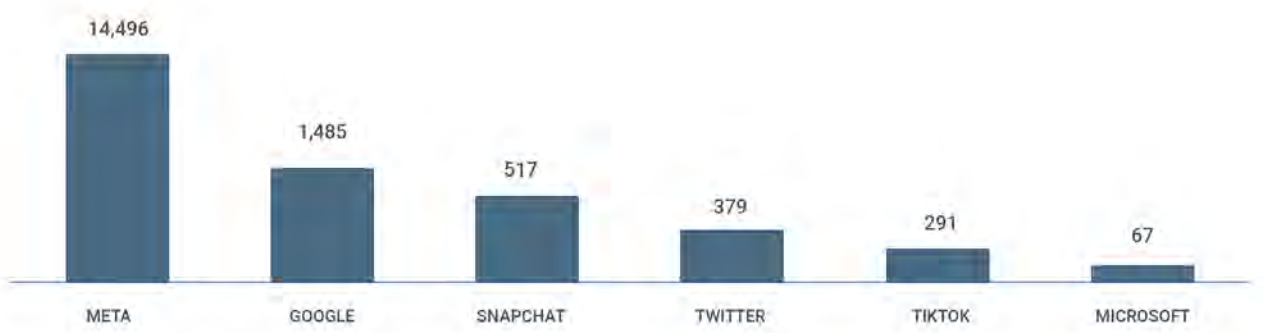
EU emergency disclosure requests to a number of OSPs from 2018 to 2021



