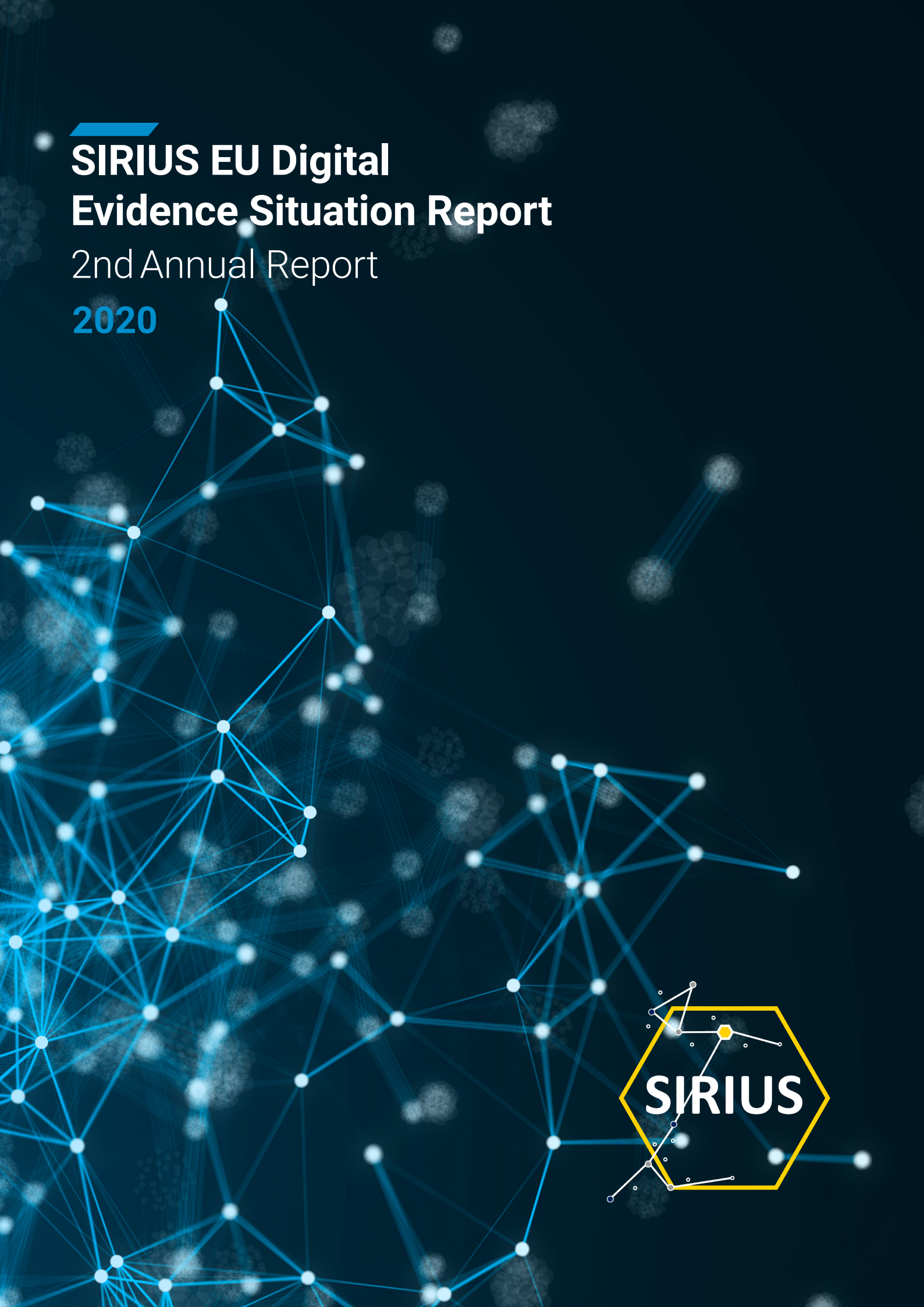
SIRIUS EU Digital Evidence Situation Report

2nd Annual Report

2020



2ND 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 grant agreement No PI/2017/391-896.
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

Catherine De Bolle

EXECUTIVE DIRECTOR, EUROPOL

It is with pleasure that I present the SIRIUS European Union (EU) Digital Evidence Situation Report 2020. This second annual flagship document provides an analysis of the access EU Member States have to electronic evidence held by online service providers, as well as its use in criminal cases in 2019.

Digital services play a critical role in the planning, execution and aftermath of crime and terrorism. The good news is that criminals often leave a digital footprint. It is with this digital footprint that successes in prosecutions can be found. The challenge lies in retrieving this information.

Since its creation in 2017, the SIRIUS project, led by Europol in strong partnership from Eurojust and with invaluable contributions from EU Member States and the European Judicial Network has become the centre of reference for EU law enforcement and judicial authorities for knowledge sharing and support in digital cross-border investigations.

The persistent relevance of electronic evidence, coupled with an increased capacity in EU Member States in requesting it, has culminated in a number of successes, including assisting the rescue of abducted and missing minors, the prevention of attacks and the identification of several terrorists, as presented in this report. There is an even greater need to take on the obstacles and challenges that both law enforcement and judicial authorities face when collecting and accessing electronic evidence. Only together can we succeed in balancing the need to investigate crimes with upholding the fundamental liberties of our system.

Ylva Yohansson

EU COMMISSIONER FOR HOME AFFAIRS

"European law enforcement has significantly improved its ability to use SIRIUS to keep people in Europe safe. When it comes to counter-terrorism, transatlantic cooperation is vital, especially in the online fight."

Ladislav Hamran

PRESIDENT, EUROJUST

This joint Report is both timely and highly relevant. It reflects the great impact of electronic evidence on all partners of the EU's security chain - from law enforcement to prosecutors, and from public to private actors.

The first part of this Report focuses specifically on the perspective of EU judicial authorities. Prosecutors and judges from across the continent have helped us to identify the obstacles and opportunities that they come across in their daily work, resulting in a concrete overview for policy-makers who want to learn more about how electronic evidence is affecting the judiciary.

I am convinced that the SIRIUS project will continue to play a pivotal role, offering practical guidance and a platform for knowledge exchange to all those who are dealing with electronic evidence. The importance of this joint endeavour cannot be overstated, because only together we can succeed in balancing the need to investigate and prosecute crimes with upholding the fundamental liberties of our citizens.

Didier Reynders

EU COMMISSIONER FOR JUSTICE

"E-evidence is of fundamental importance in a huge number of criminal investigations. Far from being limited to cybercrime, it is relevant for some 85% of criminal cases, covering every type of crime in the European Union today. In April 2018, the European Commission proposed new rules to make it easier for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute several sorts of crimes. Once adopted, the new rules should address many of the concerns raised in this year's report. I congratulate everyone who contributed to this impressive publication and I urge policy-makers to make use of this valuable insight."

EXECUTIVE SUMMARY

In a context of expanding digitalization of everyday life, electronic data also has an increasingly important role in a wide range of criminal areas. However, when it comes to cross-border data disclosure requests from authorities towards foreign-based Online Service Providers (OSPs), the existing legal framework is often considered not optimal. While policy-making and international negotiations are currently underway, **the perspectives of judicial authorities, law enforcement and OSPs themselves can shed light on how data is collected for investigation and prosecution of crime in the EU, and what the main issues are.**

EU judicial authorities in the field of electronic evidence face challenges related mainly with the retrieval of data in a time-sensitive situation. The length of procedures to formally engage with non-EU OSPs was reported as the main issue (94% of respondents) whereas, conversly, the **lack of data retention regimes in place against the extreme volatility of data** complicates the scenario. Additionally, acquisition of data is often stalled due to **the sharp increase of the challenges faced while establishing the jurisdiction/legal entity in charge of data requests.**

EU law enforcement authorities highlighted the successful use of electronic evidence in many investigations in different crime areas. The surveys conducted present similar results in comparison with the previous year. For instance, **the main issues in obtaining electronic evidence remains the same: the process required to obtain data via Mutual Legal Assistance (MLA) takes too long, and there is a lack of standardization in companies' policies.** There was an increase (+9.8%) in the number of officers that receive periodic trainings in relation to electronic evidence. Moreover, the results also show **increasing relevance of Online Gaming Platforms to criminal investigations.**

From the OSPs' perspective, from 2018 to 2019 **there was an increase of 14.3% in the volume of requests for disclosure of data**, according to transparency reports of eight companies. Germany, France and the UK continue to be the countries with the highest volume, while Poland and Finland were the countries with the highest percentage increase in comparison with 2018. **The volume of Emergency Disclosure Requests submitted by EU authorities increased by 49.7% from 2018 to 2019 and the overall success rate of requests increased from 65.9% to 68.4% in the same period.**

A chapter of this report is dedicated to the role of Single Points of Contacts (SPoCs), which are units or group of officials specialized in cross-border access to electronic evidence in EU Member States. There is no unique formal definition of SPoCs and their tasks, but they can be divided in two types: SPoCs for centralization of requests and SPoCs for knowledge-sharing and support. **In countries where SPoCs have been established, authorities and OSPs report increased efficiency in the process and faster response time in data disclosure requests.**

Finally, the report ends with recommendations to stakeholders:

For EU Judicial Authorities

- Promote national initiatives aimed at developing a clearer overview on the different available processes to request and obtain data disclosure;
- Strengthen the interconnection and knowledge exchange among EU judicial practitioners in the field of electronic evidence.

For EU Law Enforcement Agencies

- Make use of the SIRIUS platform to provide periodic training to officers dealing with cross-border requests to Online Service Providers;
- In Member States where there are not yet established, create Single Points of Contact for electronic evidence.

For Online Service Providers

- Disseminate updates about policies and changes in processes to EU authorities, also through SIRIUS;
- Publish periodic transparency reports regarding requests from EU authorities, including standardised data categories.

ABOUT THE SIRIUS PROJECT

Created by Europol in October 2017, the SIRIUS Project is a central reference in the European Union (EU) for knowledge sharing on digital cross-border investigations for law enforcement and judicial authorities. SIRIUS products and services can be easily accessed and downloaded via a web- and app-based secure platform, currently available to more than 4,500 practitioners, representing all EU Member States and 17 Third Countries with an operational agreement with Europol/ cooperation agreement or an arrangement establishing cooperation with Eurojust.

Eurojust, a partner in the project since early 2018, is expected to become a full co-beneficiary of the funded action by the end of 2020, increasing even more the judicial perspective and developing relevant knowledge products. Moreover, the European Judicial Network closely collaborates with the project and contributes to bringing important information to authorities.

The main products and services of SIRIUS include:

- Concise and practice-oriented knowledge products, such as factsheets explaining legal concepts and instruments related to electronic evidence; guidelines describing detailed processes of more than 40 Online Service Providers (OSPs) for data disclosure based on voluntary cooperation and Mutual Legal Assistance (MLA), and a database of contact details of more than 250 OSPs worldwide;
- Face-to-face and online training courses, as well as an innovative training in game format to help authorities improve the quality of their cross-border data disclosure requests and thus increase response rates, as well as remain up-to-date on latest tech developments relevant to criminal investigations;
- IT tools facilitating the structuring and interpretation of electronic data, developed by coders in Law Enforcement Authorities (LEAs) or in the framework of yearly SIRIUS Codefests;
- A Network dedicated to Single Points of Contact (SPoC) at national level: authorities in charge of centralising and sending requests for data disclosure to OSPs, to share experiences, best practices and tips. Past operations show this structure greatly facilitates efficiency of communication, which is crucial in emergency cases.

SCOPE

The scope of this report is to present data in relation to the situation of the use of electronic evidence by EU law enforcement and judicial authorities in criminal cases in 2019. To that end, this document brings together different perspectives around the same topic and makes available exclusive data collected from competent authorities in all EU Member States and from many Online Service Providers. Furthermore, it also presents the evolution of the electronic

evidence situation by comparing data with the SIRIUS EU Digital Evidence Situation Report 2019[1].

Due to the wide use of electronic evidence in investigations in the EU, it is generally quite challenging to obtain comprehensive data for thorough analysis, including statistics of total volume, success rate and main issues, for example. Therefore, this report compiles pieces of information from different sources with the aim of capturing the status of access of EU authorities to electronic evidence as accurately as possible. Ultimately, it can contribute to the identification of core issues with a view to improve the effectiveness of criminal investigations and the prosecutions.

METHODOLOGY

This report has been developed with information collected from publicly available sources, as well as from exclusive interviews and surveys conducted with competent authorities and OSPs, as described below. Because this report presents data relating to 2019, the United Kingdom (UK) is included as an EU Member State in the statistics. Furthermore, law enforcement and judicial authorities' representatives from the UK were also invited to respond to surveys conducted for the purpose of this document.

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

The transparency reports analysed for the purpose of this report were: Airbnb, Apple, Automattic, Cloudflare, Dropbox, Facebook, Google, LinkedIn, Microsoft, Snap, TikTok, Twitter[2] and Verizon Media (formally known as Oath).

- **Online surveys with European Union law enforcement**

As for the previous SIRIUS EU Digital Evidence Situation Report 2019[3], Europol conducted a survey amongst European Union law enforcement agencies. 220 responses from representatives from all EU Member States and the UK, during April and May 2020, through password-protected online form. The responses were anonymous.

A second survey dedicated to the relevance of online gaming platforms in investigations was conducted among EU competent authorities on SIRIUS during July and August 2020, also through password-protected online form. A total of 71 responses were recorded, from representatives of 20 EU Member States and the UK both from law enforcement and, to a less extent, from judicial authorities.

- **Online surveys with European Union judicial authorities**

Similarly to the SIRIUS EU Digital Evidence Situation Report 2019[4], Eurojust conducted a survey among judicial authorities in the European Union which returned feedbacks from member of the judiciary community on SIRIUS as well as from European Judicial Cybercrime Network (EJCN) and European Judicial Network in criminal matters (EJN)

contact points. Between April and June 2020, a total of 34 in-depth responses were collected from 20 EU Member States[5] and the UK through password-protected online survey. The responses were anonymous.

- **Interviews with Online Service Providers**

Europol engaged with OSPs via phone or video interviews and/or e-mail exchange with representatives from Apple, Facebook, Google, Microsoft, Snap, Twitter and Verizon Media between May and July 2020 for the purpose of this report. The findings presented based on these interviews should not be taken as the official position of any of the aforementioned private entities.

The main topics discussed with these companies were:

- Main reasons for refusal or delay in processing of requests from EU authorities in criminal investigations;
- Challenges in the process of dealing with requests for disclosure of data in criminal investigations;
- The effectiveness of Single Points of Contact in EU law enforcement authorities.

- **Workshop with US and Irish authorities**

A workshop with representatives from the United States and Irish competent authorities was organised with the aim of gathering information, comments and inputs on the current situation in relation to cross-border requests and access to electronic data in criminal investigations as well as on the legal frameworks surrounding the field. The main points touched upon during the discussion contributed in substantiating the general overview on the working field in the context of both voluntary cooperation as well as judicial cooperation.

- **Fiches Belges on Electronic Evidence**

The EJN contributed with information coming from the newly-created Fiches Belges[6] which include data collected from 19 EU Member States[7] on topics ranging from the definition of electronic evidence at national level to the applicable legal procedures and which requirements are crucial to obtain necessary evidence. 11 key questions on the procedural rules regarding electronic evidence were asked, touching upon topics such as: legal international framework, possible measures for judicial cooperation available in the EU Member States, time limits for data retention and procedure for search, seizure, preservation and production.

CONTEXT

With the digitalization of everyday life and the accelerated multiplication of products and services offered online, a huge amount of data is collected, stored and processed by private entities. In specific circumstances, access to particular datasets of targeted individuals collected by such entities can be determinant to save lives in immediate danger or to investigate and prosecute crimes:

it could be a child abuse case, a specific terrorist threat or a kidnapping investigation. In nearly any type of crime today, electronic data can make a difference. For example, IP addresses may lead to suspects and fugitives, geolocation data may allow the location of missing persons and connection logs may be essential evidence in court.

As the importance of electronic evidence increases exponentially over time, policy-making is underway in the EU to provide clarity and legal certainty to users, OSPs and competent authorities, while putting in place strong safeguards in relation to personal data protection and fundamental rights. With the objective of improving cross-border access to electronic evidence, the EU is currently taking important steps for a more robust common legal framework, including harmonising EU-wide approach[8] and negotiating bilateral agreements with third-countries, as well as multilateral treaties[9]. The outcome of these processes, especially the adoption of the new EU instrument that follows a new approach adapted to digital specifics, could radically change the way data is requested in the context of criminal investigations in terms of speed and effectiveness, while preserving user privacy.

While policy-making and negotiations are still underway, EU authorities rely either on the existing legal framework to request data from foreign-based online service providers via judicial cooperation tools, or voluntary cooperation (when companies reply to requests directly issued from foreign authorities, process generally restricted to non-content data). The existing mechanisms are often considered not optimal[10]. First, judicial cooperation mechanisms are frequently appointed by authorities as cumbersome and the process for disclosure of data can take several months, or even years, depending on the countries involved and the circumstances of the request. Second, voluntary cooperation procedures are not standardized and they provide limited legal certainty to the involved parties.

PERSPECTIVE OF EU JUDICIAL AUTHORITIES

It is against this context that over the first months of the year Eurojust engaged with the EU-wide judiciary community and beyond, in order to gather insights and draw a panoramic on the 2019 situation on cross-border requests and access to electronic data in criminal investigations as well as on the legal frameworks surrounding the field.

A direct survey tailored for EU judicial authorities resulted in a total of 34 in-depth responses received from member of the judiciary community on SIRIUS as well as from EJCN and EJN contact points of 20 EU Member States[11] and the UK; these, complemented by additional streams of information obtained via the SIRIUS Platform and a workshop with United States and Irish competent authorities, formed the basis of what is now presented in this report. To complement the perspective of EU judicial authorities, this chapter also includes the information gathered in the EJN Fiches

Belges concerning the legislation and practice from the EU Member States.

A. Success cases

The prominence of electronic information and their relevance in the investigation and prosecution of crimes has become a concrete part of the daily job of EU authorities, even more so as evidence in electronic formats is, in several circumstances, the only resource available in a case. On the other hand, the fragmentation of legislation, at national and international level, and the possibility to resort to a wide arrange of channels and legal instruments, proves to be a challenging aspect where, like in a puzzle, needs and solutions might not be matching at first sight.

What emerges clearly, then, is how in this unprecedented development of the technological and legislative landscapes, the reliance on collaboration, support, direct cooperation and partnership is a key tool for success, both at domestic and international level. What follows is a selection of some first-hand experiences collected that point towards that[12]:

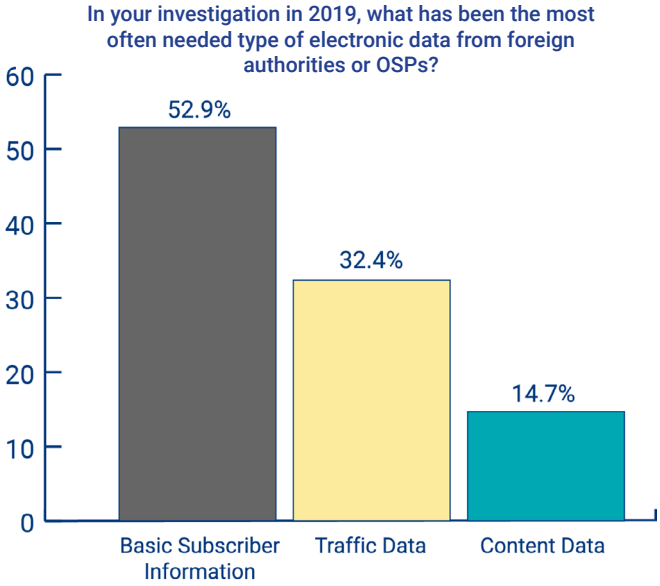
- *Our office contacted directly an OSP in the EU (which was risky because it could have led to the notification to its users about an ongoing investigation) and luckily managed to establish a very productive and trustworthy dialogue, based on domestic production orders. The OSP was dissatisfied with criminals using its infrastructure, and shared relevant subscriber and traffic data with the investigating authority;*
- *Excellent cooperation between [EU Member State] Public Prosecution (Central Department of Prosecution and Investigation) and the National Center for Missing and Exploited Children (USA) regarding the communications of child abuse or child pornography;*
- *Positive experience with cooperation with the U.S. Department of Justice, European Judicial Cybercrime Network as well as the SIRIUS Project;*
- *Positive experience with national Single Point of Contacts;*
- *Permanent direct contacts with the U.S. Central Authority facilitates cooperation as they can provide relevant advice concerning probable cause: a practical issue that requires some consultation from time to time. SIRIUS project provided very important inputs on major U.S. providers and it is very helpful to understand the possibilities for cooperation;*
- *The use of 24/7 network for retaining data is crucial[13], as well as the support offered by Eurojust on European Investigations Order (EIO) / Mutual Legal Assistance.*

B. Cross-border requests and data disclosure

Each investigation is unique, yet there are similarities that can be taken into consideration: one relates to the types of electronic data that were most often needed from foreign authorities or from OSPs during the investigations conducted in the EU in

2019.

Basic subscriber information – such as name, e-mail or phone number – emerged as the most sought after type of information in a percentage similar, and sensibly higher, to what presented in the SIRIUS EU Digital Evidence Situation Report 2019[14]: 52.9% compared to 41.7%.



