



Study on the retention of electronic communications non-content data for law enforcement purposes

Final report

Written by Milieu
September 2020



EUROPEAN COMMISSION

Directorate-General for Migration and Home Affairs
Directorate D - Law Enforcement and Security
Unit D.4 –Cybercrime

Study on the retention of electronic communications non-content data for law enforcement purposes

Final report



List of authors

Claire Dupont

Valentina Cilli

Ela Omersa

Camille Borrett

Maxime Moulac

Plixavra Vogiatzoglou

Svetla Nikova

LEGAL NOTICE

The information and views set out in this study are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

The European Commission is not liable for any consequence stemming from the reuse of this publication.

Luxembourg: Publications Office of the European Union, 2020

© European Union, 2020

The reuse policy of European Commission documents is implemented based on Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39).

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders.

PDF ISBN 978-92-76-22841-7 doi 10.2837/26288 DR-01-20-587-EN-N

ABSTRACT

This report is the result of the 'Study on the retention of electronic communications non-content data for law enforcement purposes (HOME/2016/FW/LECO/0001)' (the Study) carried out by Milieu Consulting SRL for the Commission's Directorate-General for Migration and Home Affairs, Directorate D – Law Enforcement and Security, Unit D.4 – Cybercrime. The overall objective of this Study is to collect information on the legal framework and practices for retention of and access to electronic communications non-content data (also known as metadata) in 10 selected Member States – Austria, Estonia, Germany, France, Ireland, Italy, Poland, Portugal, Slovenia and Spain. The Study investigates the regulatory framework, practices, needs and challenges of electronic communications service providers (ESPs) and law enforcement authorities (LEAs) through extensive desk research and targeted stakeholder consultation. That consultation included selected Over-the-Top service providers (OTTs) and national authorities - both national telecommunication regulatory authorities (NRAs) and national data protection supervisory authorities (DPAs).

TABLE OF CONTENTS

ABSTRACT	5
EXECUTIVE SUMMARY	14
1. INTRODUCTION	22
1.1. Study objectives and scope	22
1.2. Structure of this report	22
2. BACKGROUND AND CONTEXT OF THE STUDY	24
2.1. Legal and political context of data retention.....	24
2.2. Challenges in the current regulatory and technological context	26
3. METHODOLOGY	29
3.1. Analysis framework and key definitions.....	29
3.2. Methodological approach to the Study.....	29
3.3. Data collection	31
3.3.1. Desk research	31
3.3.2. Targeted surveys	31
3.3.3. Targeted interviews.....	36
3.4. Analysis and assessment of information	37
3.5. Challenges, limitations and mitigation measures	38
4. REGULATORY AND INSTITUTIONAL FRAMEWORK ON RETENTION OF AND ACCESS TO NON-CONTENT DATA FOR LAW ENFORCEMENT PURPOSES	39
4.1. Current regulatory framework.....	39
4.1.1. Overview of general legal framework for retention of and access to non-content data.....	39
4.1.2. Overview of institutional framework for access to non-content data.....	43
4.2. Role and function of national authorities.....	45
4.3. Key findings.....	46
5. RETENTION OF NON-CONTENT DATA	48
5.1. Types of non-content data retained	48
5.2. Concept of IP address	50
5.3. Retention periods for non-content data	52
5.4. Purposes for which non-content data are retained	55
5.5. Storage and security requirements	57
5.6. Key findings.....	59
6. ACCESS TO AND USE OF NON-CONTENT DATA BY LAW ENFORCEMENT AUTHORITIES	61
6.1. Dimensions of the issue	61
6.1.1. Statistics on the number of requests	61
6.1.2. Frequency of use of non-content data.....	64
6.1.3. Unsuccessful requests	65
6.2. Types of non-content data requests.....	67
6.2.1. Targeted versus large-scale requests.....	68
6.2.2. Types of data most frequently requested.....	68
6.3. Average age of requested non-content data.....	71
6.4. Types of crime for which LEAs can request access to non-content data	72
6.5. Benefits of the use of non-content data for investigation and prosecution.....	75