EU emergency disclosure requests to a number of OSPs in 2021, per Member State



EU emergency disclosure requests to a number of OSPs in 2021, per company

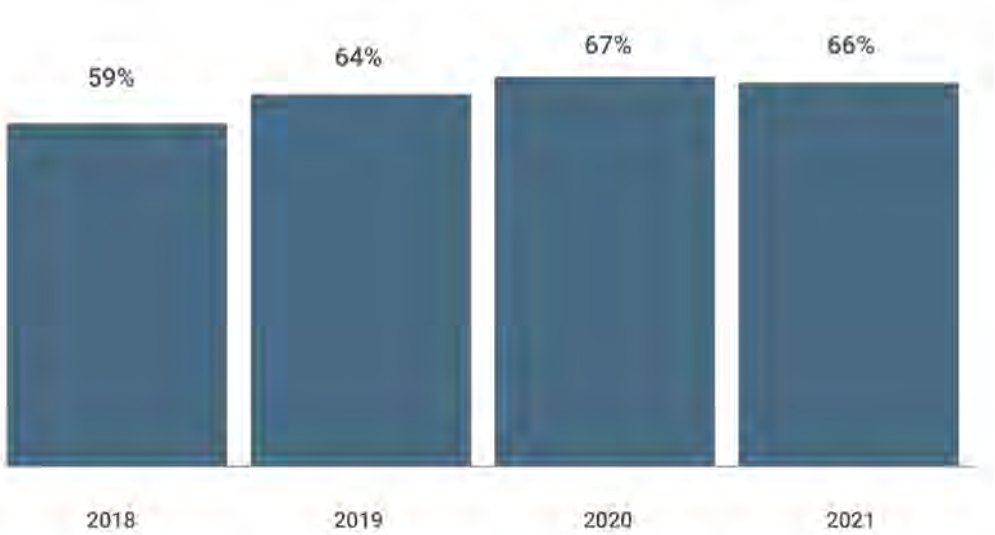


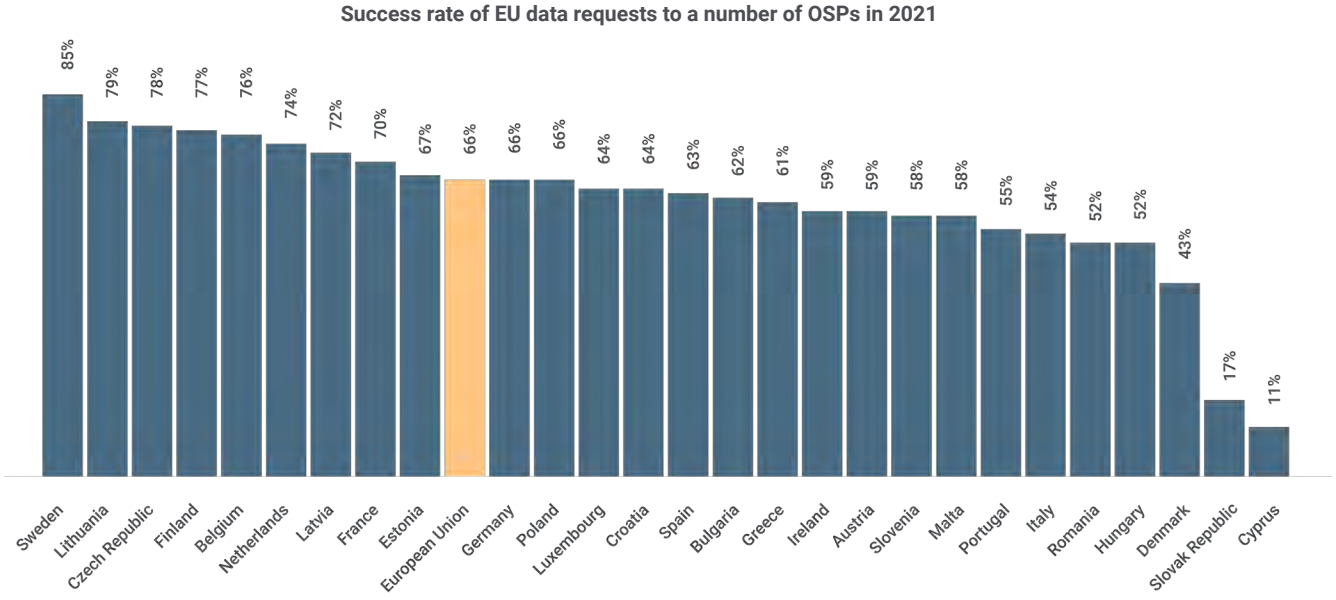
C. Success rate of EU cross-border requests for electronic evidence

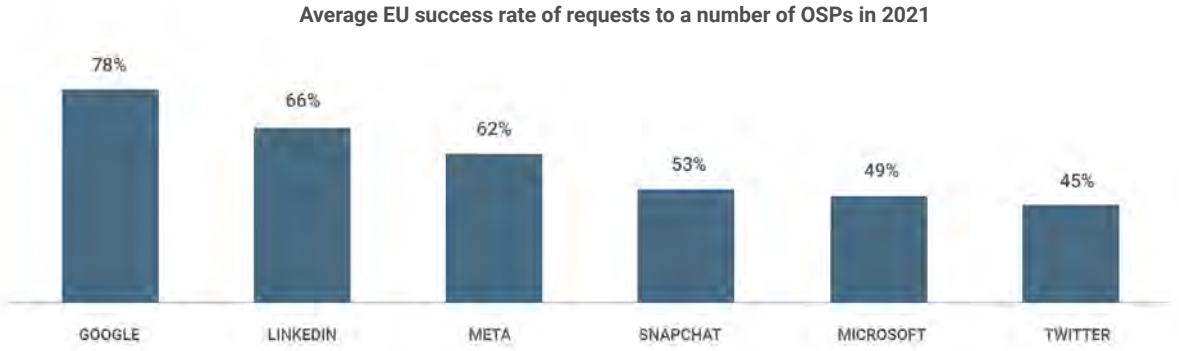
The average success rate of EU data requests slightly decreased from 67% in 2020 to 66% in 2021. This percentage represents the amount of requests which led to the disclosure of at least some data to competent authorities.

The first six countries with highest success rate were Sweden, Lithuania, Czech Republic, Finland, Belgium and Netherlands, all of which count with SPoCs established in their respective law enforcement agencies. Moreover, 78% of EU requests to Google were successful, the highest success rate among the OSPs analysed.

Average EU success rate of requests to a number of OSPs from 2018 to 2021







D. The experience of Online Service Providers with Single Points of Contact

SPoCs for cross-border data disclosure requests to foreign-based OSPs 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 OSPs under voluntary cooperation in a centralised manner.