The general classification and definitions of data categories as provided by the Budapest Convention on Cybercrime and its Explanatory Report, and used as a reference in the survey, constitute a useful and common starting point, nevertheless they are not a unique scale. As different ways of categorisation may be taken from other legal instruments, from national legislation[15] or even from the very way OSPs collect different data according to their types of services, EU judicial authorities provided a more detailed overview drawn from their personal experience in the field. Among those who selected basic subscriber information the following explanation were collated:

- *In practice, all three types of data are absolutely necessary in the frame of criminal investigation and in antiterrorism. US authorities, however, often request reference to the metadata before disclosing the content of communication or correspondence[16];*
- *90% of all the requests to OSPs refer to subscriber information and most of these requests are the first measure in an investigation;*
- *Basic subscriber information and traffic data are the most common electronic data required. There is, however, an increasing need to obtain localization data and IP traffic data;*
- *It is difficult to choose one category as judicial authorities usually make comprehensive requests that contain in most cases all three categories of data in one request. It also depends on the type of the provider and the type of the offence. Basic subscriber information and traffic data are equally represented in the requests needed from abroad;*
- *Actually, subscriber information and traffic data are most often needed and requested from foreign OSPs.*

Basic subscriber information is followed by the categories of traffic data – such as connection logs, number of messages – and content data that refers to the actual content of a communication – such as photos, e-mail/messages content, files. If the ranking is in line with what reported in relation to 2018

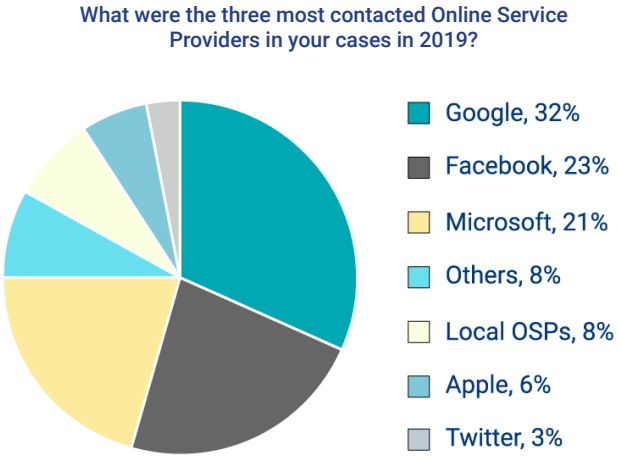
data, we notice a slight decrease in requests for both traffic data (32.4% from 40.3%) and content data (14.7% from 18.1%) at the advantage of basic subscriber information[17].

As explained below, the choice over which data category is the most requested during investigations, hence the most needed, is not an exclusive one and may vary on a case-by-case scenario:

- *It is difficult to make a choice, as authorities need all types of data, depending on the needs of the case;*
- *Content data is the most needed, but it is hardest to get. The result is that authorities mainly ask for the first two types of information [basic subscriber information, content data];*
- *Subscriber information can be useless as perpetrators use false identities. Connection logs are the most valuable, for example, to trace the real user of the domain, e-mail or social media account;*
- *Subscriber and traffic data are generally requested at the same time;*
- *Subscriber and traffic data is more likely to be obtained by police/law enforcement at earlier stage in enquiry and content data by prosecutor at later stage of investigation.*

These results are somewhat predictable, given the different levels of sensitivity and therefore protection of the different data categories.

At the receiving end of the requesting process, be it under voluntary cooperation or judicial assistance, ultimately, there are the OSPs. Whether based in the same jurisdiction of the requesting authority or with a worldwide presence, when asked to indicate the three most contacted companies in 2019, EU judicial authorities surveyed returned a quite clear overview that shows a significant predominance of three major U.S.-based tech companies: Google[18], Facebook and Microsoft.



Categorised as “Others”, and mentioned not more than once, are OSPs such as Amazon, PayPal, Viber, Whatsapp and Wix: all companies with a well-established market and geographical presence yet, in this overview, far from the relevance granted to the top ranking. Finally, among the “Local OSPs”, there are: allegro.pl and OLX.pl (two Polish marketplaces), OVH (a French cloud computing company), Worldstream (a hosting provider based in the Netherlands) and Seznam (a web portal and search engine in Czechia).

In the context of transnational criminal investigations, EU authorities can request and obtain disclosure of data held by foreign-based OSPs in multiple ways. One specific channel builds on the regime of voluntary

cooperation: by addressing directly OSPs established outside their own jurisdictions, EU law enforcement and judicial authorities can lawfully and quickly obtain non-content data (basic subscriber information and, in a minority of cases, traffic data) by a foreign-based private entity in possession or control of the data. Despite being efficient and reliable instruments, direct requests under voluntary cooperation are entirely dependent on the willingness of the OSPs to cooperate with the competent authorities and lack, therefore, an objective element of enforceability.

A more flexible way to request disclosure of basic subscriber information that considers the global reach of services offered by OSPs, regardless of their location, is included in the Budapest Convention on Cybercrime under Article 18[19], according to which "*(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: (b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control*".

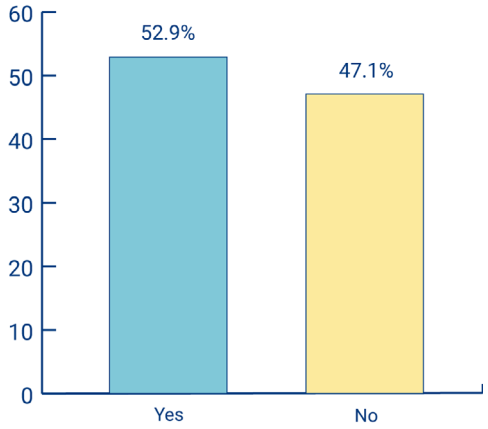
Under Article 18, competent authorities can request basic subscriber information from those OSPs that are established outside the domestic jurisdiction but that, at the same time:

- **are in possession or control over that data:** evidence does not need to be physically in possession of the OSP and can therefore be stored elsewhere as long as remotely accessible (e.g. in the cloud); and
- **offer their services in the territory:** even without a physical of legal presence a company can have a real and substantial connection with the users by means of the services provided.

Even if a production order under Article 18 has extra-territorial effects, it remains a domestic request with no enforcement mechanism in the receiving State, and, as such, needs to respect the domestic legislation of the issuing and receiving State as well as being subject to legal safeguards (e.g. in relation to data protection, human rights and liberties).

Among the judicial representatives surveyed, a slight majority of the respondents (52.9%) identified provision included under Article 18 of the Budapest Convention on Cybercrime as being part of their national legal frameworks.

Does your national legal framework (Art. 18 (1)(b), Budapest Convention) foresee issuance of domestic production orders towards OSPs abroad, but offering services in your country and being in possession or control or such information?



Further insights come from the explanations and direct reference to national legislation given for those who indicated possible to issue domestic production orders addressed to foreign-based OSPs yet offering its services within the territory, as presented in Table 1.

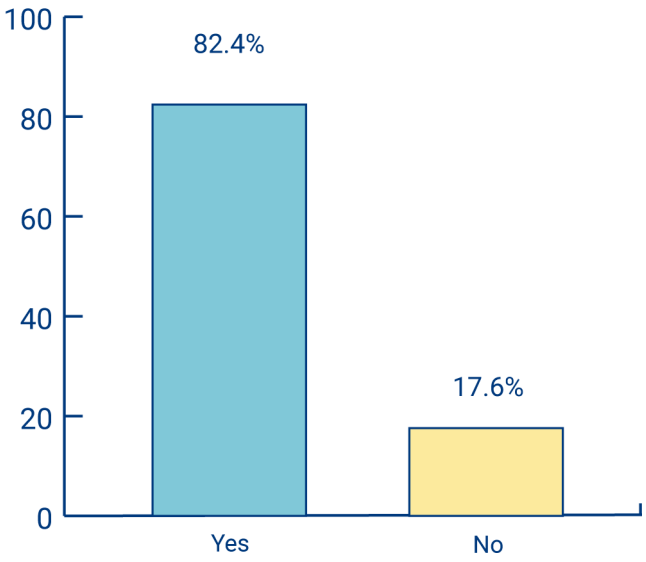
Table 1: Reference to national legislation on domestic production orders addressed to foreign-based OSPs

Belgium	The debate and legal discussions have been settled by two landmark decisions of the Belgian Supreme Court for subscriber data (Yahoo! case; decision of December 1st, 2015[20]) and content data (Skype case; decision of February 19th, 2019[21]). The Supreme Court decisions have been integrated afterwards in explicit terms in the Belgian Code of Criminal Procedures, by redefining the OSPs that have to answer to a legal domestic production order, as: «the operator of an electronic communications network; and - everyone who, within Belgian territory, make a service available or offers a service which consists in the transmission of signals of electronic communications via electronic communications networks, or which consists in allowing users to obtain, receive or circulate information via an electronic communications network. The concept also includes the provider of an electronic communication service».
Czechia	This kind of cooperation is not based on Article 18 of the Budapest Convention on Cybercrime but on general provisions of the Code of Criminal Procedure (CPC). The practice differs in relation to various providers.
France	It is possible to submit requests to foreign companies but the jurisprudence of France's highest court, the Court of Cassation, does not recognise these requests as compulsory. OSPs therefore cannot be sanctioned if they do not respond to these requests.
Netherlands	Because of many reseller-constructions a service provider established in the Netherlands often does not have access to the subscriber data or content (stored on the resold server). Experience has shown that, when sending a preservation order to the Dutch OSPs, the parties indicate that they are unable to comply because they do not have access to the information requested. In most cases, Dutch authorities actually do not preserve the data anymore, but order/demand the requested data, by sending a domestic order to the Dutch service provider. If the Dutch OSP does not wish to (voluntarily) forward the order to the reseller, the Dutch authorities will send the order directly to the foreign reseller (only after explicit permission of the issuing state because of potential risk of damage to the investigation). However, the authorities in the Netherlands cannot compel the OSP or reseller to forward the order and legally enforce such a request. If the reseller abroad is non-cooperative in providing (a) the subscriber data, (b) info about the physical location of the server or (c) a download link (snapshot), the (L)IRC[22] will advise the issuing state to send a(n) EIO/MLAT to the country where the reseller is located/incorporated.
Poland	Legal framework allows to issue a warrant for obtaining data from OSPs but they usually refuse to give an information because of lack of jurisdiction and demand to send a rogatory letter to the US or Ireland (Twitter, Facebook) or issue EIO.
Portugal	"Law no. 109/2009 (15 September) Cybercrime Law - Article 14 (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 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"[23]
Spain	Possible pursuant to Art. 588 ter j) of the Procedural Criminal Code related to access to data held in service provider´s computerised files. The precept does not limit its application to natural or legal persons having their address or registered office in Spain, therefore in can be understood that this order can refer to service providers settled in other States, in the terms and with the sense of Article 18 1 b) of the Budapest Convention.
United Kingdom	Used occasionally when OSP indicates it will produce evidence pending a domestic production order.

The focus on the general respect of legislation – be it at domestic level in the country where the requesting authority is based as well as the one where the receiving OSP is established – and the specific requirements or processes for data disclosure put in place by the private entities themselves, are not only limited to the actual disclosure of the information. They acquire a fundamental importance especially when the data and electronic information gathered will have to be presented, and admitted, as evidence in a court.

Keeping the attention on cross-border voluntary cooperation, the channel of directly addressing a foreign-based private entity to seek disclosure of information produces, in the vast majority of the cases among the surveyed (82.4%), evidence considered as admissible in court. Percentages are almost identical to what included in last year's overview[24].

Does your national legal framework allow electronic data to be gathered via cross-border voluntary cooperation by directly addressing a private entity and can the data gathered in this way be admitted as evidence?

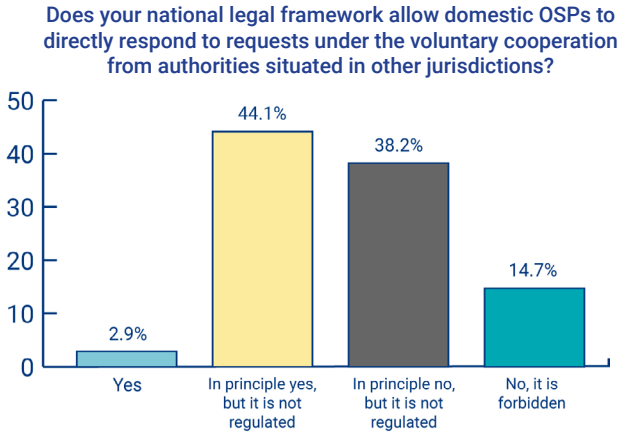


Asked to substantiate their choice with reference to national legislation, those among the 82.4% provided the responses presented in Table 2, which complement the inputs received from the Fiches Belges and reported in Table 9.

Table 2: Admission as evidence of data gathered via direct requests to foreign-based OSPs

Germany	There is no special legal framework required under German law. If the data is provided voluntarily and the request to provide it was within German law, it can be used as evidence in court.
Hungary	National legal framework does not specifically allow or specifically forbid to directly request data from someone abroad. However, if it still happens(for example, because the police uses the legal framework laid out in the criminal proceedings law used for obtaining information domestically) and the data is being sent, it is not considered as data acquired with breaching the law or harming the position of participants in the procedure, therefore it can be used as evidence.
Ireland	National legislation neither allows or prohibits it. It is a matter for the court on whether it will be admitted or not.
Latvia, Lithuania, Poland	It is generally not regulated nor specified in the law. There is not a formal ban of collecting evidence in such manner.
Portugal[25]	There is not a specific legal provision, but the principle is inscribed in the article 14 of the Cybercrime Law[26] in which the provisions regarding the preservation order do not prohibit the voluntary cooperation. This is not a consolidated interpretation due to the fact there are different interpretations and court opinions and the need for a specific legal provision is prominent.
Spain	Voluntary disclosure of electronic evidence by the online service provider is only admissible when it is related to subscriber data, where no judicial authorization is needed according to the Spanish legislation. For this reason, its admissibility is limited to that kind of data alone, not to traffic data or content data.
United Kingdom	Yes, general rules of evidence would apply. In practice it is dependant on the co-operation of the OSP.

The two-way process of voluntary cooperation entails that for every data disclosure request directly submitted to a foreign-based company, a response could involve production and handing over of information. Reversing the situation and looking at it from the perspective of the addressees: are OSPs – assuming it is part of their internal policies – allowed by their national legal frameworks to comply with direct requests coming from foreign-based authorities? Even before reporting whether they are allowed or not, it is interesting to notice how a vast majority of the respondents (82.3%) stated how this matter lacks regulation in their respective national legal frameworks, as opposed to the 17.6% of the cases where legislation is in place.



Shifting the focus on the core of the question the majority of respondents (52.9%) reported OSPs are generally not allowed to respond when they receive requests directly from foreign authorities; on the other hand, 47% state the opposite.

Building on this, and regardless as to whether domestic legislations allow it or not, it is again interesting to pay attention to how a "general principle" based on practice prevails on the legal prescriptions:

1. Within the 52.9% of the cases where OPSs are generally not allowed to respond to direct requests submitted by foreign authorities, 38.2% of the respondents reports it as based on a general practice while declaring no regulation is in place as opposed to 14.7% of the cases where that practice is the direct result of a legal provision.

   Some respondents provided additional explanation as reported in Table 3, to be read in additional to what presented in Table 10 as well:

Table 3: Countries that generally do not allow domestic OSPs to respond to direct requests from foreign authorities

Hungary	OPSs are monitored by the National Security Service for preventing any illegal access to our communication infrastructure from abroad or from anyone with malicious intent. For this reason, it is unlikely that OSPs would execute such an order, even when it is not regulated and forbidden expressis verbis.
Netherlands	Involvement of national public authority/point of entry is needed. In the case of direct answer to production orders, the GPDR applies to OSPs (within Europe). The Netherlands does not have a specific criminal procedure/ national framework for this. The Netherlands endorses the interpretation that article 18.1.b[27] of the Budapest Convention on Cybercrime offers, giving the possibility of direct access to an OSP established in a party to the convention (for example: the Netherlands), on the basis of an order or authorisation of a judicial authority of the requesting party, where it concerns subscriber information and in so far as this OSP is also active/offering his services (and has access to this data), without infringing on the sovereignty of the requested party.
Slovakia	The legislation indirectly excludes the possibility of providing evidence by means of voluntary cooperation.
Slovenia	National OSPs are bound by Slovenian legislation and they will give data for which the court order is needed, only on a basis of domestic court order.

2. Within the 47% of the cases where OPSs are generally allowed to respond to direct requests submitted by foreign authorities, 44.1% of the respondents reports it as based on a general practice while declaring no regulation is in place as opposed to 2.9% of the cases where that practice is the direct result of a legal provision.

   Some respondents provided additional explanation as reported in Table 3.1:

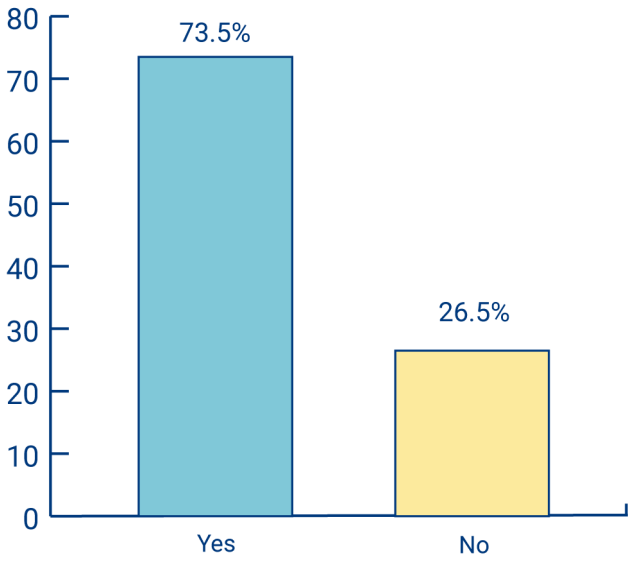
Table 3.1: Countries that generally allow domestic OSPs to respond to direct requests from foreign authorities

Portugal	There is no specific provision in the national Cybercrime legislation.
Sweden[28]	Depends on the type of information and what type of service provider. Regarding some companies (mainly carriers), it is forbidden for them to reveal information.
United Kingdom	No prohibition on OSPs doing so, yet it is no something our office would be aware of happening.

Depending on the circumstances, even when investigations have a transnational dimension and cross-border exchange of electronic information is envisaged, it might not be necessary for EU authorities to engage in any way with OSPs. This happens when, for example, parties involved in a case (such as the holder of a targeted account, a suspect or even a witness) are willing to provide access to electronic information voluntarily or on the basis of the authorisation of the competent legal authority. An additional alternative form of this direct access to electronic information is also contained in Article 32 of the Budapest Convention on Cybercrime[29], according to which: "(*1) A Party may, without the authorisation of another Party: (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system*".

The two key aspects of what Article 32 establishes are its cross-border aspect, whereby investigative authorities can obtain information stored in a different jurisdiction, and the automatic recognition of information gather on this basis as evidence in court, without the need to issue a process under judicial assistance (EIO / MLA). On this, a clear majority of respondents (73.5%) reported it as being incorporated in their national legislation.

Does your national legal framework allow cross-border direct access to electronic information (e.g. with consent of data subject, with authorisation of the competent legal authority, or according to Art. 32 (b) Budapest Convention)?



Some respondents added ulterior information in relation to their national legal frameworks, shown in Table 4.

Table 4: Cross-border direct requests for data disclosure with consent of the data subject

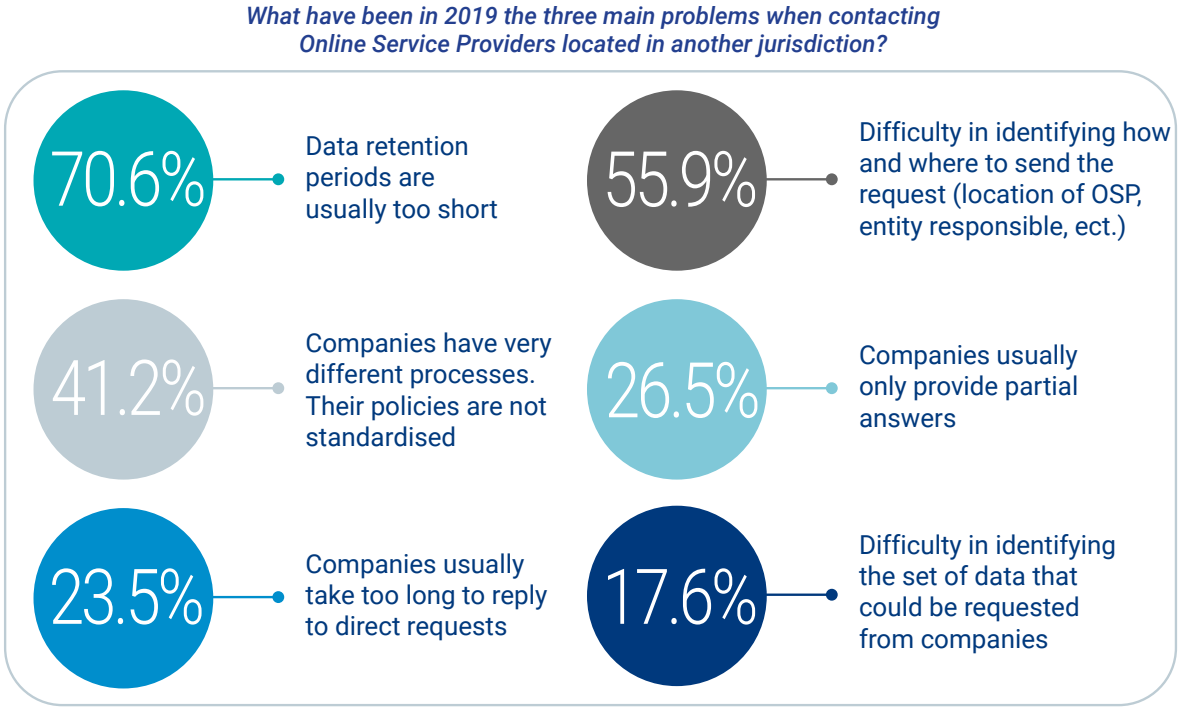
Austria	With the consent of the data subject or with the use of the legally seized electronic device of the suspect.
Belgium	"Art. 88ter Belgian Code of Criminal Procedure: The investigating judge may extend the search in a computer system or part thereof, begun pursuant to Article 39a, to a computer system or part thereof located in a place other than that in which the search takes place: – if this extension is necessary to reveal the truth about the crime that is the subject of the search; and – if other measures would be disproportionate, or if there is a risk that evidence would be lost without this extension. The extension of the search in a computer system may not extend beyond the computer systems or parts thereof to which the persons entitled to use the computer system under investigation, in particular, have access. (…) If it emerges that these data ARE NOT ON THE TERRITORY OF THE STATE, they will only be copied. In that case, the examining magistrate will immediately inform the Federal Public Service Justice, which will inform the competent authority of the State concerned, if this can reasonably be determined. In the event of extreme urgency, the examining magistrate can order the extension of the search referred to in the first paragraph orally. This order shall be confirmed in writing as soon as possible, stating the reasons of extreme urgency."
Czechia	In many cases, this practice is not considered to be a "cross-border" access and does not refer to the Art. 32 of the Budapest Convention on Cybercrime.
France	Art 51-1 (3) of the Penal Procedure Code: "Where it is known in advance that data which is accessible from the initial system or available for the initial system is stored in another computer system situated outside the territory of the French Republic, it is collected by a judicial police officer, pursuant to the conditions of access provided by any international agreements currently in force."
Germany	This is possible with the consent of the data subject and solely based on Article 32 of the Budapest Convention on Cybercrime. No specific German legislation exists.
Hungary	This is possible and working, and implemented by police. The Budapest Convention on Cybercrime was incorporated into the criminal proceedings law with a separate act with the textual content of the Convention.
Ireland	Access to account information is only allowed where the subject permits or consents to the access. Access may be granted by a judicial authority on foot of an interception order allowed in law.
Portugal	"Law no. 109/2009 (15 September) Cybercrime Law - Article 15 (Search of computer data): 1. When, 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 authorizes by order, or orders, a search in that computer system, and, where possible, leads the event. 2. The order of the preceding paragraph has a maximum validity of 30 days, under penalty of nullity. 3. (…) 4. (…) 5. When, during a of search, there are reasons to believe that the information sought is stored in another computer system or in a different part of the previous system, but these data are legally accessible from the initial system, the search can be extended by authorization of the competent authority in accordance with paragraphs 1 and 2."
Slovakia	No specific procedure is regulated in the national law, but in principle the Act 351/2011 Coll. on electronic communications as amended, GDPR and the Act on Data Protection would need to be considered by providers and/or by other entities or natural persons, where applicable.
Slovenia	When a court order for a search of electronic device is issued, the investigators can access electronic evidence, if that is possible by using the searched device (with username and password), no matter where data are stored.
Spain	There is not a special legal provision in the Spanish Criminal Procedural Law about extended search in cross-border cases. In such cases, Article 32 of Budapest Convention on Cybercrime remains applicable. Nevertheless, the Prosecution Service in its Guidelines nº 5/2019 about searches of electronic devises and computer equipment's, concludes as follows: "The jurisdiction of the Spanish Courts shall extend to the search of any computer system located in Spain, regardless of whether the data is stored on servers located outside the national territory, provided that they are lawfully accessible from the searched system." So far, there is no case law from the Supreme Court or the Constitutional Court dealing with this question or backing up that conclusion.
United Kingdom	In Scotland there is no prohibition on doing so in the domestic laws of evidence, and to the best of knowledge has not been challenged when it has happened.

From a broader perspective, Article 32 of the Budapest Convention on Cybercrime is encapsulated in a longer list of investigative measures available in the EU drawn from the same legislative source; on this Table 11 offers a wider point of view.

C. Challenges

The possibility to directly engage with OSPs based in foreign jurisdiction is with no doubt a powerful tool that allows disclosure and transmission of relevant electronic data to be used as evidence for investigation and prosecution of crime; it does not come without some specific challenges though. Here the correct way to interpret the feedback received is within the context of an ongoing investigation where the element of time is crucial and any deviation, obstacle or criticality encountered can have a very significant impact on the final outcome of a case.

EU judicial representatives were requested to identify the three most challenging aspects faced while contacting foreign OSPs in the context of requests for electronic evidence under voluntary cooperation. As per the result presented in last year's overview[30], the predominant issue, pinpointed by the 70.6% of respondents, lamented the short data retention periods of the information collected after a preservation request / order is submitted to the companies by EU competent authorities.



The 55.9% of surveyed expressed their difficulty in identifying how and where to send requests to companies (for example, establishing the correct entity responsible for cooperating voluntary with public authorities) whereas the 41.2% recognised as an issue the lack of standardisation of OSPs' policies when dealing with incoming requests for data disclosure.

The combination of receiving only partial answers to production orders coupled with the perceived slowness of OSPs in replying to direct requests were chosen respectively by 26.5% and 23.5% of respondents. Finally, additional problems reported with a lower prevalence were:

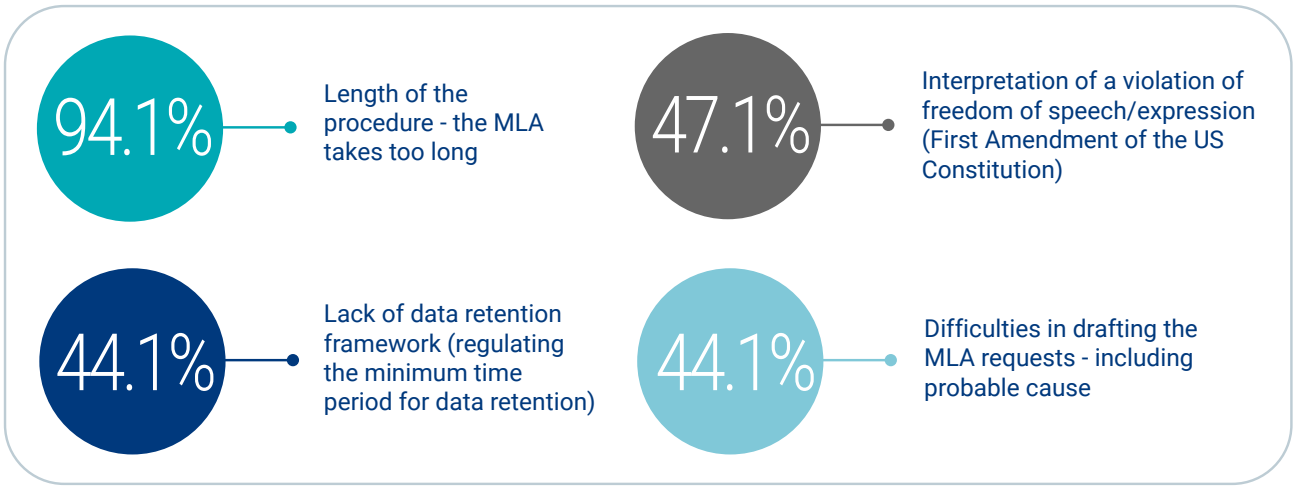
- Difficulty in identifying the data that could be requested from companies: 17.6%
- Lack of timely response in emergency cases: 11.8%
- Difficulty to understand or find clear and objective guidelines provided by the company: 8.8%
- Companies change processes and response formats too often: 8.8%
- Other: 5.9% - some complementary explanations point to the fact that OSPs usually require MLA procedures to handle data disclosure requests or national legal frameworks do not allow gathering of electronic data via direct cross-border voluntary cooperation;
- Difficulties arising from the different terminology used by the different service providers and the law enforcement authorities defining the data types: 2.9%
- Format of the response is not easily usable for analysis (for example, non-editable PDF form): 2.9%

The comparison with information featuring in the SIRIUS EU Digital Evidence Situation Report 2019[31] shows how, even though with different weights, the recurring issues polling higher refer all to: the perceived lack of timely responses from OSPs, the very diversified policies in place among companies and the difficulty in identifying correct methods and channels for the submission of requests.

An insightful perspective to substantiate the overview on the main challenges EU practitioners face in relation to OSPs comes, once again, from the workshop with United States and Irish competent authorities. Even if from a slightly different standpoint[32], the issues identified as the most relevant generally match the panoramic presented above in relation to data retention periods as well as to technical and procedural difficulties. Clear mention was made towards issues such as: recognising the correct private entity responsible for handling data disclosure requests, the lack of standardisation of processes and their rapid change and, not at last, the very diverse format of the responses obtained by OSPs. Due consideration was also given to those instances where the communication between authorities and OSPs is not smooth enough, therefore causing potential delays along the process of request and disclosure of data at the detriment of rapid and time-bounded investigations.

Voluntary cooperation between OSPs and EU competent authorities is only one of the available instruments and, in different cases, law enforcement and judicial authorities in the EU need to resort to the channels offered by judicial cooperation to seek disclosure of data under mandatory cooperation. This can happen in case specific dataset are necessary for investigations – mainly Content Data –, if domestic legislations require it for the admissibility of evidence in court or ultimately if the process of voluntary cooperation is not pursuable.

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



When asked to identify the main problems encountered with Mutual Legal Assistance processes towards competent authorities in the United States, EU judicial authorities surveyed reported almost unanimously (94.1%) the long time needed for MLA procedures as the most challenging issue encountered in 2019. This, despite being a recurring and long-standing challenge, seems in some instances offset by the good degree of cooperation established between EU and US authorities in the field, as testified by a responded who noted how *"the length of procedure is an issue. Nevertheless, U.S. authorities are very helpful and in urgent cases they are able to provide evidence in a short period of time. Permanent direct contacts with the U.S. Central Authority facilitate cooperation. A sufficient advice was provided concerning probable cause. It is a practical issue that requires some consultation from time to time. SIRIUS project provided very important inputs on major U.S. providers and it is very helpful to understand the possibilities of cooperation".*

Following this main procedural issue, 47.1% and 44.1% of respondents identified respectively the 'Interpretation of a violation of Freedom of speech/expression (First Amendment of the Constitution of the US)' and the 'Difficulties in drafting the MLA requests including probable cause' as problematic when addressing legal processes to authorities based in the U.S. An equally relevant problem, identified by the 44.1% of respondents, is the 'Lack of data retention framework regulating the minimum time period the OSP has to keep the data of their users'.

Taken all together, and looking back at what reported in the SIRIUS EU Digital Evidence Situation Report 2019[33], the main challenges highlighted appear to be the same both in terms of content and actual impact on daily activities of EU authorities.

Lastly, additional problems reported yet with a lower prevalence among the surveyed are:

- Replies are often partial: 23.5%
- Difficulty in identifying set of data that could be requested: 8.8%
- Difficulties arisen from the different terminology used by the different service providers and the law enforcement authorities defining the data types: 5.9%
- Other: 5.9% – some complementary explanations read as: *"The main issue is the need of unified identifier to obtain the evidence. However, in many cases only the nickname is available. In such cases the U.S. authorities cannot provide the evidence, since the provider is unable to identify an account" and the "requirements to provide various evidence grounding the MLA requests".*

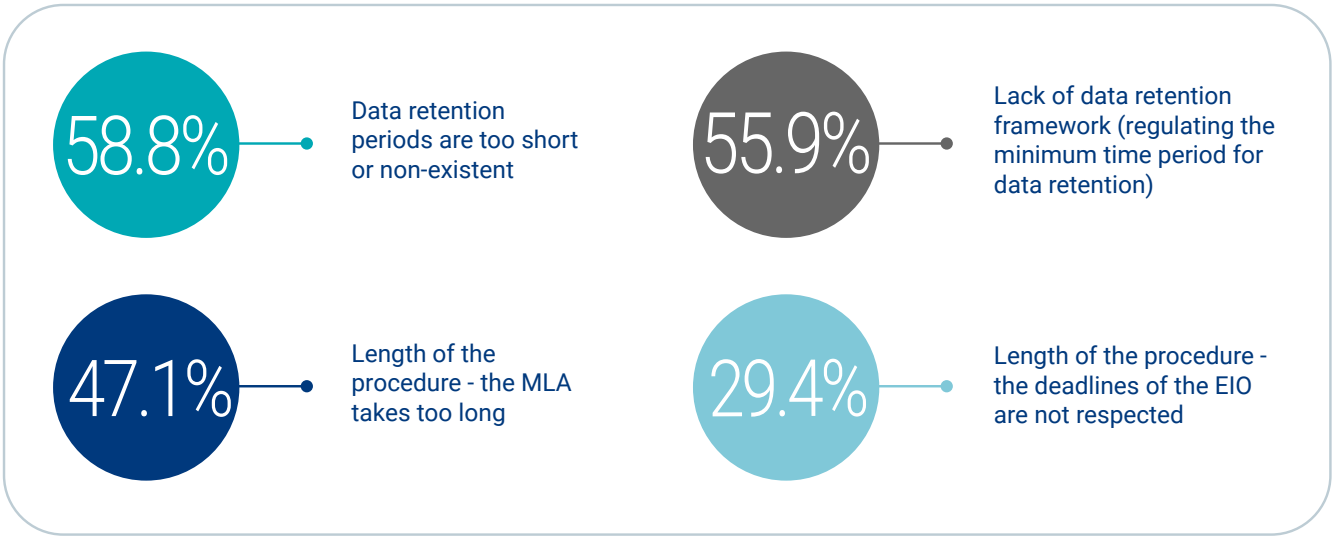
Looking at this very same topic of discussion, two specific challenges here presented emerged also from the direct engagement with those institutions located at the receiving end of the MLA processes initiated by EU counterparts. Regarded from their perspective, US authorities referred to the meeting of legal standard of probable cause as a constant issue, which, due to its specificity to the U.S. legal framework, is part of training activities provided to EU colleagues.

The second challenge mentioned referred tangentially to the issue identified with the lack of data retention framework for OSPs to store user data; on this, US authorities stressed the importance of receiving MLA process complete of indication to a Preservation Request (PR) previously submitted to the targeted OSP: essential for serving a legal process with the certainty of finding the data sought.

As not all the OSPs are U.S.-based and several have legal entities established in the EU territory that can be addressed via judicial cooperation channels, a question mirroring the one just presented was also asked.

Regarding the use of the EIO or MLA with other EU Member States, 58.8% of respondents identified the short data retention periods or their absence as the main problem, followed closely by the 55.9% who stated there is a 'lack of data retention framework regulating the minimum time period the OSP has to keep the data of their users'.

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



The general 'length of the procedures' initiated with another EU MS was indicated as a relevant challenge by the 47.1% of surveyed, whereas other time-related issues referring to the 'length of EIO procedure', lack of respect of deadlines for recognising and executing EIO or the 'lack of timely response for urgent cases (such as destruction of evidence, detention of a suspect)' were identified as the main issues respectively by the 29.4% and 17.6% of respondents.

Lastly, additional problems reported yet with a lower prevalence are:

- Replies are often partial: 26.5%
- Difficulty in identifying set of data that could be requested: 14.7%
- Difficulties arisen from the different terminology used by the different service providers and the law enforcement authorities defining the data types: 14.7%
- Other: 5.9% – some complementary explanations read as: "*The follow up of a 24/7-request (by EIO/MLA) takes too long. The term of 60 days is not always respected*" and "*It is difficult to identify some European providers. In a particular case, 3-4 States were in question as potential addressees of an EIO. The scope of data to be available was unclear and issues are also often related to hosting providers*".

A quick comparison to the SIRIUS EU Digital Evidence Situation Report 2019[34], shows how, over time, the general reference to data retention periods and lack of related frameworks as well as length of procedures keep emerging as the most prominent ones among EU authorities.

During the direct engagement with Irish competent authorities on the challenges faced when receiving legal processes addressed to OSPs established in the Republic of Ireland, the reference to the preservation of data against the minimum data retention periods was particularly stressed. In such a context Preservation

Requests are essential, primarily to ensure the presence of the data sought by the requesting authority but, even more so, as according to Irish domestic legislation, expressed reference to the unique identifier contained in a PR is necessary to formally engage with OSPs based in Ireland.

It goes without saying that request and disclosure of data for investigation and prosecution of crimes are only possible when the actual information are stored, retained and potentially accessible from OSPs. At European level the current absence of a unified data retention regime of electronic communication data, poses concrete challenges to cross-border investigations involving electronic evidence[35]. More specifically, rules have been subject of disputes regarding mainly the balance between obligation for OSPs to retain data and intervention on the sphere of privacy. This, undoubtedly, has affected the data retention regulation in different Member States, resulting in a landscape that is far from being homogenous across the EU.

Widening the horizon of the discussion and building on this recurrent element identified as a crucial issue, the EU judicial community was therefore asked whether at nation level a regime regulating retention of data is in place.

With this in mind, the gap between those who reported having a data retention regime in place domestically (70.6% of respondents) and those who do not have it (29.4%) need to be further corroborated reporting the explanations given.

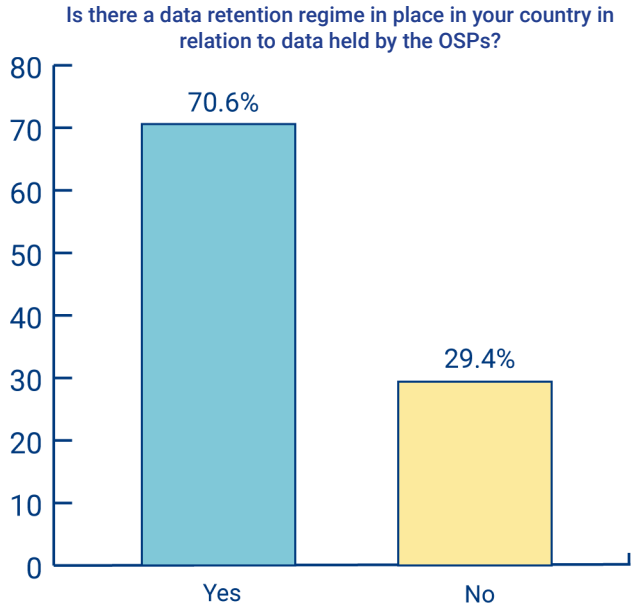


Table 5: Countries where data retention regimes are domestically in place

France	The legal system of data retention has been the object of an appeal before the European Court of Justice.
Hungary	The Hungarian data retention regulation did not change despite to the Tele2 Sverige case[36]. Otherwise, data retention is 1 year for successful communication and 6 months for failed answers (like not answered calls).
Ireland	Yes, covered by Section 6 of the Communication (Retention of Data Act) 2011.
Italy[37]	1 year for traffic data.
Luxembourg	6 months.
Poland	12 months (logs).
Portugal	The data retention regime in place is complex and fragmented in several legal instruments yet the specific types of data regard essentially communication data (basic subscriber information, traffic data and information on location). The legal regime consists of the conjugation of articles 187º and 189º of the criminal procedural code, article 14º of the Cybercrime Law and Law 32/2008, 17/07 (which transposed Directive 2006/24/CE). Essentially, basic subscriber information is retained up until the end of the commercial relationship and for 1 year after its termination. TD and information on location is retained for 6 months. Between 6 months and one year, traffic data and information on location is retained and can be obtained by order of the examining judge in investigations that comprehend serious crime (terrorism, violent and highly organized criminality).
Spain[38]	Law 25/2007, of 18 October, on the retention of electronic communications and public communication networks data (the Data Retention Law), still in force, which implemented Directive 2006/24, and also Article 588 ter j of the Criminal Code on Data held in service provider´s computerised files states.
United Kingdom	Generally covered by Part 4 of the Investigatory Powers Act 2016.

It appears clear that retention periods are different depending on the country; in addition to what is included in Table 5, the Fiches Belges add:

Table 5.1: Countries where data retention regulations are in force.

Belgium	12 months.
Bulgaria	3 months, with the possibility for extension up to 6 months in total.
Czechia	6 months.
Denmark	12 months.
Estonia	12 months.
Finland	3 months.
Latvia	18 months.
Lithuania	6 months, with the possibility for extension for 6 months.

On the other side of the spectrum, those who reported not having a data retention regime in place in their Member States, further explained in Table 6.

Table 6: Countries where data retention regimes are not domestically in place

Austria[39]	Following the decision of the ECJ in Digital Rights Ireland, the Austrian regime was repealed by the Austrian Constitutional Court in its decision from 27 of June 2014. Since then there is no data retention regime in force in Austria. However, law enforcement authorities can access data that has been stored by the providers for billing purpose.
Netherlands	No mandatory retention system. OSPs differ in their business processes when it comes to (the term of) keeping records for their administrative and, or, billing purposes. If traffic data is available (often not), it varies how long the data is kept by the OSP. The time the data is available by the OSP varies between 30 and 90 days (and what is kept depends of the settings).
Slovakia	Providers retain data for the period necessary for their business purposes. Periods / deadlines are not regulated by law. The period is defined by internal policies of providers (some data is retained only for hours, days, others for weeks, depending on a provider).
Slovenia	Although, since July 2014 there is no data retention regime in Slovenia following a constitutionality judgement of the Slovenian Constitutional Court, with an amendment of Criminal Procedure Act (ZKP-N) obtaining data in electronic communication network has been updated. The amended provisions do not constitute a general obligation for operators, ISPs and information society service providers to store data for purposes of possible criminal investigation, but rather a legal basis for disclosure of data they store for other (billing, commercial) purposes. So-called "precautionary retention" of traffic and location data of all users for possible future criminal investigation interfered heavily with the constitutional rights regarding the protection of personal data and communication privacy. However, that does not mean that retention of data is always unconstitutional measure, but they must be proportioned – necessary, adequate and effective in reaching desired and justified goal.
Sweden[40]	Data retention only required of carriers.