Depending on the applicable national legal framework and internal working processes, SPoCs may also perform other tasks as they pertain to cross-border access to electronic evidence, as further detailed below.

SPoCs perform tasks that include:

- Channelling cross-border data disclosure requests under voluntary cooperation from national competent authorities to one or more foreign-based OSPs in a centralised manner;
- Ensuring that requests are compliant with the applicable domestic laws, as well as OSPs' policies and other requirements;
- Reviewing and/or validating the requests

for voluntary cooperation in accordance with the established working procedures and/or otherwise providing legal or policy-related advice to the requesting competent authorities;

- Rejecting non-compliant requests;
- Receiving responses from OSPs and forwarding them to the requesting officer; and
- Engaging with representatives of relevant OSPs on matters pertaining to cross-border data disclosure under voluntary cooperation and other relevant matters.

Most OSPs consider the SPoC approach as highly beneficial to the overall process of data disclosure in criminal investigations, as these units act as quality filters for requests for data, leading to less frictions and higher success rates. For instance, the analysis of Transparency Reports from seven OSPs demonstrate countries with SPoCs had a success rate 8% higher than those countries without SPoCs.

Average success rate of countries with or without an established SPoC for centralisation of requests to OSPs in 2021

Some OSPs reported that they are dedicating resources to actively create working arrangements with SPoCs in countries where they are not yet implemented. In this context, the benefits reported by OSPs in relation to the SPoC approach are:

- Working with a SPoC contributes to increased quality of requests and, in consequence, 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 may be disclosed. Additionally, some OSPs reported that the rejection rate of requests submitted by SPoCs is considerably lower when compared to the national average;
- 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 authorities benefit from the provided information;
- Establishing SPoCs helps to minimise duplication of requests regarding the same case from different units or even law enforcement agencies; and
- SPoCs are efficient tools to build greater cooperation between OSPs and law enforcement agencies.

Some OSPs which have received a low volume of requests for data disclosure from law enforcement have reported they have little or no experience in engaging with SPoCs in the EU. However, they see SPoCs as important channels to disseminate relevant information about the company's process in the future.

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

Following the submission of requests for data disclosure in the context of criminal investigations, it may often happen that OSPs and competent authorities need to communicate further to clarify aspects of the request, before any data is released. This could take place because of specific requirements that have not been met, or because the circumstances of the investigation need to be clarified. The need for communication between OSPs and authorities or for amendment of the original request may cause delays in the process of data disclosure. As a matter of fact, Section b of this chapter demonstrates that 34% of data disclosure requests in the EU have not been successful in 2021.

There is no publicly available data in relation to the main reasons for refusal or delays in processing direct requests for voluntary cooperation issued by EU authorities. However, during the interviews conducted by the SIRIUS team, OSPs have provided information on the most common issues encountered, which are presented below, not classified by order of importance.

- **Procedural issues**

Requests for disclosure of data are often delayed or rejected due to procedural issues such as missing dates, the fact that no legal basis is mentioned, lack of signature or even because they are addressed to the wrong legal entity.

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

Most OSPs 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 or persons and how the data sought may help to avert it. What may occur in practice is that, for example, due to confidentiality concerns or extreme time pressure, authorities may not provide complete details of the incidents, which may lead the OSPs to request supplementary information. Moreover, there can also be different interpretation of emergencies, or lack of understanding from untrained officials regarding the necessary thresholds.

- **Lack of sufficient context about the case under investigation**

Similarly to the issue previously identified in the case of emergencies, requests may also lack the necessary details about the case under investigation in non-emergency circumstances. Most OSPs require authorities to identify the nature of the case and to justify why the data is needed in the context of a criminal investigation. If there is no clear connection between the data requested and

the case under investigation, OSPs may request supplementary information, which can lead to delays in the process, or even reject the request altogether.

- **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 OSP to locate the specific account of interest. Commonly accepted identifiers are e-mail addresses, phone numbers with country code or platform-specific unique usernames. Furthermore, a mistake as simple as typos in the identifiers may also lead the OSP to believe the targeted account does not exist.