Further examples depicting the concreteness of the fragmentation of the EU landscape are included in the Fiches Belges and reported below, in Table 6.1:

Table 6.1: Countries that generally allow domestic OSPs to respond to direct requests from foreign authorities

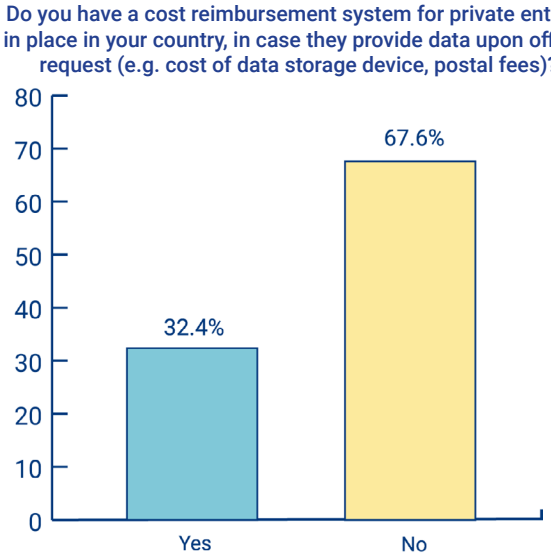
Romania	There is no legal obligation to retain data.
Germany	The application of the data retention provisions is currently suspended as the German Federal Administrative Court (Bundesverwaltungsgericht) has decided to transfer the final interpretation of the data protection guideline for electronic communication[41] to the Court of Justice of the European Union[42].

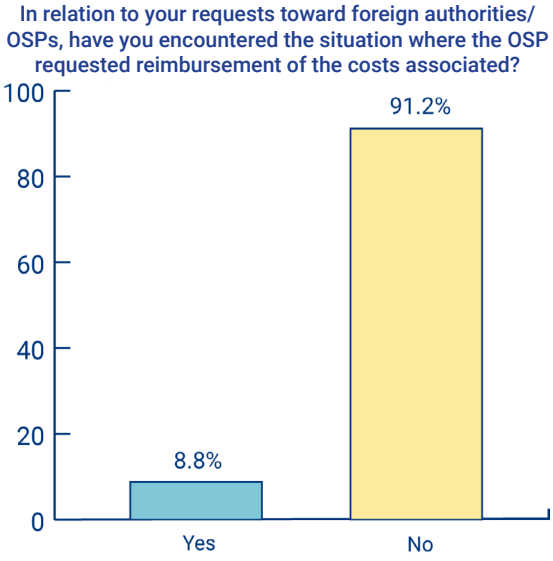
Looking ahead at possible future challenges that could have a role in the process of request and disclosure of electronic information, two dedicated questions focused on the so-called cost-reimbursement system which entails that OSPs may seek reimbursement for costs in responding to authorities requests for information as provided by law or domestic legislations. U.S. federal law allows charging governmental authorities in exchange of their cooperation[43] and some EU Member States (e.g. Austria and Belgium) have similar provisions in place too[44].

This mechanism, intended to offset the expenses occurred in replying to authorities requiring access to data, features as a standard part of some OSPs policies, nevertheless, it seems somewhat limited and not widely applicable to EU-based direct requests for data.

The comparative analysis of the feedback received on the matter shows that the majority of respondents does not have a cost reimbursement system in place (67.7%) and

never received a demand for compensation of the costs associated to reply to a production order (91.2%). Opposite answers to both questions, despite being a minority, demonstrate, on the other hand, that such a mechanism does exist yet its application is quite sporadic.





Among the 32.4% of respondents who reported having a cost reimbursement system in place domestically, as listed in Table 7, there are:

Table 7: Cost-reimbursement system in the EU

Austria[45]	In Austria the law (§ 111 StPO - criminal process law code) states, that everyone is obliged to give (a copy of) their data (on a hard drive) to the police if asked. In return, everybody (except the accused person) has the right to request an appropriate and customary or collectively agreed compensation for their costs for their service. These costs can be applied after they have cooperated with the police.
Germany	This will in most cases be based on Art. 23 of the 'Judicial Remuneration and Compensation Act' (JVEG) on 'Third party compensation'.
Netherlands	If operational costs are encountered in the execution of a claim, they are eligible for reimbursement according to invoicing guidelines, insofar as the claimed costs are reasonable. In order to assess what is reasonable, one of the factors taken into account is what comparable parties charge.
Poland	Storage costs charge the provider.
Sweden	For carriers regarding specific type of data.

In parallel, out of the 8.8% of respondents who reported having experienced receiving a bill for the handing over of the data, further explanation was provided in one instance:

- Slovakia: *Yes, we encountered such problem with a European country. In a child pornography case subscriber and traffic data related to numerous IP addresses were requested. The authorities of the country in question requested to pay a sum of money per IP address. Consultation did not lead to a solution and finally the data retention period expired. As a consequence, evidence was not provided.*

The discussion revolving around such a topic and its potential transformation into a future growing trend impacting more and more the EU as well, is also fed by recent concrete changes in some of the OSPs' policies and the emphasis attributed by some news reports[46]. The exchange with the US authorities proved to be, as previously, useful to substantiate the expertise on cost reimbursement systems in place; even though it has not yet appeared significantly in relation to MLA processes, competent authorities in the United States do receive invoices when, in the context of domestic procedures, they request OSPs to produce data for ongoing investigations. The practice, which appears limited without interesting the majority of OSPs, leaves governmental agencies the possibility to challenge the requests for OSPs to be reimbursed, for example on the basis of proportionality of compensation requested. Belonging to the majority of those EU Member States that do not have a cost reimbursement system in place and never received a demand for compensation by OSPs in 2019, there is Ireland: the competent authorities approached during the workshop were not aware of this practice happening with MLA processes.

In the survey submitted to the EU judiciary community this year, no specific question addressed openly the topic of encryption, yet, seen from other angles, it represents a topic that poses concrete and significant challenges in the field of electronic evidence. As several sources pointed out already[47], strong encryption is a cornerstone of the contemporary digitalised democracies as it protects privacy and the most fundamental human rights while fostering development of digital economies. Encryption as a basic service's feature of numerous OSPs therefore does not come as a surprise nor does the trend observed among some of extending cryptography by default to as many services as possible[48]. The implications of such a widespread use of encryption, pointing towards a potential interference with the ability of law enforcement and judicial authorities to obtain the information needed as evidence for investigations, are not kept unvoiced in their call for specific provisions to be introduced[49]. At present time, what remains a certainty thought, is that the most pressing challenges related to the technological developments and legal landscape surrounding the field remain matter for research and discussion in search for a response.

D. Fiches Belges on electronic evidence: legislation and procedures in the EU Member States

Despite being a topic in constant evolution and with a multitude of nuances, there is a common understanding among the EU Member States interviewed that electronic evidence is information/data of evidentiary value that is kept/stored in digital format. However, the vast majority of Member States (apart from Germany, Hungary, Latvia, Netherlands and Spain) do not have the legal definition of electronic evidence in their national legislation.

Some countries have indirect definition, for example:

- In Austria and Belgium the Criminal Procedure Codes contain the regulation for subscriber, access, traffic and location data;
- In Slovenia they are defined as "information/data in an electronic format";
- Some Countries - Bulgaria and Slovenia - refer to the definitions provided for in the Budapest Convention on Cybercrime, and others - Belgium, Italy and Portugal - even to the Council of Europe (CoE) guide and doctrine;
- There are also references to the law on electronic communication that provides relevant definitions - Belgium and Slovenia.

The domestic approach in defining what electronic evidence is extends also to data categories, thresholds and national procedures for data request and disclosure. All Member States that provided input to the EJN indicated they recognise in general the following categories of data:

1. Subscriber data;
2. Traffic data; and
3. Content data.

In several countries additional data categories are foreseen in the national legislation; some examples are reported in Table 8[50].

Table 8: National definitions of electronic data categories

Romania	Access data and location data are divided into separate category.
Germany	Location data comes along with traffic data.
Czechia, Romania	Definitions provided for in the Budapest Convention on Cybercrime apply in judicial cooperation.
Portugal	Subscriber and access data were indicated separately - although with the same rules for their obtaining - and traffic and location data.
Estonia, Hungary	No difference for data categories as there are no different thresholds for preservation and production of data (Estonia); or whether data can be obtained by taking coercive measures or by submitting a request, nor are there requirements and thresholds for access (Hungary). Additionally, for Hungary the classification of data has significance only when choosing the proper technical method for performing an investigative measure.

In general, the threshold and procedure of obtaining data depends on the level of intervention into privacy, with basic subscriber information having the lowest, and content data the highest standard of judicial requirement.

Nevertheless, in Denmark a court order is necessary to obtain subscriber data, meanwhile in other Member States, law enforcement and/or prosecutors have the ability to receive this information. Important information of practical nature was provided by the Netherlands, where, due to the many reseller-constructions in the businesses of hosting providers, subscriber data is often in possession or control of the foreign-based reseller and the degree of collaboration depends on the willingness of the OSPs[51].

The legal systems becomes more complex in relation to traffic data (where the common

rule to access it is with the authorisation by a court/judge), including location for those countries that classified it into a separate data category. The threshold that allows authorities to obtain access to this category of data is mostly related to the seriousness of crime and the competent body that authorises the access. Besides, in the countries where data retention is not legally foreseen[52], it becomes technically hampered, if not impossible, to obtain historical traffic/location data.

For the seriousness of crime, the main criteria is the length of imprisonment that varies from at least 1 year (Belgium) up to the 5 (Bulgaria) or even 6 years (Denmark). Countries such as Denmark, Germany, Portugal and Slovenia have also a list of crimes that allows authorities to obtain traffic data during the investigations.

As mentioned previously, the strictest conditions apply for obtaining content data, which requires national authorities to present additional justification such as: purpose, necessity, reasonable grounds for the relevance of data requested for the criminal proceedings, assessment of the proportionality of intervention into privacy, and, - what is a common rule - the acquisition of an order from a court/judge.

It appears therefore clear that, in line with the diverse characteristic, provisions and requirements pertaining to the multiple categories of data, a variety of channels are available to competent authorities to request and obtain disclosure of electronic information.

As demonstrated by the direct feedback from EU judicial authorities surveyed, the disclosure of data from foreign OSPs is not an immediate process and the length of different procedures can have a significant impact in the conduction of investigations[53]. Hence it is fundamental to rely on a mechanism that would guarantee that data is kept available by OSPs while the process for its requests is ongoing. The information collected in the Fiches Belges show how all respondents[54] reported that preservation of data is possible in their countries to a greater or lesser extent.

The main differences between Member States, on this topic, are:

- time limits for preservation (30 days, 90 days, 6 months or 12 months) and the possibility for extension;
- the authorities competent to request preservation (usually authorisation by a judicial authority, either by a prosecutor or by court, is required).

When it comes to voluntary cooperation with the OSPs, the regulation of the procedures and even the admissibility of the evidence differs depending on whether a MS acts as an issuing or as an executing country. Complementing the direct feedback received and presented in Table 2, among countries that deem admissible evidence acquired directly from the foreign-based OSPs, there are: Czechia, Finland and Sweden. Additional Member States listed also further criteria as presented in Table 9.

Table 9: Regime of voluntary cooperation in the EU

Austria	If the data is necessary for the prevention or investigation or prosecution of a criminal offence or for the execution of a sentence, if the public interest on the request overweighs the fundamental rights of the person concerned and if the involvement of the competent authority in the requested State would be ineffective or inappropriate.
Belgium	Consent of user is needed.
Bulgaria	If the OSP abroad has access to subscriber data and if foreign OSP provides services also in Bulgaria and if there is no violation of sovereignty.
Italy	Consent of user is needed.
Netherlands	If the OSP abroad has access to the subscriber data and provides also services in the Netherlands, and if there is no violation of sovereignty.
Slovenia	The consent of data possessor is needed; the court decides on admissibility on a case-by-case basis.

The other respondents - Estonia, Hungary, Romania, Latvia and Slovakia - indicated that an official MLA request is needed in order to use the obtained information as evidence in the criminal proceedings; otherwise, it may be used for intelligence purposes.

As previously mentionned, when a Member State plays the role of the executing country, many either restrain or have no legislation that would allow domestically-based OSPs to provide information directly to foreign authorities. Complementing the direct feedback received and presented in Table 3 the Countries that generally do not allow domestic OSPs to respond to direct requests submitted by foreign authorities are: Austria, Denmark, Estonia, Finland, Latvia and Sweden.

Other Member States provided detailed information as follows in Table 10.

Table 10: Countries that generally do not allow domestic OSPs to respond to direct requests from foreign authorities

Belgium	Theoretically there is a possibility for Belgian OSPs to cooperate with foreign authorities under Article 18 of the Budapest Convention on Cybercrime, but it is believed that they would be reluctant to do it without notifying the Belgian judicial authorities and asking permission.
Portugal	No legal regulation yet it is possible to use the 24/7 Network to obtain subscriber and access data as no judicial authorisation is needed.
Spain	No legal regulation yet it is possible to use the 24/7 Network to obtain data for which no judicial authorisation is needed.

On the other hand, OSPs from Italy and the Netherlands may directly provide data to foreign authorities but only on a voluntary basis and only regarding subscriber data (Netherlands). Nevertheless, Italy indicated that usually OSPs would require a court order to disclose information, whereas for the Netherlands an MLA request would be needed in most cases due to legal and contractual issues.

Voluntary cooperation, as seen throughout this report, is not the only channel for competent authorities in the EU to engage with OSPs. Since all the respondents[55] have ratified the Budapest Convention on Cybercrime, the range of investigative measures which are available for the international cooperation regarding electronic evidence, is rather similar in all EU Member States. Moreover, Austria, Germany, Hungary, Slovenia and Sweden in their replies referred to the well-known principle that all the measures that are possible in a domestic

case can be executed upon a request for legal assistance. In addition, the principle of reciprocity, which provides a chance for successful cooperation even in the absence of any common legal instrument, was mentioned by Austria, Belgium, Bulgaria, Denmark, Netherlands, Slovakia and Slovenia.

Summarising the replies along with the Articles 26, 29-34 of the Budapest Convention on Cybercrime[56], which provide investigative measures for international cooperation, the measures reported in Table 11 may be performed in the following Member States[57]:

Table 11: Investigative measures available in the EU

Spontaneous information (Art. 26)	Austria, Belgium, Bulgaria, Denmark, Latvia, Lithuania, Netherlands, Portugal, Slovakia, Spain.
Expedited preservation of stored computer data (Art. 29)	Austria, Belgium, Bulgaria, Czechia, Denmark, Estonia, Germany, Hungary, Italy, Latvia, Lithuania, Netherlands, Portugal, Romania, Slovakia, Slovenia, Spain.
Expedited disclosure of preserved traffic data (Art. 30)	Austria, Belgium, Bulgaria, Czechia, Denmark, Estonia, Germany, Hungary, Italy, Latvia, Lithuania, Netherlands, Portugal, Romania, Slovenia, Spain.
Mutual assistance regarding accessing of stored computer data (Art. 31)	Austria, Belgium, Bulgaria, Czechia, Denmark, Italy, Latvia, Lithuania, Netherlands, Portugal, Slovenia, Spain.
Trans-border access to stored computer data with consent or where publicly available (Art. 32)[58]	Austria, Belgium, Bulgaria, Denmark, Hungary, Italy, Lithuania, Netherlands, Portugal, Spain.
Real-time collection of traffic data (Art. 33)	Austria, Estonia, Hungary, Latvia, Lithuania, Portugal, Slovenia, Spain.
Mutual assistance regarding the interception of content data (Art. 34)	Austria, Estonia, Hungary, Latvia, Lithuania, Portugal, Slovenia, Spain.

Finland, being a party to the Budapest Convention on Cybercrime, in its reply referred to the following measures: request for information to service providers; confiscate/copy a document; search of data contained in a device/remote search; traffic data monitoring; telecommunications interception.

For Sweden, the absence of ratified Budapest Convention on Cybercrime does not mean that obtaining of electronic evidence can be compromised since search and seizure, request for subscriber information and secret interception of telecommunication (both traffic data and content data) and secret data interception is possible (the latter being used to circumvent encryption for serious offences).

Concerning the international legal framework that is applicable in the context of judicial cooperation, there is a strong uniformity in the replies received. The Directive on the European Investigation Order[59] is the major instrument to obtain electronic evidence across EU. For those Member State that do not take part in the EIO Directive (Denmark and Ireland), other international acts are available and refer to:

- European Convention on Mutual Assistance in Criminal Matters with additional protocols (1959);
- EU Convention on mutual assistance in criminal matters (2000);
- Budapest Convention on Cybercrime (2001).

Ratified by all respondents except Sweden; this does not jeopardize legal cooperation with Swedish authorities – the above mentioned conventions still provide a broad opportunities to retrieve necessary digital evidence. Italy, in turn, stressed that the Budapest Convention on Cybercrime can be used only when no other convention or treaty is applicable.

Furthermore, almost every Member States pinpointed to UN Conventions[60], such as:

- UN Convention against Transnational Organized Crime (2000);
- UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) – can be useful for judicial cooperation.

Apart from that, multilateral and bilateral treaties, as well as principle of reciprocity can be in force in cooperation between Member States.

In a Union where 27 Members States cooperate on a daily basis the element of the working language is not to be overlooked. The applicable language rules mostly depend on the legal instrument that is being used in cooperation since many Member States declared different languages for different international acts. For example, some countries (Austria, Bulgaria, Netherlands, Slovakia) accept broader scope of languages with the Council of Europe conventions than when working with EIO. Along with the official language(s) of the Member States, English is considered the most common language that authorities accept when receiving requests. Exceptions from this rule are nonetheless present and interest: Austria, Bulgaria, Czechia, Germany, Italy, Spain, Slovakia and Portugal where authorities only accept requests drafted in their respective national language(s). However, even then, it is possible to send a request in another language upon the principle of reciprocity (as it happens in Austria for instance). In any case countries are invited to keep in mind the time that would be needed for translation of a request into the national language of the executing state: this, as a matter of fact, may cause delays in the execution phase of an order/request.

PERSPECTIVE OF LAW ENFORCEMENT

In order to capture the perspective from EU law enforcement in relation to the processes for cross-border access to electronic data in 2019, Europol conducted an extensive research with LEAs. 220 officers from all EU Member States contributed their experiences and opinions, as well as success stories, which demonstrate how important electronic data is in fighting crime and fostering security. This research present similar results when compared with data from the SIRIUS EU Digital Evidence Situation Report 2019[61], confirming trends and showing some developments. Furthermore, this chapter also presents results of a separate survey dedicated to the relevance online gaming platforms in criminal investigations in the EU.

A. Success cases

In many circumstances, digital data is crucial for criminal investigations and may be the only option to identify and/or locate criminals and victims, as well as serve as evidence for prosecution. Europol invited law enforcement officers to share some of the successful cases they had in 2019, in which requests to OSP for disclosure of data was used. The responses received make it clear that cross-border access to data is paramount in a wide range of crime areas, for example allowing the police to locate abducted minors, prevent terrorist attacks and identify suspects, saving numerous lives. Some of the responses received are presented below:

- *We had to find an abducted child. We did know the offender, but not his location. So we asked Facebook for disclosure of specific data (because the offender communicated over Facebook) and they could provide us GPS data. Therefore, we could arrest the offender and rescue the child.*

- *We identified a person who threatened a rampage at a shopping mall based on IP address data disclosed by Facebook.*

- *We were able to identify an ISIS fighter using a messaging app based on the IP address, which we received from an Online Service Provider.*

- *In most cases, electronic evidence obtained through direct requests or MLA is essential in investigations. However, the most rewarding ones are cases related to search of fugitives and search of missing, kidnapped persons. We have a number of success stories in relation to these two types. In case of missing or kidnapped persons, emergency procedures are usually used.*

- *Several foreign-based OSPs have disclosed data in cases like missing minor in combination with sextortion and with that information we found a lot of missing minors.*

- *The kids of a famous person were threatened on Instagram. Based on information that was provided by Facebook (upon a valid Emergency Disclosure Request) the suspect could be investigated before serious damage took place.*

- *This department was conducting investigations against an international organized crime group that was offering agricultural machines online. Criminals used bank accounts from [country A], e-mail accounts from [country B], VPN, hacked accounts from [country C] and acted from [country D]. The group affected victims all over Europe. Obtaining information from foreign-based OSPs was one of the keys to identifying this group, including their heads!*

- *We prevented an attack on our royal family with information from Google.*

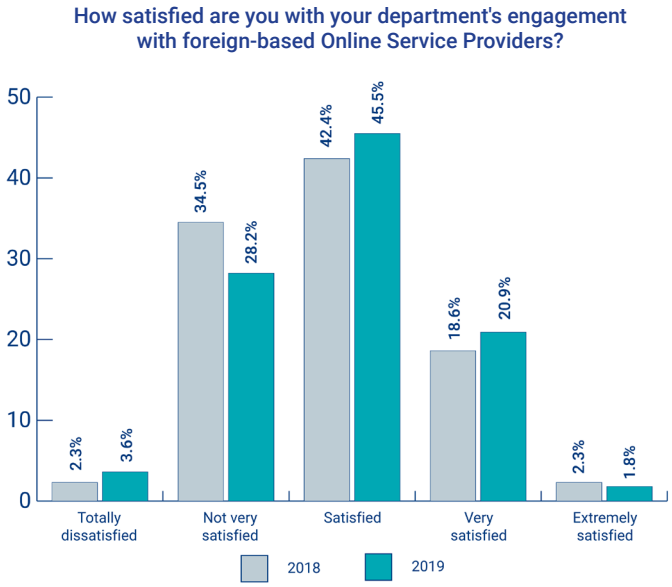
- *Due to a request for registered user data, several cases of money laundering and fraud have already been successfully identified. In a murder case, the data from Google's location was the main indication*

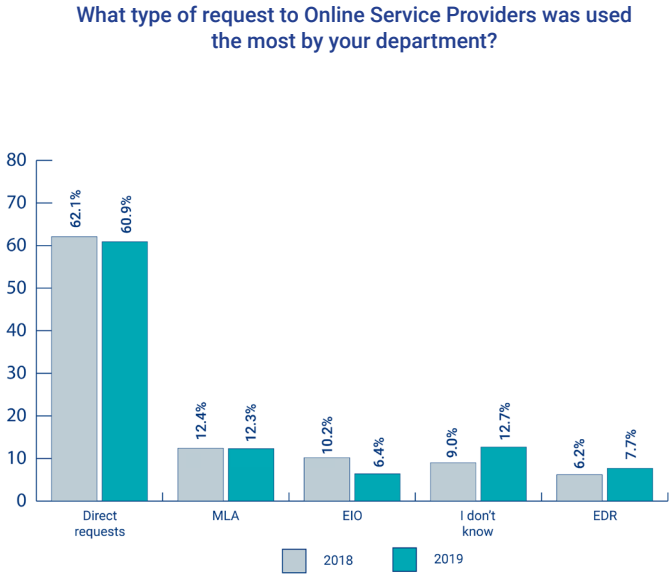
of evidence and conviction. We use the Sirius platform regularly, especially because of the Guidelines.