- **Linguistic barriers**

OSPs 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 OSPs and authorities may be required, and in some cases requests may need to be amended.

- **Jurisdictional challenges**

Some OSPs 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, several OSPs 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.

Similarly, as OSPs must respect the domestic legislation where 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 the country that they are based in.

- **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 which services of the OSP are of concern, define a specific and narrow timeframe of relevance for the information sought or list the specific datasets that are being requested. For instance, requests that include language requiring "all available data" concerning specific account(s) are generally considered to be overly broad.

- **Lack of reply from authorities when OSPs asks for additional information**

When OSPs require additional information to process a request, they generally reach out to the competent authority using the

same channel used for the submission of the request. In such situations, authorities may mistakenly understand that the OSP 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 rejection of requests.

F. Existing and future challenges from the perspective of Online Service Providers

Representatives of the OSPs interviewed for the purpose of this report have discussed the existing and future challenges in matters related to electronic evidence. Several of them reported significant improvements in the process of engaging with EU competent authorities in the context of criminal investigations in the last five years. This positive trend is a result of a better understanding and preparedness both from the side of public authorities and the OSPs themselves, many of which have dedicated teams to deal with requests for data from authorities.

While there are still challenges in the process, OSPs report overall improvements in the level of awareness of EU law enforcement officers, better quality of requests and higher acceptance of the use of online portals, for example. Some of the OSPs have also praised the work of SIRIUS and acknowledged its important role in facilitating access to relevant information, training law enforcement officers and promoting the sharing of best practices. In addition, some OSPs praised previous SIRIUS EU Digital Evidence Situation Reports, noting that this annual document is important for stakeholders to better understand each other and improve their own processes.

In this context, the four existing and future challenges listed below have been identified by several OSPs.

- **Ensuring the authenticity of requests**

Several OSPs mentioned that ensuring the authenticity of requests for data from law enforcement is an area of concern. Specifically, they want to make sure that data is disclosed to authorised officials only and that bad actors are not exploiting the existing processes for engagement with law enforcement. Most OSPs use the e-mail domain of the requester as one of the criteria to authenticate incoming requests. Some even use the repository of EU official e-mail domains provided by SIRIUS, as part of the SIRIUS Programme for OSPs. However, many OSPs take into account that e-mail addresses of authorities could be compromised and therefore implement additional checks, taking into account the IP address that originated the message or authenticating dubious requests via phone calls to trusted contacts. Moreover, the creation of online portals dedicated to law enforcement, as well as the establishment of working arrangements with SPoCs are seen as beneficial to verifying the authenticity of requests.

- **Proactively reporting emergency situations to local competent authorities**

Several OSPs reported having reached out to law enforcement to proactively report

emergencies. According to them, the process works very well in the US, where most of the OSPs interviewed indicated that they have direct engagement with the US Federal Bureau of Investigations. In the EU, the process of reaching out to local police authorities, especially in emergency cases, appears more challenging, as OSPs often rely on points of contact previously established in the concerned country or use open source information about local police stations. The main challenges in this process are identifying the correct 24/7 emergency point of contact in a foreign country and dealing with language barriers.

- **The impact of the metaverse on electronic evidence**

Most OSPs acknowledged that it is too early to assess what will be the impact of future online technologies in the electronic evidence acquisition process and not all of them are investing in areas such as AI, AR and VR.

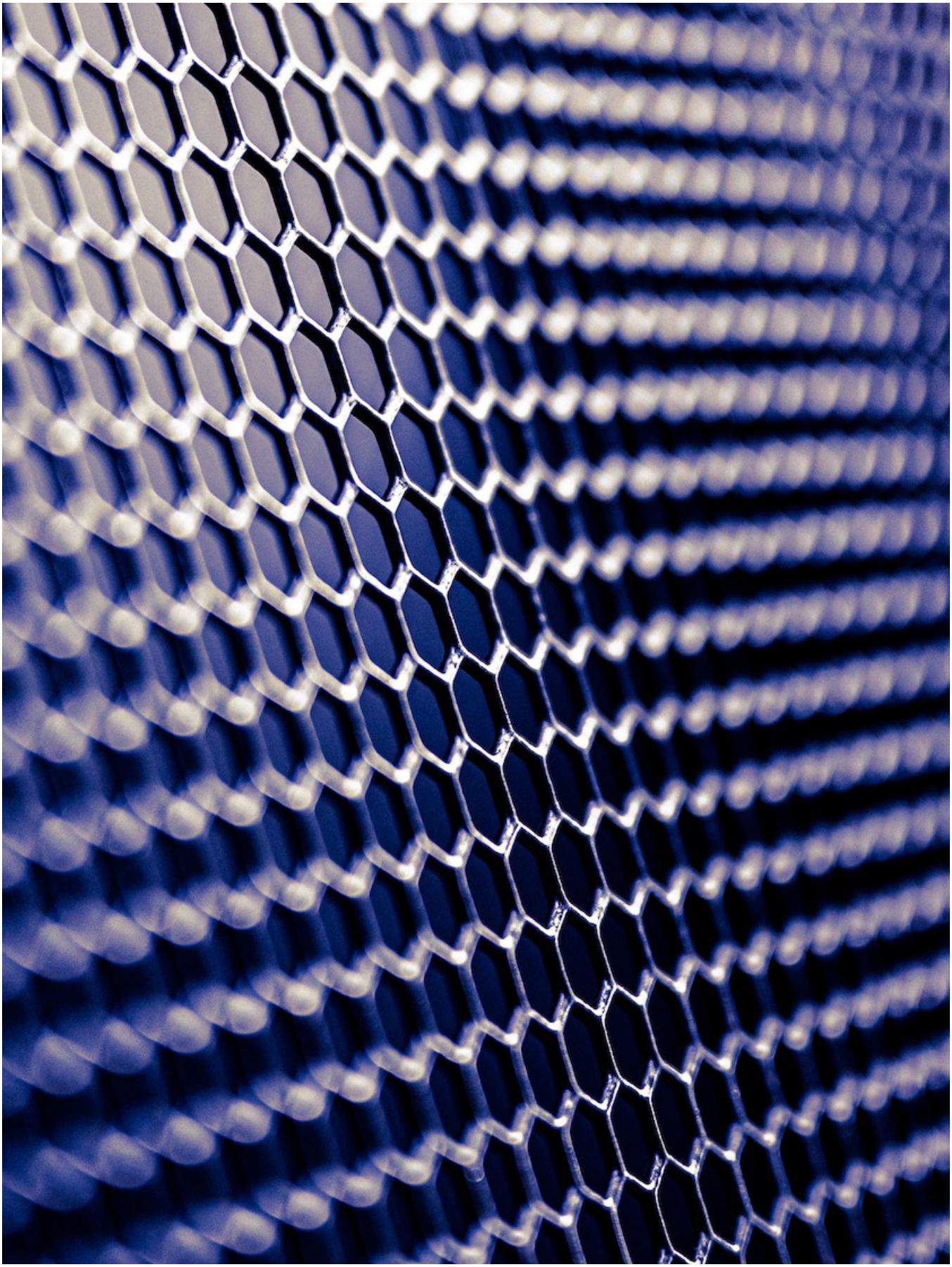
Some OSPs believe that the increased volume of collected data could lead to a higher volume of requests for data disclosure in the context of criminal investigations in the future.

One OSP acknowledged that the team dealing with law enforcement requests is currently not involved in the launch of new products and services, but that moving forward, there might be a need for better coordination among internal teams, in order to minimise the impacts to the electronic evidence process.

Another OSP has highlighted that VR may present important challenges to law enforcement in the future. There may be potential evidence that only exists in the 3D virtual world. For example, a user might have software in the 3D virtual space that builds a swastika in front of other users, but that is not an image per se, if one does not take a screenshot of it. Additionally, actions performed in VR do not necessarily take place in the real world. Therefore, an illegal action that took place in VR did not happen per se in the real world and one may not even be able to produce physical proof of it.