- *In many of our cases, the use of electronic evidence lead to the suspects or allow the identification of a victim. It is simply the time delay that causes the issues.*
- *It has already been possible in several cases to identify offenders using the mobile phone numbers or e-mail addresses disclosed by Facebook or Instagram. This works very well.*
- *There are many cases that were finalized or guided directly through the use of direct requests, since in most cases we require basic subscriber information confirmation to acquire a search warrant. This kind of confirmation provides plausible cause in terms of [country] Criminal Law. SIRIUS is being used on daily basis, in numerous different ways, including guides on contacting OSPs, Tools, Guidelines etc.*

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

The research conducted with law enforcement from all EU Member States shows that 45.5% of respondents report being satisfied with their department's engagement with foreign-based OSPs, as opposed to 28.2% of them stating they are not very satisfied.





To complement the quantitative analysis presented above, respondents were invited to evaluate the current process of lawfully requesting data from foreign-based OSPs in the context of criminal investigations. Europol received numerous responses from officers providing their opinions in the matter, presenting both positive and negative views.

Selected responses in relation to the existing processes are presented as follows:

Positive:

- *Processes are getting better, due to training and sharing experiences nationally and via Europol, the processes of emergency disclosures and MLAs are more successful. However, companies outside and inside EU do not have standardized approach to requests. Mostly recommended, even within emergency requests, is to contact company via MLA or investigation order, which could make the process longer.*
- *I have good experiences with law enforcement portals. Because they are user-friendly and clear.*
- *Basically the process works well. Sometimes, when short on time, it is difficult to get a court order in time. Therefore, requests are often rejected. In addition, sometimes it is necessary to discuss the release of the requested data, especially content data, which takes time. It would be good if all OSPs would allow an online request, similar to Facebook. A direct contact person in case of problems would also be a relief.*
- *The process of voluntary data transfer works very well. In some cases, the functionality of the platforms and easier operation could be implemented.*
- *The procedure is at the moment fairly simple, as data can be requested in several ways. The biggest issue is the length of the process (takes a lot of time to acquire the original content data), while BSI is fairly easy to acquire for a good part of OSPs.*
- *For every direct request, I first check SIRIUS platform to verify if something changed in the request procedure. Using the published templates on SIRIUS we already had a lot of positive answers upon our requests.*
- *Process is getting better although there are still many companies that don't answer requests in a sufficient way. Another problem is that public prosecutors tend to avoid EIO or MLA, so we have to live with what we get on a voluntary base.*

Negative:

- *Slow and unreliable. Companies are not transparent about the data they have on their customers, making it hard to draft the proper request. Also, companies keep hiding behind jurisdiction even though they have EU / local presence. The MLA process is in many cases too slow for digital evidence.*
- *The process is complicated, as every OSP has different policies. Requests are answered slowly. Most of the time, data disclosed does not help in the investigation, as IP data is not provided or too old (IP addresses can only be traced back seven days in [country A]).*
- *Disparate, unclear, varies upon provider, extremely slow, bureaucratic with too many barriers to cross to identify entity data quickly in order to identify locations, possible accounts and therefore individuals.*

By the time we do receive this, other evidence potentially held on devices, financial, CCTV, etc is gone.

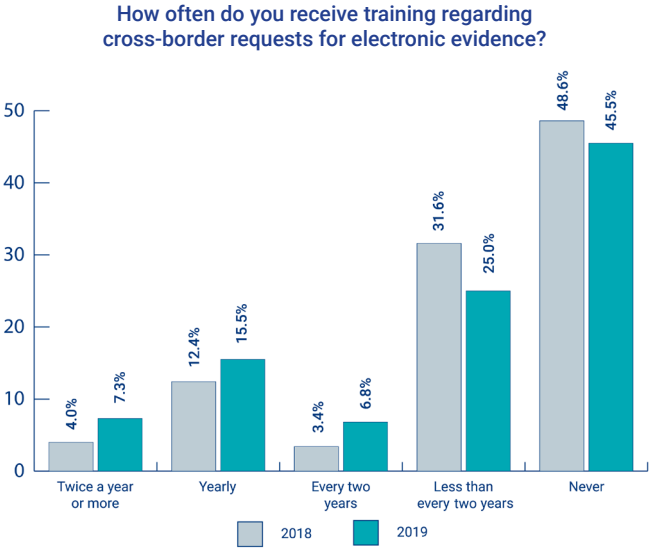
- *Very time consuming and cumbersome. No handling against rejected requests although legal requirements are met. Inquiries only possible in English, no clerks with knowledge of my national language. This makes the explanation of difficult facts and the legality of the request very susceptible to misunderstandings.*

- *Difficult and confusing process for most of the police officers. Often there is only one person in every unit, who does the requests for the others.*

- *Judicial (EIO and MLA) process takes way too long to be useful, especially in cybercrime cases.It would be useful to standardize processes, information to be requested and to be properly updated about changes. It would be useful to have a contact person for our country to clarify and solve any doubts that may arise in a short period of time.*

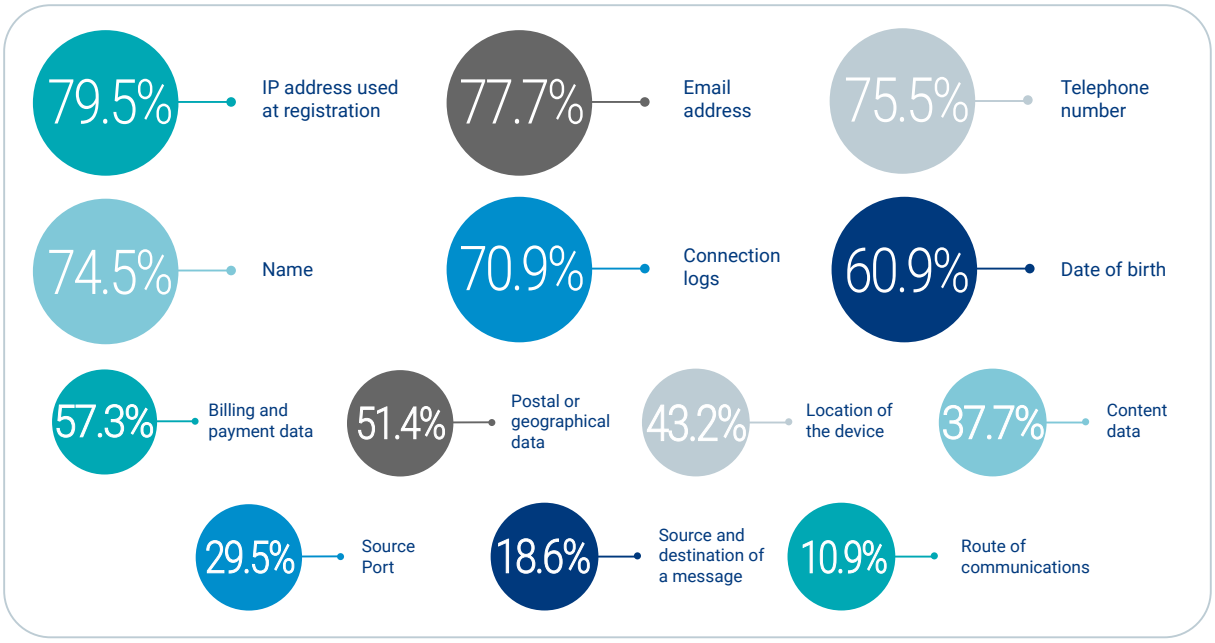
Direct requests from LEAs to OSPs for voluntary cooperation remains the most used aproach, chosen by over 60% of respondents as the main type of request. In relation to the previous year, there has been a 1.5% increase in the importance of emergency disclosure requests and a decrease of 3.8% in relation to EIOs.

There is a significant increase of 9.8% in the number of officers that reported receiving trainings in relation to cross-border electronic evidence at least every 2 years. However, the number of officers reporting they never received such trainings remains high, at 45.5%.



In the survey conducted this year, Europol introduced a new question about the most important types of data needed for investigations. Instead of using the terminology basic subscriber information and traffic data, which may allow room for different interpretations, respondents had the option to choose specific datasets which they consider to be the most important ones in criminal cases. Results show that the five most important datasets in criminal investigations are: IP address used at registration, e-mail address, phone number, name and connection logs (data, time and IP address of connection), as they where selected by over 70% of respondents. It is worth noting that 37.7% of respondents consider content data (data in digital format such as text, voice, videos, images and sound) to be amongst the most important types of data to investigate and prosecute crime.

In the majority of the investigations in 2019, what are the most important types of data your department needed?

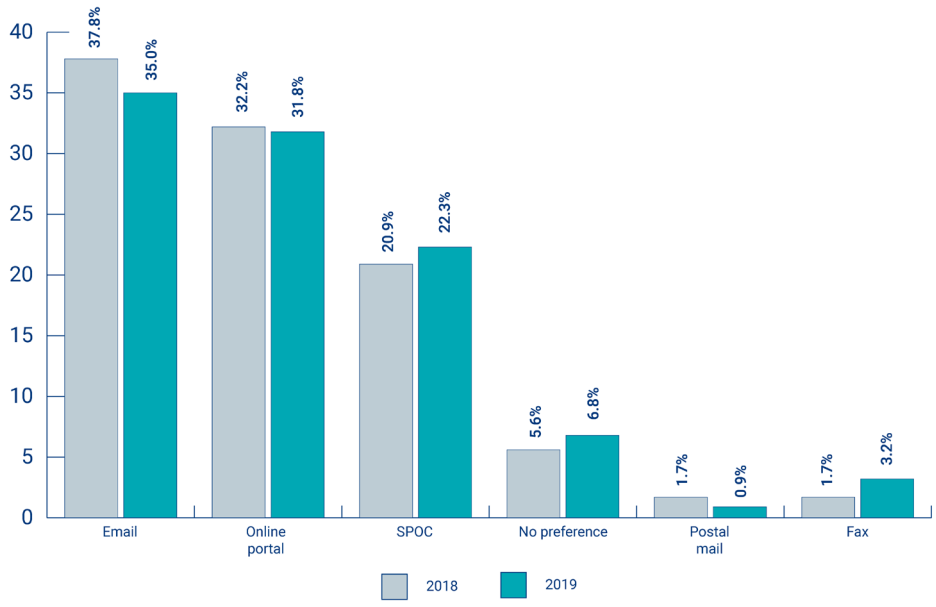


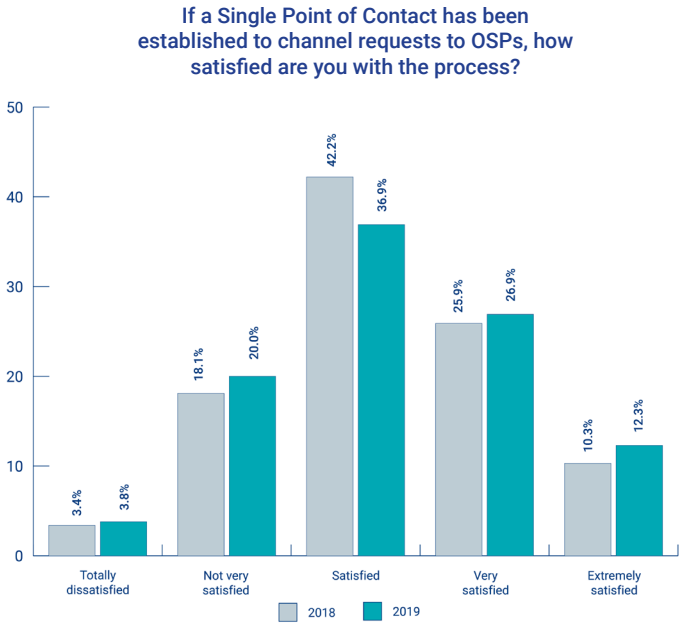
Other datasets that were mentioned by less than 10% of respondents as the most important do not appear above. These datasets are:

- Duration of communications: 9.5%
- Format of data: 5.5%
- File size: 4.1%

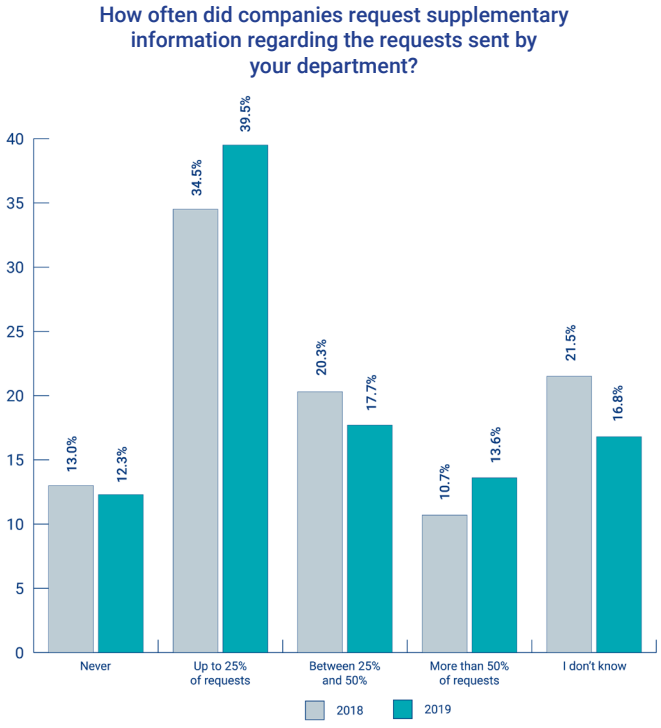
C. Submission of cross-border requests

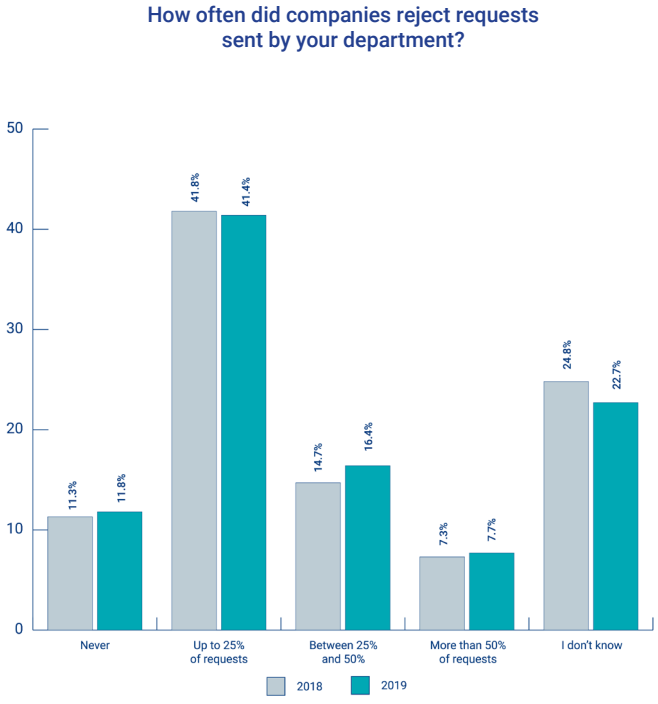
What is your preferred channel for submission of direct requests to Online Service Providers?





In relation to the preferred channels for submission of requests from LEAs to OSPs, there has been only very slight changes in relation to last year's results. E-mail remains the preferred channel for submission of requests, appointed by 35% of respondents, followed by dedicated online portals, appointed by 31.8%. The least favourite channels remain fax and postal mail. In countries and/or agencies where a SPoC has been established, 76.2% of respondents stated they are satisfied, very satisfied or extremely satisfied with the process (130 respondents out of 220 responded to this question).





13.6% of respondents stated that OSPs asks for supplementary information in the majority of the requests sent for disclosure of data, while 12.3% said they were never asked for it. In relation to rejection of requests by the OSPs, 7.7% of respondents said it happened in the majority of the cases. 41.4% of respondents stated that less than a quarter of all the requests sent by their department were rejected. To illustrate those cases, respondents had the option to write what are the most common reasons stated by OSPs for rejection of their department

requests to OSPs. The most mentioned reasons were:

- MLA is required;
- Recent IP addresses from the targeted user are not from my country;
- The data is no longer available;
- Data stored in a country where the investigated actions are not a crime (e.g. defamation or hate speech cases);
- Requests do not meet all the company's requirements.

In certain situations, officers may require assistance to prepare direct requests to OSPs or to initiate a MLA request. In relation to direct requests, 36.8% of the respondents stated they consulted a SPoC, followed by 28.7% who used the SIRIUS Platform and 23.2% who sought assistance from their National Central Unit. These top three responses remained the same in relation to the data from previous report[62]. However, it is worth noting some differences. On one hand, both SPoCs and National Units had a decrease of 3.9% and 4.5% respectively. On the other hand, the use of the SIRIUS Platform for assistance on direct requests has increased 6.6%.

Responses that scored less than 6% in relation to assistance in the preparation of direct requests were:

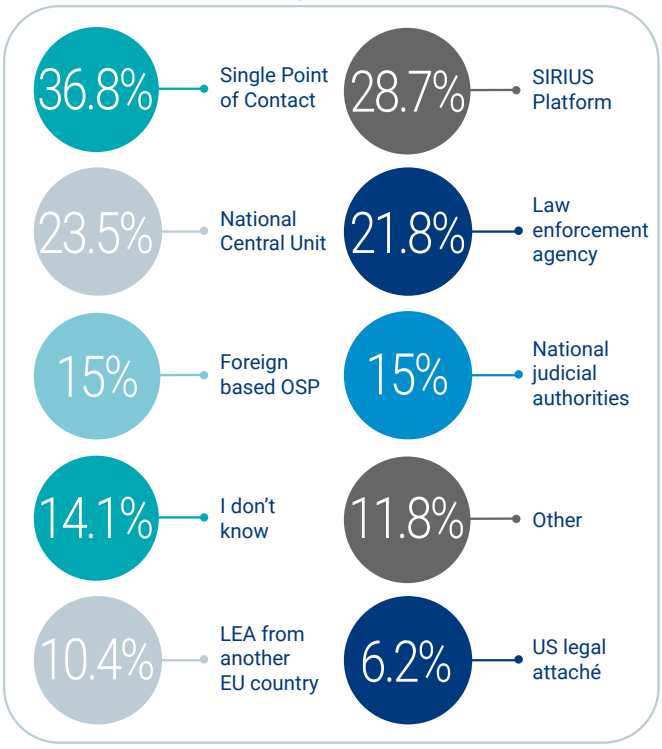
- Law enforcement agency from a non-EU country: 5.5%
- Other: 4.5%
- US Department of Justice: 0.9%
- US Embassy: 0.9%

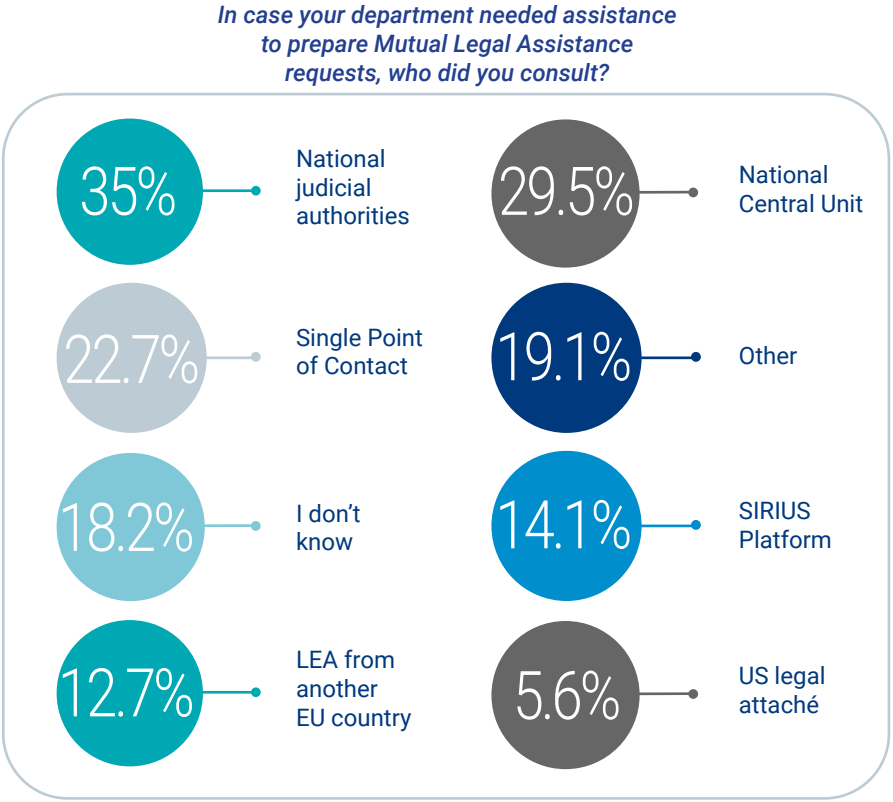
When it comes to assistance in relation to MLA, 35% of respondents stated they consulted national judicial authorities, followed by 29.5% who consulted National Central Unit and 22.7% who consulted SPoCs. The SIRIUS platform was consulted by 14.1% of respondents, which represents an increase of 9.0% in relation to the previous year.