- **Difficulty in disseminating information to a high number of officers in a position to submit requests for data**

As the importance of electronic evidence increases in criminal investigations, so does the number of law enforcement officers who need to submit requests for data to OSPs. Training and outreach activities addressed to an increasing number of officials worldwide represent a challenge for OSPs. Most OSPs believe that the establishment of SPoCs in law enforcement agencies facilitates the dissemination of relevant information, leading to higher quality of requests. Moreover, some OSPs also mentioned that they are increasing the resources dedicated to performing active outreach to law enforcement.



RECOMMENDATIONS

A. For EU Law Enforcement Agencies

1. Create or expand the capacity of units acting as SPoCs for cross-border data disclosure requests under voluntary cooperation

As noted in previous chapters, SPoCs can improve the speed and effectiveness of cross-border requests for electronic evidence under voluntary cooperation. Therefore, it is recommended that such units are created or expanded within EU competent authorities, considering the exponential increase in volume of requests in recent years. Moreover, it is also recommended that existing SPoCs should have the required knowledge and resources to deal with electronic evidence pertaining to AI, AR and VR technology and understand how these can be abused by criminals.

2. 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. As this need continues to grow, it is recommended that training activities on cross-border access to electronic evidence are included in routine training programmes for investigators and first responders.

3. Ensure the security of e-mail systems, including the obligatory use of strong passwords and two factor authentication to all law enforcement officers

There is a growing concern among OSPs that bad actors may try to gain access to law enforcement e-mail services in order to send fake data disclosure requests to companies. Therefore, EU law enforcement agencies should deploy the obligatory use of strong passwords that have to be changed regularly and two-factor authentication to all e-mail accounts, as well as continuously invest in the security of their internal systems. If possible, law enforcement agencies should also digitally sign e-mail messages sent to OSPs[38].

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

B. For EU Judicial Authorities

1. Strengthen capacity on different modalities and specific procedures for requesting and obtaining electronic data

Capacity-building of the EU judicial community is essential. Constant training on the different modalities and specific procedures for requesting and obtaining data disclosure can ensure that the EU judiciary has the required knowledge and skills to properly identify and rely on appropriate investigative and prosecutorial solutions that

match the specific needs of a case, to the benefit of all stakeholders involved — States, service providers and their users, and civil society.

In this regard, EU judicial authorities are strongly encouraged to use and benefit from the support and resources offered by EU actors active in the field of judicial cooperation, including Eurojust, the EJN, the EJCN and the SIRIUS Project.

2. Enhance mutual trust, exchange of expertise and best practices among EU judicial practitioners on cross-border access to electronic evidence

Recognising the challenges faced by EU judicial practitioners in an exponentially growing field of data digitalisation and evolution of technologies, it is of paramount importance to enhance mutual trust among judicial authorities in the EU so as to increase the interoperability of their daily efforts as well as foster knowledge sharing and exchange of best practices on accessing electronic evidence from different jurisdictions.

In this regard, EU judicial authorities are strongly encouraged to actively engage with the judicial community in the dedicated fora on the SIRIUS restricted platform. These contain, alongside first-hand experiences and know-how on different angles from which cross-border access to electronic evidence can be approached, updates on relevant developments in the area.

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

C. For Online Service Providers

1. Take measures to identify and prevent fake requests for data disclosure from unauthorised persons

It is highly recommended that OSPs build resilience against disclosing data to unauthorised persons. To achieve this, OSPs should put in place mitigation measures such as making use of the SIRIUS repository of official EU e-mail domains, providing training to staff to identify e-mail spoofing, promoting proactive outreach to EU law enforcement to authenticate data disclosure requests, engaging with trusted points of contact within law enforcement to verify dubious requests and deploying technical solutions to authenticate incoming requests for user data in the context of criminal investigations.

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

OSPs 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 OSPs 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.

3. When launching new products and services, especially in relation to AI, AR and VR, consider their impact on electronic evidence

When launching new products and services, especially in relation to AI, AR and VR, OSPs should ensure their Law Enforcement Response Teams are adequately prepared to deal with requests from competent authorities for new datasets.

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

ENDNOTES

1 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://bit.ly/3FuJrWI.

2 Europol and Eurojust Joint Report, Common challenges in combating cybercrime, as identified by Eurojust and Europol, June 2019, available at: https://bit.ly/3PxCCbK

3 https://bit.ly/3PBFILO

4 https://bit.ly/3HB0PM3

5 Austria, Belgium, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain and Sweden.

6 https://bit.ly/3htBV6x

7 SIRIUS EU Digital Evidence Situation Report 2021.

8 For example: Facebook, Google, Twitter and Uber

9 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021, 7 December 2021; Europol, European Union Terrorism Situation and Trend report 2022 (TE-SAT), 13 July 2022.

10 Europol, https://bit.ly/3srv7rX, 3 October 2022

11 https://bit.ly/3gE8tKm

12 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).

13 The category of "subscriber information" as set out in the Budapest Convention on Cybercrime is also widely referred to as "basic subscriber information".

14 All data referring to 2020 has been rounded to allow immediate comparison with 2021 data.

15 Article 18 – Production order. Available at: https://rm.coe.int/1680081561.

16 https://bit.ly/3zA4bdJ

17 The term "domain name registration information" is intended to cover information for "identifying and contacting the registrant of a domain name" (Explanatory Report to the Second Additional Protocol to the Budapest Convention, para. 76). "Information […] for identifying or contacting the registrant of a domain name'" refers to information previously publicly available through WHOIS lookup tools, such as the name, physical address, email address and telephone number of a registrant. Some Parties may consider this information a subset of subscriber information as defined in Article 18(3) of the Budapest Convention (Explanatory Report to the Second Additional Protocol to the Budapest Convention, para. 81).

18 Article 32 – Trans-border access to stored computer data with consent or where publicly available. Available at: https://rm.coe.int/1680081561.

19 Pertaining to production orders of data within a person's or a service providers' possession or control, where such person is within your state's territory or such service provider is offering services within your state's territory.

20 Pertaining to trans-border access to stored computer data with the consent of the person who has the lawful authority to disclose the data or where the data is publicly available.

21 Pertaining to direct requests for domain name registration information to OSPs situated abroad, which are in possession or control of such information.

22 Pertaining to direct orders for subscriber information to OSPs situated abroad where such information is within their possession or control.

23 Pertaining to interception of telecommunications authorised by one Member State of a subject located in another Member State, from which no technical assistance is required.

24 SIRIUS EU Digital Evidence Situation Report 2021 and SIRIUS EU Digital Evidence Situation Report 2020

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

26 According to the views of the industry gathered in individual interviews with different OSPs.

27 See, for example, Facebook, Information for law enforcement authorities; Twitter, Guidelines for law enforcement; and Microsoft, Questions about Microsoft's law enforcement requests practices.

28 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://bit.ly/3yScwsD

29 https://bit.ly/3Yo6paF

30 https://bit.ly/3FVfBfC

31 https://bit.ly/3HEU5wW

32 https://bit.ly/3j5884H

33 https://bit.ly/3WjDfHR

34 https://bit.ly/3Wj0x0p

35 More detailed information for the mentioned data retention related case law is available in the SIRIUS EU Digital Evidence Situation Report 2021.

36 Amendment I (1791): Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. https://bit.ly/2pKiOqx

37 The analysis of EDRs does not include data from LinkedIn, as this company does not report on EU EDRs separately.

38 For example, adding digital signature to an e-mail message is possible with Microsoft Outlook as indicated at https://bit.ly/3Fb3mLV

REFERENCES

All links were accessed in September 2022.

- Google Transparency Report
- LinkedIn Government Requests Report
- Meta Government Requests for User Data
- Microsoft Law Enforcement Requests Report
- Snap Inc. Transparency Report
- TikTok Information Requests Report
- Twitter Information Requests

ACRONYMS

- AI: Artificial Intelligence
- AR: Augmented Reality
- CJEU: Court of Justice of the European Union
- EDR(s): Emergency Disclosure Request(s)
- EIO: European Investigation Order
- EJN: European Judicial Network
- EU: European Union
- IP: Internet Protocol
- MLA: Mutual Legal Assistance
- OGP(s): Online Gaming Platform(s)
- OSP(s): Online Service Provider(s)
- SPoC(s): Single Point(s) of Contact
- UK: United Kingdom
- US: United States of America
- VR: Virtual Reality