Responses that scored less than 6% in relation to assistance in the preparation of MLA were:

- Other: 5%
- Foreign-based online service providers: 5%
- Law enforcement agency from a non-EU country: 3.6%
- Agency from another EU country: 2.7%
- US Department of Justice: 1.4%
- US Embassy: 1.4%

In case your department needed assistance to prepare direct requests to companies, who did you consult?





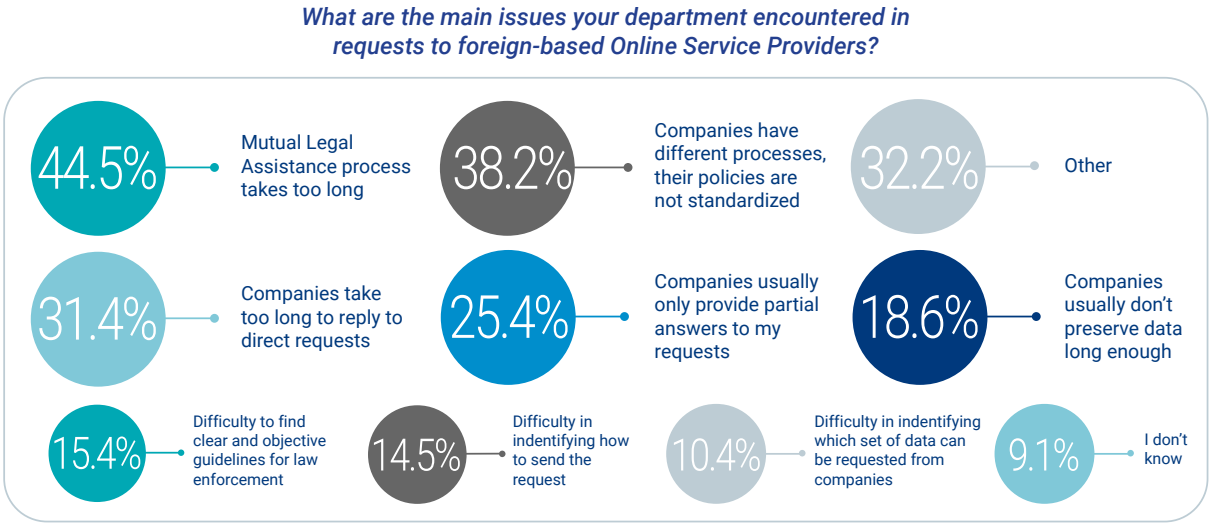
D. Issues encountered by EU law enforcement

LEA officers were invited to appoint up to three main issues faced by their department's engagement with OSPs, in the context of cross-border requests for electronic evidence in criminal investigations. In this survey, the first two issues were exactly the same ones as in the previous year. The first one was the long period for obtaining data via MLA, which was chosen by 44.5% of respondents. The second main issue was the lack of standardization of companies' polices and processes, for 38.2% of respondents.

The third main issue reported was the long period for obtaining responses from companies. This is followed by the fact that companies only provide partial responses to requests. Only 1.4% indicated there are no problems in the process to request access to OSP data.

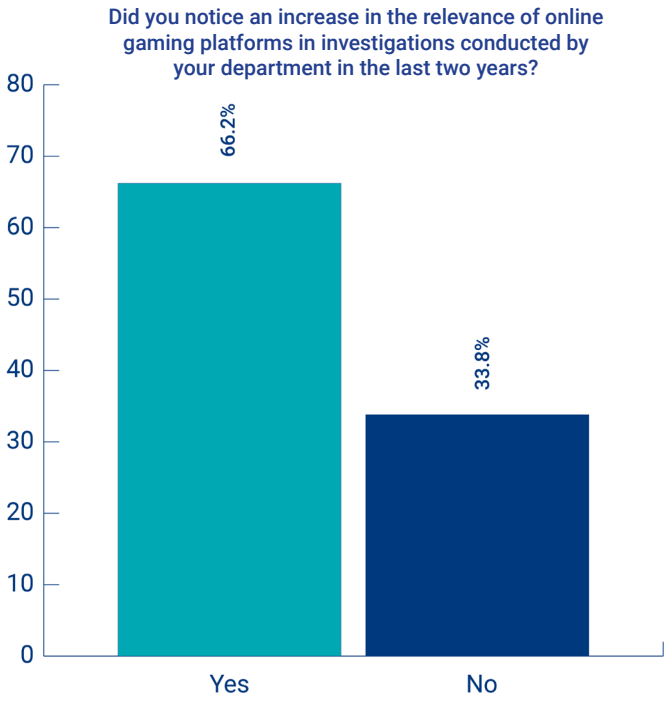
32.2% of respondents identified other issues, which scored less than 9% each:

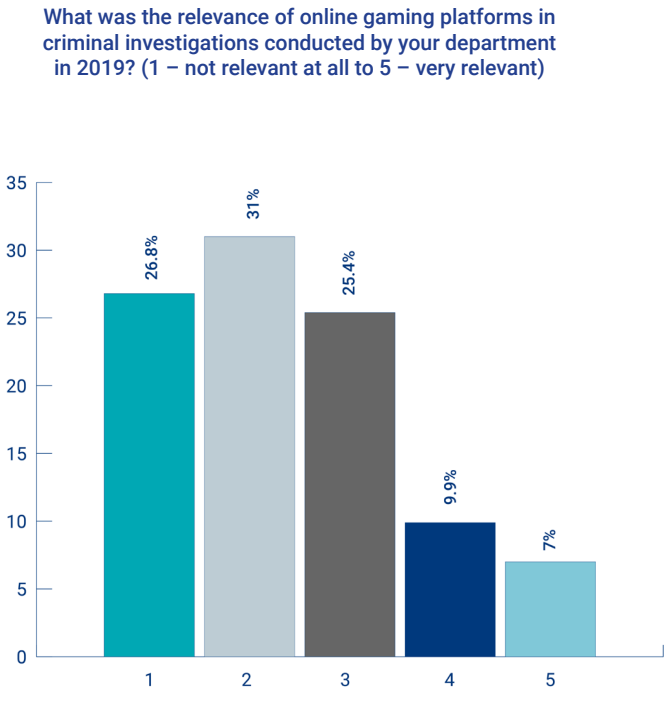
- Requests are usually only accepted in English, not in my own language: 8.6%
- Companies' guidelines are too complicated or too long: 8.2%
- Information is only available in English, not in my own language: 6.8%
- Companies' responses are not easy to analyse and understand: 5.9%
- Companies change processes and responses formats too often: 3.6%
- Lack of technological resources to analyse responses from service providers: 3.6%
- Other: 3.6%



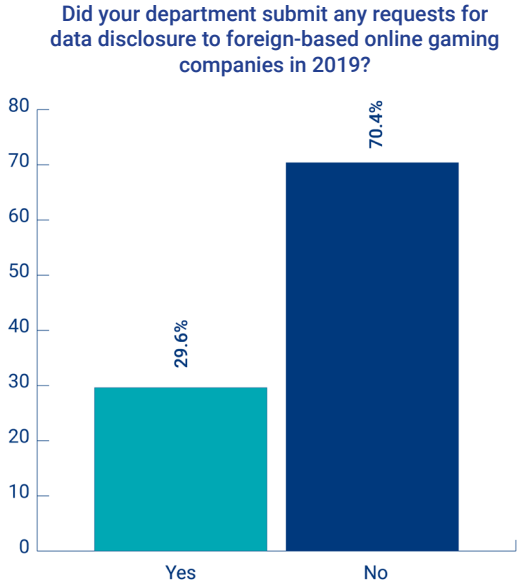
E. The relevance of Online Gaming Platforms in investigations

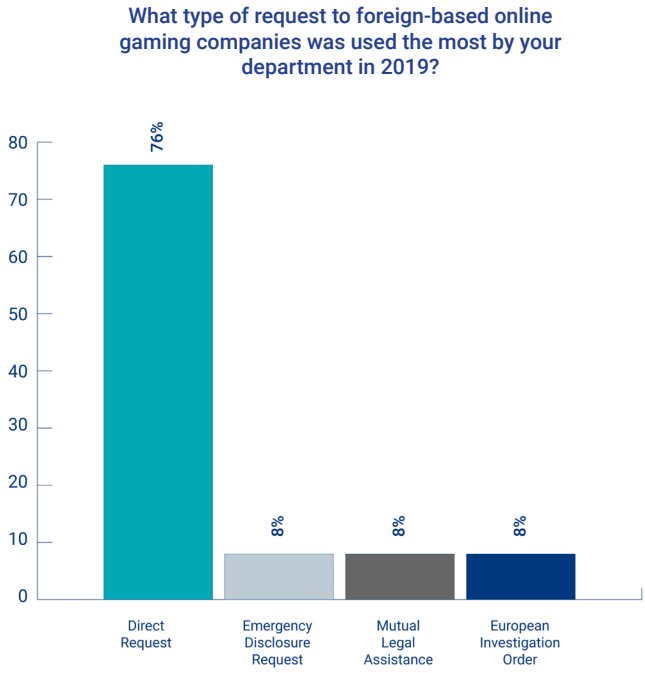
In order to better understand the relevance of Online Gaming Platforms (OGP) in investigations in the EU, the SIRIUS team conducted a separate survey. 66.2% of respondents state that they observed increased relevance of these platforms in criminal cases in the last two years. Despite this increase, only 7.0% of respondents say online gaming platforms were very relevant in investigations in 2019, while 26.8% say they were not relevant at all.

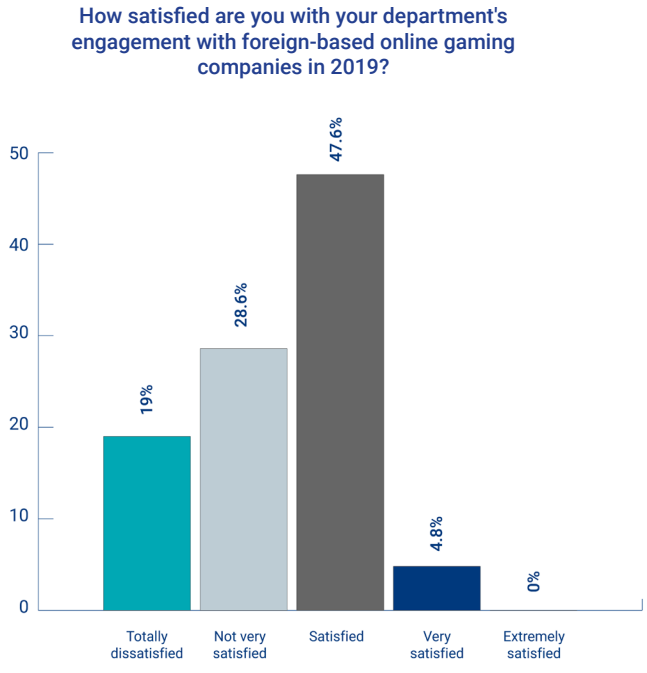




29.6% of respondents state that their department submitted at least one request for data disclosure to foreign-based online gaming companies in 2019. Among these respondents, 76.0% replied that the type of requests most used was the Direct Request and 52.4% say they are satisfied or very satisfied with the engagement.







PERSPECTIVE OF ONLINE SERVICE PROVIDERS

A. Analysis of Transparency Reports

Many OSPs periodically publish publicly available transparency reports, which include information about governmental requests for disclosure of data worldwide. Since not every country records central statistics in relation to requests to OSPs, the transparency reports offer an important source of information to understand the situation of the use of digital evidence in criminal investigations in the EU.

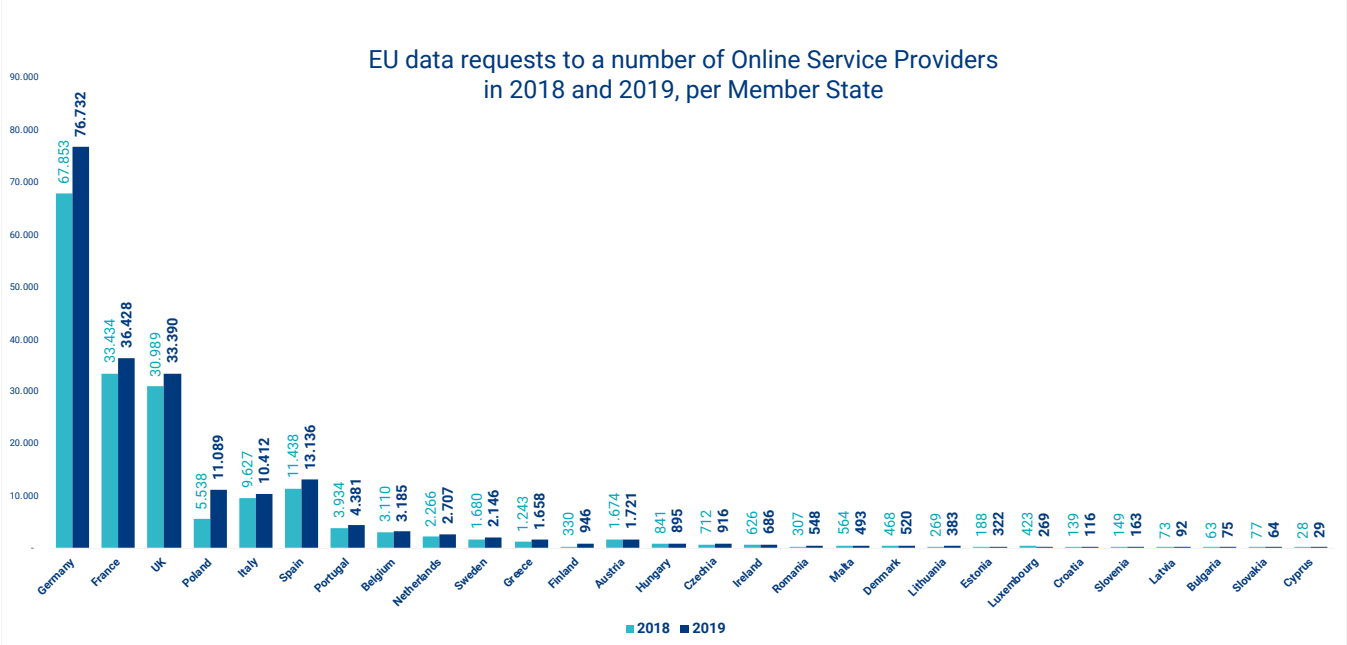
There are three main limitations in the use of transparency reports. First, there are differences in the way certain data is recorded and also in the type of data that is included. This makes it impossible to analyse certain data from a wider perspective. Second, in situations when requesters followed an MLA procedure, it may not be possible for the OSP to identify the country that originated the request. Therefore, data presented on transparency reports is likely to reflect mainly direct requests from authorities to foreign-based OSPs. Finally, not all companies publish transparency reports or include detailed information about requests in the EU. Hence, the data collected represents a fraction of all the requests for disclosure of data sent to OSPs.

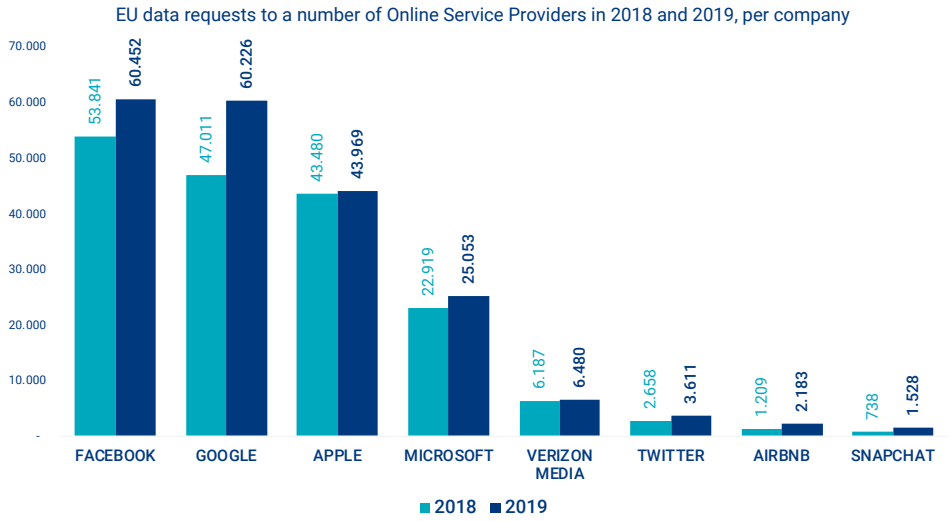
Data was collected from transparency reports published by Airbnb, Apple, Automattic, Cloudflare, Dropbox, Facebook, Google, LinkedIn, Microsoft, Snap, TikTok, Twitter and Verizon Media. However, OSPs that reported less than 100 requests from EU authorities in 2019 were not included in the analysis presented in this chapter[63].

Volume of data requests per country and per Online Service Provide

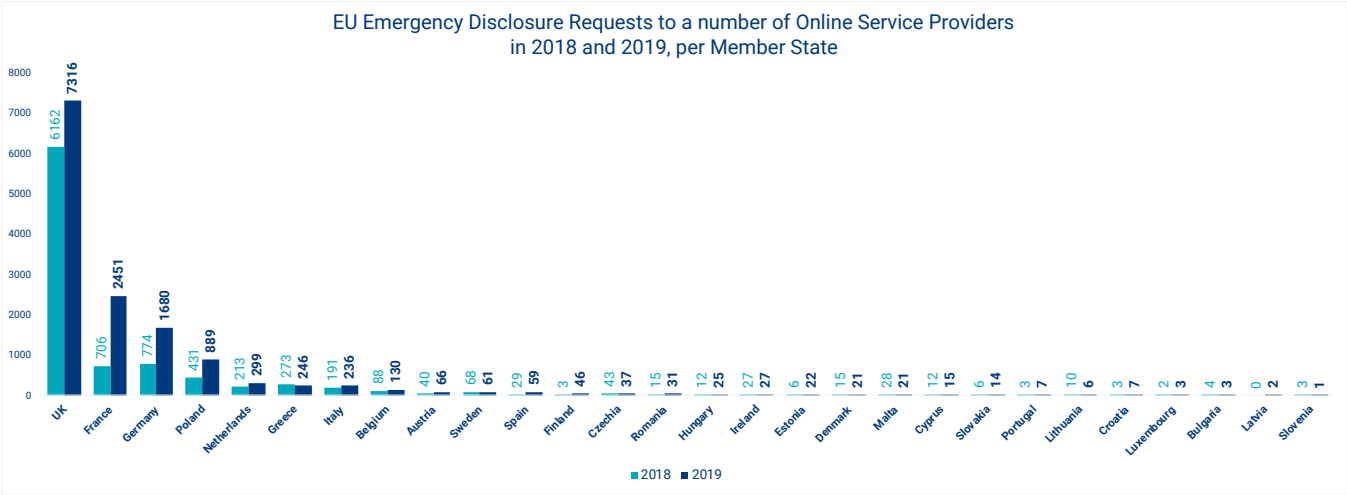
The volume of data requests submitted from EU authorities to OSPs increased by 14.3% from 2018 to 2019, taking into consideration data from Airbnb, Apple, Facebook, Google, Microsoft, Snapchat, Twitter and Verizon Media. The majority of all the requests (72.0%) were sent by three EU Member States: Germany (37.7% of requests), France (17.9%) and UK (16.4%). The countries that increased the most their requests from 2018 to 2019 were Finland (+186.7%) and Poland (+100.2%). On the opposite direction, four countries saw a decrease in the total volume of requests: Croatia (-16.5%), Luxembourg (-36.4%), Malta (-12.6%) and Slovakia (-16.9%). Facebook and Google remained the OSPs that received the majority of the requests (59.3% in 2019).

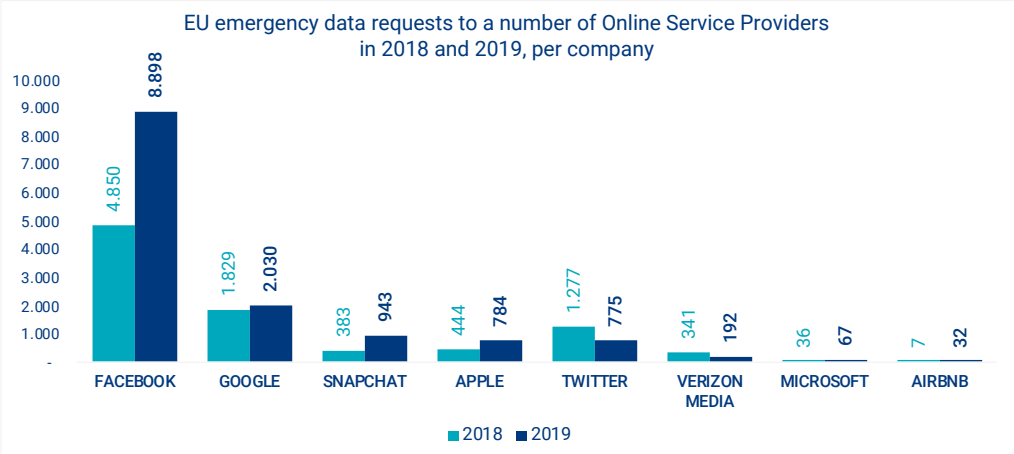
EU data requests to a number of Online Service Providers in 2018 and 2019, per Member State





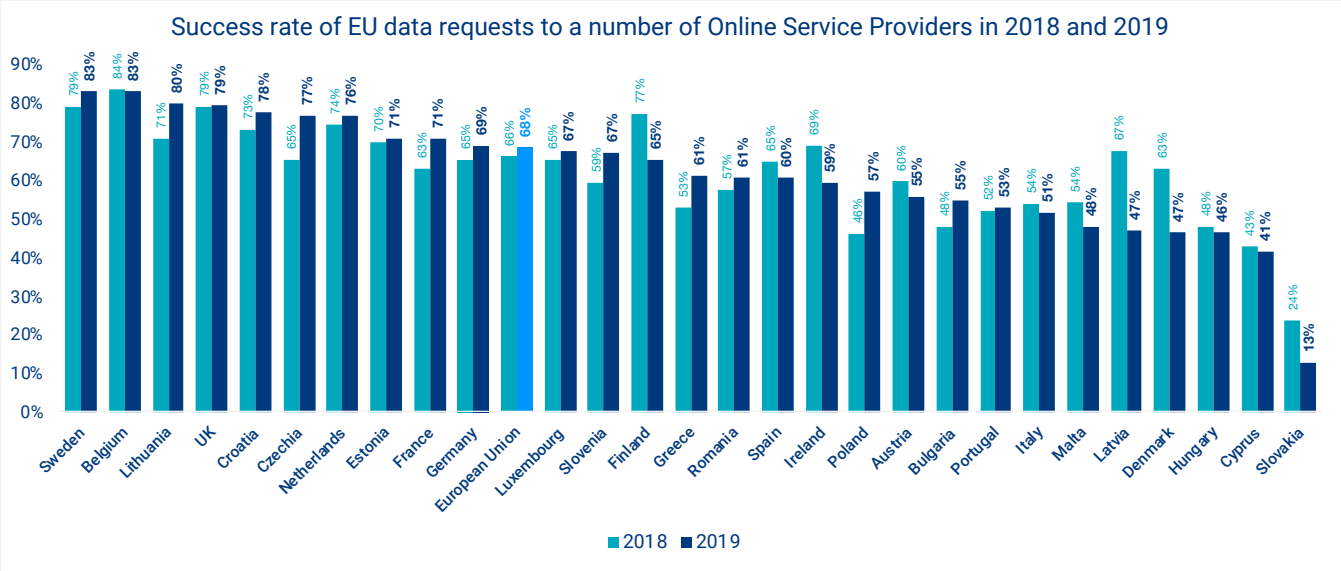
In relation to EDRs, there was an increase of 49.7% in the total volume from 2018 to 2019. The majority of EDRs was submitted by the UK (53.3%). France and Germany increased the number of EDRs by 247.2% and 117.1%, respectively. In 2019, Facebook remained the company that received most of EDRs and also showed an increase of 83.5% in comparison with the previous year.





Success rate of EU cross-border requests for electronic evidence

The success rate of EU cross-border requests for electronic evidence is calculated by dividing the total number of requests submitted by those to which some data has been disclosed by OSPs, taking into account the transparency reports of the companies previously mentioned. From 2018 to 2019, taking into account data from the OSPs mentioned above there has been an increase of 2.6% in the overall success rate in the EU: from 65.9% to 68.4%. Sweden, Belgium and Lithuania were the EU Member States with the highest rate. Germany, which submitted most of the requests, increased the success rate from 65.1% to 68.6%. The main reasons that led to unsuccessful requests are analysed on section 7.3 of this report.



B. Challenges from the perspective of Online Service Providers

With global presence and a high number of users, many OSPs also face challenges in dealing with worldwide data disclosure requests in criminal investigations. More specifically, two challenges were mentioned by most of the OSPs interviewed for this report, which are listed below.

- *Difficulty in disseminating updates and new relevant information at scale to governmental authorities*

Many OSPs reported that it is hard to disseminate updates and relevant information in relation to cross-border data disclosure requests at scale. Changes to the process of dealing with governmental requests and launch of new products and services generate the need to disseminate information to authorities that would be relevant for future requests. However, because of the large number of authorities at national level and the high number of countries concerned, disseminating relevant information frequently requires the allocation of many

resources. Many OSPs reported that the dissemination of updates is generally more effective in countries where SPoCs have been established. Moreover, many of these OSPs highlighted the benefits of the SIRIUS Project and its important role in promoting knowledge sharing amongst EU authorities.

- *Authentication of incoming requests*

The authentication of incoming governmental requests for disclosure of data in criminal investigations remains a challenge to most OSPs. In order to ensure the legitimacy of requests or new registration in their Law Enforcement Response Portals, OSPs generally rely on the e-mail domains used by authorities, as well as on signatures and stamps in the documents provided. In situations where the e-mail domain or other elements of the request cannot be verified by the OSP, some reported collaborating with previously established contacts in the country or with the alleged agency/institution via other means in order to ensure that the request received is valid. At scale, this is a process that requires time and resources.

C. Reasons for refusal or delay in processing direct requests for voluntary cooperation from EU authorities

Understanding recurrent issues in the process of requesting cross-border access to electronic evidence is an important step to identify potential improvements that could render data disclosure in criminal investigations faster and more effective. Although statistics in this regard are not available, interviews with OSPs indicated many of the main issues that lead to rejection or delays of requests were quite similar across different providers. OSPs also indicated that it is possible that the reasons vary depending on the country. Furthermore, some of them clarified that in the EU most issues generally are solved by contacting the authority, thus delaying responses, but not rejecting all the requests.

This year, four of the main issues mentioned by OSPs remain the same as the ones described in last year's report and are listed below. Two issues mentioned in 2019 were not cited this year: "Requests for data that require judicial cooperation" and "Lack of preservation request". Finally, a new issue has been mentioned by OSPs: "Miscommunication when OSP request additional information". All the items reported by OSPs in 2020 are listed below, following a random order.

- *Wrong legal entity addressed*

Many OSPs have offices in several countries, but not all of them store user data. They may have one or even several legal entities acting as data controllers, depending on the location of the user. In certain cases, authorities address requests to wrong legal entities of the same company, which are not acting as data controllers for data related to the targeted user. In these situations, authorities are often requested to amend the original request or to issue a new one, with the correct name and address of the appropriate legal entity.

- *Non-existent data*

There are several reasons why data may be non-existent. For example, data could have been deleted by the user or the dataset requested is not collected by the company. Moreover, it is also possible that the account identifier has been misspelled in the request or the account never existed.

- *Wrong account identifier provided*

Account identifiers are unique datasets that are linked to one specific user account in a given platform. For instance, e-mail addresses and phone numbers with country code are generally good identifiers. However, there can be confusion in relation to user names, vanity names, account IDs and URLs, as depending on the platform they are not unique and/or can be changed at any time, several times. Whenever a given dataset is not unique or is not collected by the OSP, it does not serve as a valid account identifier. Because this varies a lot from company to company depending on their business needs and models, it is frequently a reason that leads to delays and rejection of data disclosure requests.

- *Lack of reference to legal basis for direct requests under the domestic legislation of the requesting authority*

When reviewing incoming requests for data disclosure from authorities based outside of their own jurisdiction, some OSPs require that the requesting authority lay down the legal basis for such requests under their domestic legislation.

- *Overly broad requests*

When requests are not very specific regarding the datasets concerned or for any other reason they would lead to the disclosure of a large amount of data about one or more users, they may be considered disproportionate and overly broad by OSPs. It is worth noting that not every company provides clear information to authorities in relation to all the datasets collected, which can also lead to broad requests for data disclosure. Some OSPs have indicated that this issue has improved in comparison with the last year and that they have the impression that authorities have a better understanding of the datasets that may be requested.

- *Miscommunication when OSPs request additional information*

Some OSPs have indicated that a recurrent issue is the miscommunication with the requesting authority when additional data is required. They reported that in some cases there is a long delay in responses from the requesting authority or that their messages have not been properly interpreted.

THE SINGLE POINTS OF CONTACT APPROACH

A. SPoC concept

Keeping up-to-date knowledge regarding online platforms products and services, as well as their policies and contacts, requires a large allocation of resources. This is because the digital environment is constantly evolving and authorities often need to ensure specialization of investigators and prosecutors to keep up with changes in the way platforms are abused by criminals, as well as companies' requirements for data requests.

Consequently, many law enforcement and judicial authorities have developed specific expertise in this area and have designated resources either to centralize requests and/or to support requesters in the process. These units or groups of specialized officials are commonly known as Single Points of Contact (SPoC), and may be more or less formal depending on the needs. In some countries, the creation of SPoCs happened organically and they became a centre of reference to deal with requests to foreign-based companies. In other countries, formal units were set up with the objective of dealing with such requests and improving the effectiveness of the overall process.

There is not a unique formal definition of what SPoCs are, but they generally can be divided in two types: SPoCs for centralization of requests and SPoCs for knowledge-sharing and support. Even with this categorisation, their structure and responsibilities still varies a lot, as further explained below. In any case, the SPoC process offers many benefits from LEAs, judiciary and OSPs perspectives and may facilitate the information flow in relation to cross border electronic evidence.

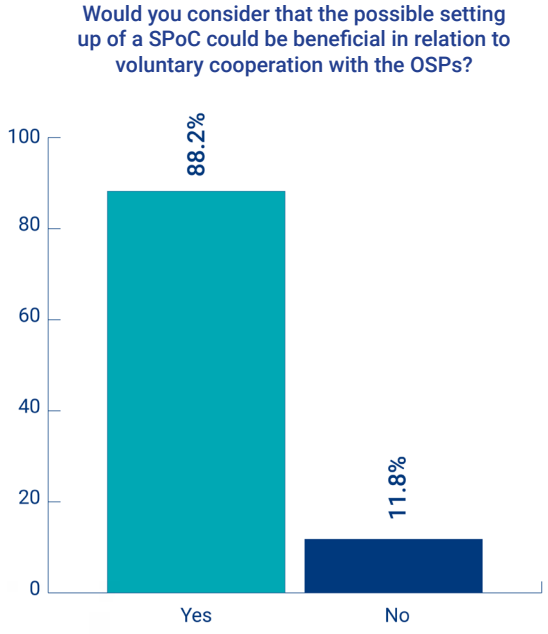
All the companies interviewed for the purpose of this report welcomed the SPoC approach and said their ability to provide fast responses is substantially higher. When dealing with requests submitted by SPoCs for centralization of requests, OSPs reported generally good quality of requests (e.g. procedural requirements in good order, correct identifiers provided, datasets specified) due to the specialization and experience of the requester. SPoCs with well-trained personnel are also preferred in emergencies, as the information flow is more direct and there is the possibility for direct contact if needed. OSPs also reported easier procedure to disseminate updates and other relevant information about their products, services and processes where there are SPoCs established.

In the EU, Austria, Belgium, Czechia, Denmark, Finland, France, Germany, Lithuania, Latvia, Malta, Netherlands, Slovenia, Spain and Sweden are the countries which reportedly have established SPoCs either for centralization or requests of for knowledge-sharing and support.

Even if not present in all EU Member States nor following one unique model, SPoCs and their establishment seem welcomed by the vast majority of EU authorities surveyed. Within the EU judiciary community, for

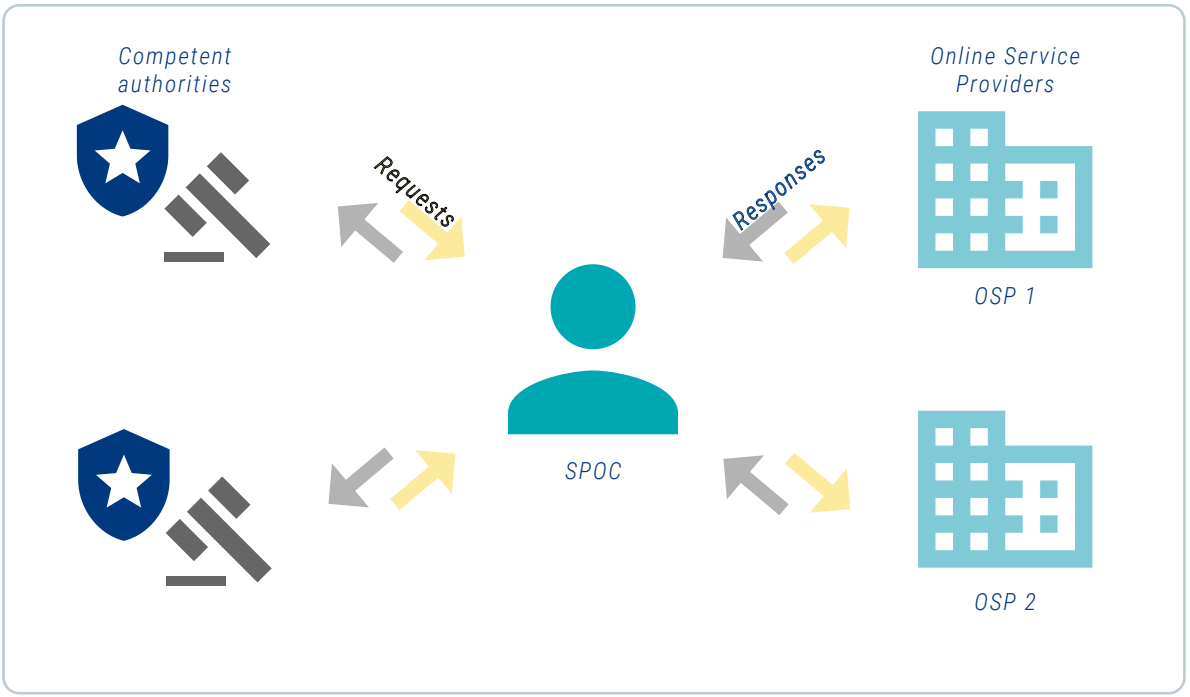
example, 88.2% of surveyed expressed themselves in this direction on the basis that SPoCs would bring about advantages such as:

- SPoCs would eliminate any doubts as to whether a direct request under voluntary cooperation is a viable channel. A SPoC dedicated to that would de facto certify it.
- A SPoC system would be beneficial at the level of the General Prosecution Office as it has the leading role of the criminal investigations.



A minority of respondents (11.8%) further explained its choice pointing towards past direct experiences that would make SPoCs not necessary, expressing its preference for a stronger coordination and formation of law enforcement and judicial authorities or pointing out that the biggest challenge remains the limit posed by voluntary cooperation with some OSPs.

SPoCs for centralization of requests



SPoCs for centralization of requests are designated persons, units or institutions who centralize, review and submit requests from governmental authorities to OSPs. These SPoCs are responsible for dealing with requests and receiving responses, acting as a reference point in relation to electronic evidence and engagement with national and foreign OSPs.

SPoCs receive requests from individual officers in different units, review them to ensure compliance with applicable legislation and policies, and send them to OSPs. Depending on how they are set up, SPoCs may receive responses from the OSPs and forward them to the original requesters. This way, SPoCs act as single entry point between OSPs and LEAs in a specific Member State, improving and standardising the quality of requests with a view to ensure faster responses.

SPoCs for centralization of requests perform tasks that may include:

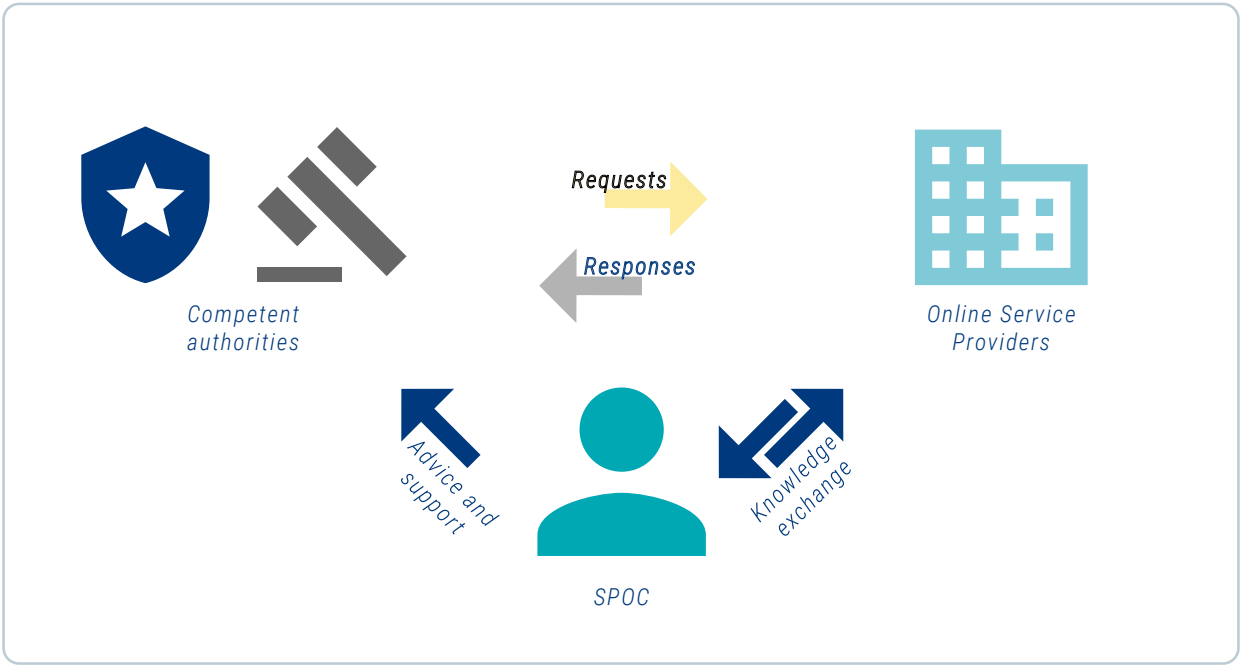
- Centralization of direct requests from national authorities in relation to electronic evidence to some or all OSPs;
- Ensure necessary standards in accordance with applicable law, as well as the companies' policies and requirements;
- Authorisation or validation of the submission of requests for voluntary cooperation in accordance with national legal framework or established working policy and/or otherwise providing legal or policy related advice to entities centralising the requests, related to the matters of voluntary cooperation with OSPs;
- Submission of the requests to OSPs using the necessary channels (e.g. e-mail, online portal for law enforcement, fax);
- Receive responses from OSPs and forward them to the officer or unit which originated the request;
- Process the responses from OSPs before sending them to the officer or unit which originated the request (e.g. parsing or decrypting data);
- Provide information and advice to national authorities in all OSP-related matters, acting as a national centre of reference;
- Engage with representatives from relevant OSPs to discuss issues in the process for requests for disclosure of data under voluntary cooperation;
- Coordinate information flow among different agencies in relation to outgoing requests regarding the same investigation;
- Gathering of statistics and monitoring the trends.

Therefore, SPoCs may deal with the centralization of direct requests for voluntary cooperation, depending on the agency. The process for the establishment of SPoCs for centralization of direct requests for voluntary cooperation is not rigid. In principle, once a unit or group of officials receives the mandate to act as a SPoC within an agency, they must

establish internal procedures. They must also provide clear guidelines on how investigators and officials must address requests to them as well as effective channels of communication between SPoCs and other units. It is necessary that SPoCs establish agreements with OSPs individually, so to initiate a centralized procedure. Based on such agreements, OSPs may start to accept only requests coming from SPoCs, while redirecting other requesters to the established procedure.

In relation to the internal processes, some SPoCs for centralization of requests have created their own templates which must be used by officers from other units who want to create and submit a request for data disclosure to OSPs. Such templates must be submitted to the SPoC, which will then process and create the request to the OSPs. In some countries, SPoCs deal only with a limited number of OSPs, with which they have already established contacts and have a clear understanding of their process. In these countries, other OSPs may be approached by officers without the need to involve the SPoC.

SPoCs for knowledge-sharing and support



Some authorities may have opted for SPoCs whose main task is to support and advise authorities in the process to obtain cross-border access to electronic data. These SPoCs are not necessarily involved in the preparation or submission of requests and they are not centralizing the flow of information. Instead, they act as a Centre of Reference, both to OSPs and to other officials and have the role to keep up-to-date contact details of OSPs and relevant information about their processes for data-disclosure requests in order to support investigators, officers and judicial authorities who must request data from OSPs. These SPoCs play an important role in the effectiveness of the dissemination of relevant information to EU

authorities in relation to electronic evidence.

SPoCs for knowledge-sharing and support perform tasks that may include:

- Provide information and advice to national authorities in all OSP-related matters, acting as a national centre of reference;
- Engage with representatives from relevant OSPs to discuss issues in the process for data disclosure requests;
- Keep up-to-date information in relation to OSPs contact details, policies, best practices and requirements;
- Disseminate to competent authorities relevant information, including OSPs' processes and contact details;
- Provide trainings to other units or governmental institutions.

The process for establishment of SPoCs for knowledge-sharing and support varies. It is crucial that these units have clear channels of communication with other investigators and officials and continuously perform outreach activities to OSPs. For SPoCs to become the centre of reference in cross-border access to electronic evidence, they must be able to provide up-to-date information, including regarding OSPs procedures, applicable legislation and correct contact details, as well as disseminate relevant information to other units.

B. Benefits and Challenges of SPoCs

The establishment of SPoCs both for the centralization of requests and for knowledge-sharing and support brings several benefits, which are listed below. From the perspective of public authorities, the creation of SPoCs:

- Allows them to build expertise in the field, enhancing the quality of requests for voluntary cooperation, including the necessary information depending on each OSP's process;
- Guarantees certainty on channels and methods when engaging directly with OSPs;
- Makes the process faster and more effective, as public authorities outside of SPoCs do not have the need to keep up to date with fast evolving processes and policies of different companies;
- Facilitates the gathering of reliable statistics, which can lead to important analysis in relation to trends in the use of the internet for criminal purposes;
- Ensures requests for voluntary cooperation meet all necessary requirements taking into consideration domestic and international legislation, as well as companies' policies, improving success rates and response time;
- Facilitates the information flow between OSPs and authorities building mutual trust.

OSPs report greater efficiency in countries where SPoCs are established in relation to the overall process for data disclosure under voluntary cooperation in criminal

investigations.

From the OSPs' perspective, the creation of SPoCs:

- Facilitates the authentication of authorities, ensuring requests originate from authorized officials and that data is only disclosed to them;
- Decreases the processing time, as the quality of requests is potentially higher. This is due to the fact that specialized officers tend to be more familiar with the type of data that may be requested in each situation, which is the correct channel for submission, which valid identifiers are necessary and other requirements.

Although there are many benefits, SPoCs in EU countries also report some challenges faced both in their conception, establishment or run-up phases. SPoCs are at the service of the different public authorities in their respective Member States and can acquire different shapes according to, for example, the overall national organisation of law enforcement and judiciary competent authorities, hierarchical and working relationships and procedures. The issues described are mainly related to the allocation of human resources and providing proper trainings to staff. Besides, it may also be a challenge to educate other authorities in their own organisation or country on how to use SPoCs, which type of data to provide and to know what to expect from OSPs. In certain countries, the establishment of the SPoC is followed by an exponential growth in demand for their service and expertise, which is not always accompanied by reinforcement in staff at the needed pace, leading to backlogs.

C. SPoC Case Studies

Germany

The creation of SPoCs was driven by the need to improve success rates of requests to OSPs. As a federalized State, Germany has many law enforcement agencies. The country has opted for the creation of different SPoCs, and one of them is for knowledge sharing and support and general questions, the others are SPoCs at agency level for the centralization of requests. The SPoCs at agency level focus on different crime areas, such as counter-terrorism, left-wing and right-wing extremism or serious and organized crime.

In the past, it was challenging to identify which should be the best unit for being a SPoC, as well as to convince investigators to channel their requests via the SPoC. At the BKA, the SPoC deals with all the foreign-based OSPs. They try to establish contacts and continuously improve cooperation with foreign-based OSPs to optimize the processes and - if necessary - to mediate in case of problems related to inquiries. It is very important for them to understand, for example, the OSPs' specific requirements and policies in relation to user notification, since a notification to a suspect could jeopardize ongoing investigations.

Finland

When the need to request data from OSPs emerged, investigators from different police departments started to request help from the International Affairs unit within the National

Bureau of Investigation (NBI), which was already dealing with requests and other matters related to foreign partners. At the beginning, there was only one person dealing with all the requests, but as the volume increased, more staff has been allocated to the unit. In the past, the Finnish SPoC found it challenging to properly train the staff dealing with requests, since there was first the need to understand and establish processes in order to gain efficiency. Today, there is no domestic legislation that requires police departments to send requests for data disclosure to OSPs via the SPoC unit within the NBI. However, even without a legal obligation, there is a growing demand for the unit to act as a national SPoC for centralization of requests, which requires constant adaptation.

Belgium

The unit responsible for fighting cybercrime has become a SPoC over time: it was not planned to have this role at the outset. Twelve years ago, this unit sent their first request to Microsoft, which responded positively and disclosed the data related to the criminal investigation. After that, local police agencies started to ask the cybercrime unit for help with this type of requests and eventually that unit took on a SPoC role more formally and became a separate unit.

It was challenging at first to understand the correct processes for voluntary cooperation of each OSP, including which channel to use and what kind of data could be requested. As a central unit to deal with requests, it was also challenging to educate the investigators who submit requests through them about the correct way to request data. To overcome this challenge, nowadays the requesting officer must fill in a template to be sent to the SPoC. The SPoC is the unit receiving the responses in a centralized manner and it processes them in certain cases, before passing them along to the investigators, so as to facilitate their work.

In Belgium, the SPoC centralizes requests for a specific number of OSPs, due to limited capacity in terms of human resources. When it comes to other OSPs which are not part of their contacts, investigators might approach the company directly following domestic legislation, without the need to involve the SPoC.

According to the Belgian SPoC, many OSPs prefer to deal with their unit instead of individual officers, since this facilitates the process from their perspective as there will not be the need to authenticate the requesters of each incoming request. By centralizing the process in a few number of SPoCs, it is easier for the OSPs to ensure the requests are legit and that the disclosure of any data is done only to authorized government officials.

Spain

Spain has SPoCs established in four different agencies: two of them nation-wide (the Policía Nacional, Guardia Civil), and two of them with a regional scope in Catalonia and Navarra (Mossos d'Esquadra and the Policía Foral de Navarra), as detailed below.

- Policía Nacional

The Spanish National Police has designated the unit called SITEL Service to operate as

a SPoC for centralization of requests, which also acts as a national centre of reference, maintains expertise and engage with OSPs to discuss issues in the process. The unit initially created in 2001, operates today with 24/7 capacity, dealing with requests to domestic and international service providers, in the context of criminal investigations. Their requests are managed through an internal platform, which is accessible by officers.

- Guardia Civil

The Telecommunications Intervention Group was created in 1999, acting as a SPoC for requests to national telecommunications providers. As OSPs began to emerge, the unit gradually acquired the functions of a SPoC. Today, the unit operates as a SPoC for centralization of requests, ensuring compliance with all applicable regulations, as well as OSPs' specific requirements.

- Mossos d'Esquadra

The SPoC unit within Mossos d'Esquadra was formally created in 2007. Today, they operate as a SPoC for centralization of requests, reviewing outgoing requests and processing incoming responses from OSPs.

- Policía Foral de Navarra

Within the Policía Foral de Navarra, the SPoC unit deals with data disclosure requests to private entities since 2000. Back then, most requests were directed to telephone providers. Today, the unit operates as a SPoC for centralization of requests, also reviewing outgoing requests and processing incoming responses from OSPs.

The Netherlands

The Dutch approach to SPoC is the result of the cooperation of different roles of both law enforcement and judiciary authorities in criminal investigations: this makes the model a hybrid between SPoCs for centralization of requests and for knowledge-sharing and support. The 'Interception and Sensing Department' (I&S) of the Dutch National Police serves as the actual SPoC for centralization of requests whereby it handles outgoing requests for foreign-based OSPs on the basis of pre-established agreements with a number of companies in relation to voluntary disclosure of non-content information. More specifically, I&S works with Dutch OSPs, foreign resellers (whenever they can access subscriber information held by Dutch OSPs or stored content data hosted in servers in The Netherlands) as well as in relation to voluntary disclosure of non-content information of those U.S.-based OSPs which are located or have servers in The Netherlands.

This is complemented by the cooperation with the authorities at the National Public Prosecutor's Office, where dedicated Prosecutors serve as point of contact for Dutch telecommunications companies, data centres and hosting providers, on top of centralising outgoing direct requests to OSPs via the Interception and Sensing Department, receiving replies, analysing and dispatching them to the concerned agencies.

In their function of SPoC for knowledge-sharing and support, Dutch authorities provide information and advice to national LEA and judiciary authorities in all OSP-

related matters acting as a centre of expertise while collaborating with policy officers within the Public Prosecutor's Office and the legislative and policy sections of the Ministry of Justice and Security. Concerning incoming requests from foreign-based authorities to OSPs based in The Netherlands, these are handled following different modalities. However, in those cases I&S also acts as SPoC for the Dutch OSPs.

RECOMMENDATIONS

A. For European Union Judicial Authorities

- *Promote national initiatives aimed at developing a clearer overview on the different available processes to request and obtain data disclosure*

While discussions on new EU legislation on electronic evidence are on the way, judicial authorities need to bridge the current gap. As the field of electronic evidence is inextricably tied to the unprecedented development of the technological landscape that surrounds all aspects of EU citizens' lives, it appears fundamental for the EU judicial community to rely on clear and shared investigative and prosecutorial solutions that match specific needs, in particular in the absence of harmonised rules at EU level. As presented in these pages, the direct feedback received often referred to the absence of legal clarity on certain topics. Therefore, in such a fast-evolving landscape and while progress at policy level, national and international, is ongoing, investing in the constant training of EU authorities fulfilling their duties would fill gaps to the extent possible for the benefit of all involved stakeholders.

- *Strengthen the interconnection and knowledge exchange among EU judicial practitioners in the field of electronic evidence*

General advancement, as common in an exponentially growing field, is brought forward initially by the concrete efforts of those working on a daily basis on a concerned topic. With regards to the field of electronic evidence, judicial cooperation and cross-border data disclosure, it is paramount to always strive to widen the reach of knowledge-exchange projects in order to serve an ever-growing community of EU competent authorities while, at the same time, benefitting from and updating the offer on the basis of the different expertise and angles from which electronic evidence can be approached.

In this, the SIRIUS restricted platform can provide concrete means to the daily efforts of EU judicial authorities as well as promote knowledge exchange with other actors in this field.

B. For European Union Law Enforcement Agencies

- *Make use of the SIRIUS platform to provide periodic training to officers dealing with cross-border requests to Online Service Providers*

Although there has been an improvement in 2019, 45.5% of law enforcement officers still report never having received training on how and when to make cross-border requests to OSPs. As electronic evidence gains importance in criminal cases, providing periodical training to officers can lead to more effective and faster investigations. This is particularly important when dealing with emergencies and time-sensitive cases.

Law enforcement officers and judicial authorities can find more information about how to register on SIRIUS at https://www.europol.europa.eu/sirius.

- *In Member States where there are not yet established, create Single Points of Contact for electronic evidence*

The digital environment is constantly evolving and changes are frequent in the way platforms are abused by criminals and in the way OSPs operate. The establishment of SPoCs for centralization of requests or for knowledge-sharing can largely contribute to enhanced capacity in dealing with electronic evidence, also leading to more effective and faster investigations. There are extensive benefits to this approach, as detailed in Chapter 8.

Established SPoCs are invited to join the restricted SIRIUS SPoC Network page, which aims at facilitating the exchange of best practices among these specialized units. For more information contact sirius@europol.europa.eu.

C. For Online Service Providers

- *Disseminate updates about policies and changes in processes to EU authorities through SIRIUS*

The SIRIUS platform is designed to securely facilitate knowledge-sharing in relation to cross-border access to electronic evidence amongst law enforcement and judicial authorities in the EU. Therefore, SIRIUS can play a key role in complementing the dissemination strategy of relevant information, leading to improved quality of request and avoiding unnecessary inquiries. Ultimately, this can contribute to faster and more effective data disclosure requests in criminal cases. OSPs may contact the SIRIUS Team at sirius@europol.europa.eu or at sirius.eurojust@eurojust.europa.eu.

- *Publish periodic transparency reports regarding requests from EU authorities, including standardised data categories*

Transparency reports are extremely important from an analytical perspective, as they give a clearer picture of cross-border access to electronic evidence, identify trends and common issues, and better inform authorities of which mistakes to avoid. Since products and services from OSPs vary widely, it is understandable that transparency reports will reflect this variety and include each company's specific information. However, in order to properly analyse the data, a minimum standardisation level is highly recommended. The SIRIUS project recommends that companies publish transparency reports in editable format (e.g. .csv) at least yearly, distinguish civil from criminal cases and include at a minimum the breakdown of data listed below. It is recommended to include the breakdown per country, for instance when it concerns direct requests from foreign-based authorities or requests from domestic authorities that identify a foreign country as the originator via MLA procedure.

- Total number of requests;
- Number of accounts concerned by requests;
- Disclosure rate of all types of requests;
- Total number of emergency requests;
- Number of accounts concerned by emergency requests;
- Disclosure rate of emergency requests;
- Total number of preservation requests.

ENDNOTES

1 SIRIUS EU Digital Evidence Situation Report 2019.

2 The number of requests received by Twitter in 2018 has been reviewed in relation to the previously published SIRIUS EU Digital Evidence Situation Report 2019. This report takes into account the new breakdown of data included in the Transparency Report published by the company in August 2020.

3 SIRIUS EU Digital Evidence Situation Report 2019, p.15.

4 Ivi, p.20.

5 Austria, Belgium, Czechia, Estonia, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

6 Available on a dedicated area on EJN's website, under the section on e-evidence. The section, available for consultation and constantly updated, was created by the EJN Working Group on e-evidence together with the EJN Secretariat and with the support of the members of the European Cybercrime Network and the National Specialised Cyber Units.

7 Austria, Belgium, Bulgaria, Czechia, Denmark, Estonia, Finland, Germany, Hungary, Italy, Latvia, Lithuania, Netherlands, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden. In the context of the Fiches Belges information regarding United Kingdom was not reported as UK was not considered a EU Member State.

8 The Commission proposed on the 17 April 2018 the e-evidence package: a Proposal for a Regulation of the European Parliament and the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD) and a Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final - 2018/0107 (COD).

9 Press release 'Council gives mandate to Commission to negotiate international agreements on e-evidence in criminal matters', 6 June 2019.

10 EU Commission's Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (SWD/2018/118 final).

11 Austria, Belgium, Czechia, Estonia, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

12 In general, textual feedbacks featuring this report were edited to ensure clarity, conceal sensitive data, or translated from different EU languages into English.

13 The role of the 24/7 Network as an effective way to request preservation of data is confirmed by the information provided in the Fiches Belges and further developed under the Section 5.4 'Fiches Belges on e-evidence: legislation and procedures in the EU Member States' of this report.

14 SIRIUS EU Digital Evidence Situation Report 2019, p. 20.

15 A complementary overview on the definition of electronic evidence and data categories at EU national level is reported under the Section 5.4 'Fiches Belges on e-evidence: legislation and procedures in the EU Member States' of this report.

16 The engagement with US authorities during the workshop dedicated to electronic evidence and cross-border data disclosure touched upon the topic of data request and meeting of the probable cause standard as laid down by US

legislation. The common practice shared suggested EU authorities to request basic subscriber infromation as the first step of an investigation in order to progress within the investigation and follow-up with additional requests for data-sets requiring higher legal standard of proof, if needed.

17 SIRIUS EU Digital Evidence Situation Report 2019, p. 20.

18 Including one mention attributed to YouTube.

19 Article 18 – Production order.

20 A comprehensive analysis of the Yahoo! Case and relative judgement is available on the 'Cybercrime Judicial Monitor' (Issue 1 June 2016, pp. 14-30).

21 Full text of The Judgement of the Court.

22 National Centre for International Legal Assistance.

23 It is worth reporting the clarification given by Portuguese respondent that replied 'No' to the question posed. It reads: "It does not prohibit the request, but the issuance of a production order, given its coercive enforcement as stated in article 14 of the Cybercrime Law (Law n.º 109/2009, 15/09) is restricted to the domestic based entities. It's worth noting that the aforementioned legal provision, in its n.º 4, applies to ISPs, rather than OSPs."

24 SIRIUS EU Digital Evidence Situation Report 2019, p. 20.

25 It is fair to mention that the issue is not completely regulated in the cybercrime law of Portugal and that due to consideration needs to be given, in practice, to the roles of Investigating Judges and the Prosecutors in the collection of digital evidence, as stated in the Criminal Procedure Code.

26 "Law no. 109/2009 (15 September) Cybercrime Law - Article 14 (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. (...)
3. (...)
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
   c. any other information about the location of communication equipment, available under a contract or service agreement.

27 "(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: (b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control".

28 Even though Sweden does not appear among the Countries signatories of the Budapest Convention on Cybercrime, it could still be possible that the Country enacted similar provisions as part of its national legal framework. This is, as a matter of fact, confirmed by the information included in the Fiches Belges, as reported in the Section 5.4 'Fiches Belges on e-evidence: legislation and procedures in the EU Member States' of this report.

29 Article 32 – Trans-border access to stored computer data with consent or where publicly available.

30 SIRIUS EU Digital Evidence Situation Report 2019, p. 21

31 Ibidem

32 The named workshop approached the topic related to challenges from a domestic, and not cross-border, perspective as the experience presented by participants related to the engagement with, respectively, US and Ireland-based OSPs.

33 SIRIUS EU Digital Evidence Situation Report 2019, p. 21.

34 Ivi, p. 22.

35 The current state of the art is also the result of the ruling of the Court of Justice of the European Union that, in 2014, overturned the Data Retention Directive (DRD). CJEU judgement: ECLI:EU:C:2014:238 (case C-293/12).

36 Comprehensive information on the case and related judgement is available on the CJEU website.

37 Furthermore, as presented in the Fiches Belges, in Italy the data retention period depends on the category of data. Pursuant to Italian legislation, telephone traffic data is retained for 24 months, unsuccessful/missed calls traffic data for 30 days and electronic communications traffic data for 12 months. For certain crimes the period may be extended up to 72 months.

38 Additional information presented in the Fiches Belges report for Spain a retention period of 12 months with the possibility either for an extension for a maximum of 24 months or to limit it to a shorter period of not less than 6 months. For such purpose, the Government will take into consideration the data storing costs and the relevance of such data for the purpose of detection, investigation and bringing to trial serious forms of criminal activities.

39 Expanding further the Austrian case, as reported in the Fiches Belges, traffic data must be deleted by the OSPs or made anonymous as soon as the payment process has been completed and the charges have not been contested in writing within a period of three months.

40 In Sweden, as presented in the Fiches Belges, location data for mobile phone calls is retained for 2 months, data on internet access for 10 months (except for data identifying the equipment where the communication is finally separated to the subscriber) and all other non-content data for 6 months.

41 Guideline 2002/58 / EG.

42 For the time being - September 2020 - data is stored only for billing purposes with the period being dependent on the OSPs' policy.

43 In relation to U.S.-based OSPs, this is regulated by 18 U.S.C. §2706.

44 EU Commission's Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (SWD/2018/118 final), p. 282.

45 The feedback coming from Austrian authorities emerged in internal discussions within the SIRIUS Platform.

46 As an example: 'Have a Search Warrant for Data? Google Wants You to Pay', The New York Times, 24 January 2020

47 A useful selection of insightful analysis on the topic of encryption comes from: the 1st and 2nd 'Joint Report Europol-Eurojust of the observatory function on encryption' as well as form the ENISA's Opinion Paper on Encryption.

48 As an example: 'Facebook Says Encrypting Messenger by Default Will Take Years', Wired, 1 October 2020.

49 As an example: 'MI5 chief asks tech firms for 'exceptional access' to encrypted messages', The Guardian, 25 February 2020.

50 The Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation

Orders for electronic evidence in criminal matters deals even with four data categories: subscriber, access, transactional and content data, see explanation in recital (21).

51 In line with the feedback contained in Table 1 under the section 5.2 'Cross-border requests and data disclosure' of this report.

52 As reported in Tables 6 and 6.1 under section 5.3 'Challenges' of this report.

53 The reference is to section 5.3 'Challenges' of this report.

54 With the exception of Sweden.

55 With the exception of Sweden.

56 The full text of the named articles and of the entire Budapest Convention on Cybercrime are available on the Council of Europe's website.

57 The list here provided is not exhaustive, as respondents indicated the possibility to use other legal instruments (EIO Directive being the most common reference) and reciprocity. EJN Fiches Belges on e-evidence provide more detailed information.

58 Article 32 of the Budapest Convention on Cybercrime was also part of the survey submitted to EU judicial authorities and presented in Table 4 under section 5.2 'Cross-border requests and data disclosure' of this report.

59 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

60 It is necessary to point out that the UN Conventions here mentioned have been ratified everywhere across the EU.

61 SIRIUS EU Digital Evidence Situation Report 2019, p.15.

62 Ivi, p.19.

63 OSPs that reported less than 100 requests were: Automattic (26 requests), Cloudflare (7), Dropbox (41), LinkedIn (83) and TikTok (64). Some of these companies adopt the policy of not responding to direct requests issued by EU authorities, which are considered to be a type of voluntary cooperation. Therefore, since a formal judicial cooperation is required, requests originating from EU Member States could have been reported as being from the country where the company is based.

64 SIRIUS EU Digital Evidence Situation Report 2019, p.21.

REFERENCES

All links were accessed in September 2020.

- Airbnb, Airbnb Law Enforcement Transparency Reports, https://www.airbnbcitizen.com/transparency
- Apple, Transparency Report, https://www.apple.com/legal/transparency/
- Automattic, Transparency Report, https://transparency.automattic.com/
- Cloudflare, Transparency Report, https://www.cloudflare.com/transparency/
- 'Council of the European Union, Council gives mandate to Commission to negotiate international agreements on e-evidence in criminal matters, https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/
- Dropbox, Transparency Overview, https://www.dropbox.com/transparency
- ENISA, Opinion Paper on Encryption, 12 Dec 2016, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption/view
- Eurojust, Cybercrime Judicial Monitor, Issue 1 June 2016, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Pages/CJM.aspx
- European Commission, Commission Staff Working Document, Impact Assessment, 17 Apr 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129550845&uri=SWD:2018:118:FIN
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN
- Europol, SIRIUS EU Digital Evidence Situation Report 2019, 20 Dec 2019, https://www.europol.europa.eu/newsroom/news/sirius-european-union-digital-evidence-situation-report-2019
- Europol-Eurojust, 1st Joint Report of encryption observatory function, 11 Jan 2019, http://www.eurojust.europa.eu/press/News/News/Pages/2019/2019-01-28_First-EP-EJ-Report-on-Encryption.aspx
- Europol-Eurojust, 2nd Joint Report of encryption observatory function, 18 Feb 2020 https://www.europol.europa.eu/publications-documents/second-report-of-observatory-function-encryption
- Facebook, Government Requests for User Data, https://transparency.facebook.com/government-data-requests
- Google, Google Transparency Report, https://transparencyreport.google.com/
- LinkedIn, Government Requests Report, https://about.linkedin.com/transparency/government-requests-report
- Microsoft, Law Enforcement Requests Report, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report
- Snap Inc., Transparency Report, https://www.snap.com/en-US/privacy/transparency/
- TikTok, Transparency Report, https://www.tiktok.com/safety/resources/transparency-report
- Twitter, Information requests, https://transparency.twitter.com/en/information-requests.html
- Verizon Media, Government Data Requests, https://www.verizonmedia.com/transparency/reports/government-data-requests.html

ACRONYMS

- EDR: Emergency Disclosure Request
- EIO: European Investigation Order
- EJN: European Judicial Network
- EU: European Union
- IP: Internet Protocol
- ISP: Internet Service Provider
- LEA: Law Enforcement Authority
- MLA: Mutual Legal Assistance
- OGP: Online Gaming Platforms
- OSP: Online Service Provider
- SPoC: Single Point of Contact
- UK: United Kingdom
- USA: United States of America