6.5.1.	Evaluation of the decisive character of non-content data	75
6.5.2.	Indirect value of non-content data.....	76
6.5.3.	Admissibility of non-content data	76
6.6.	Key findings.....	77
7.	PROCEDURE TO ACCESS NON-CONTENT DATA.....	79
7.1.	LEA procedures for requesting access to non-content data	79
7.1.1.	Ex-ante authorisations for LEAs to access non-content data.....	79
7.1.2.	Use of SPOCs.....	82
7.1.3.	Rules and procedures for LEAs to request and access authorised non-content data.....	83
7.2.	Measures for ESPs to Process requests from LEAs	85
7.2.1.	Management practices to process requests to access non-content data.....	85
7.2.2.	Vetting process.....	89
7.2.3.	Use of platforms and other tools	89
7.2.4.	Other measures.....	91
7.3.	Ex-post monitoring and control procedures.....	91
7.4.	Cross-border procedures	92
7.4.1.	Cross-border instruments available to European LEAs	92
7.4.2.	Cross-border procedures and connected challenges for ESPs.....	94
7.4.3.	Possible future developments in cross-border requests.....	94
7.5.	Quick freeze and other alternatives to data retention.....	95
7.5.1.	Data preservation (quick freeze).....	95
7.5.2.	Issues related to data preservation.....	97
7.5.3.	Other alternatives to mandatory data retention	98
7.6.	Key findings.....	99
8.	RETENTION OF AND ACCESS TO NON-CONTENT DATA FROM OTT SERVICE PROVIDERS	101
8.1.	Regulatory framework.....	101
8.1.1.	Overview of general legal framework for retention of and access to non-content data.....	101
8.1.2.	Role and function of national supervisory authorities.....	102
8.2.	Retention of non-content data by OTTs	103
8.2.1.	Purposes for which non-content data are retained and types of non-content data	103
8.2.2.	Data retention periods	104
8.2.3.	Storage and security requirements.....	104
8.3.	Access to and use of OTTs' non-content data	104
8.3.1.	Numbers of access requests to OTTs and numbers of unsuccessful requests.....	104
8.3.2.	Types of non-content data and types of crime	107
8.4.	Procedure to access OTTs' non-content data.....	108
8.4.1.	Procedure for requesting access to OTTs' non-content data and associated challenges	108
8.4.2.	Alternative procedure for requesting access to OTTs' non-content data.....	109
8.5.	Key findings.....	109

9.	LESSONS LEARNED AND FUTURE CHALLENGES	111
9.1.	Stakeholders' views and opinions	111
9.2.	Technological developments and connected challenges	113
9.2.1.	Current challenges.....	114
9.2.2.	Upcoming challenges.....	115
9.3.	Conclusion.....	118
9.3.1.	Regulatory and institutional framework and its challenges.....	118
9.3.2.	Types of non-content data	119
9.3.3.	Retention periods of data.....	120
9.3.4.	Storage of data	121
9.3.5.	Restrictions on the right to access non-content data	121
9.3.6.	Procedure to access data	122
9.3.7.	Alternatives to mandatory data retention	122
9.3.8.	Technological challenges.....	123
	REFERENCES	124
	References at EU level	124
	References at Member State level	128
	ANNEX I: ANALYSIS FRAMEWORK.....	146
	ANNEX II: KEY CONCEPTS AND DEFINITIONS	151
	ANNEX III: DETAILED ANALYSIS OF INFORMATION.....	156
	ANNEX IV: RESULTS OF THE SURVEY TO LAW ENFORCEMENT AUTHORITIES (LEAS).....	180
	ANNEX V: RESULTS OF THE SURVEY TO ELETRONIC COMMUNICATION SERVICE PROVIDERS (ESPS)	204
	ANNEX VI: SURVEY QUESTIONNAIRE TO LAW ENFORCEMENT AUTHORITIES (LEAS)	229
	ANNEX VII: SURVEY QUESTIONNAIRE TO ELETRONIC COMMUNICATION SERVICE PROVIDERS (ESPS)	245

LIST OF FIGURES

Figure 1: Methodological approach to the Study	30
Figure 2: Replies to LEA targeted survey, by EU Member State and type of LEA	32
Figure 3: Replies to LEA targeted survey, by role in criminal procedure	33
Figure 4: Replies to LEA targeted survey, by area of crime	34
Figure 5: Replies to ESP targeted survey, by EU Member State and territorial activity	35
Figure 6: Replies to ESP targeted survey, by type of electronic communication service provided	35
Figure 7: Classification differences between subscriber and traffic data	49
Figure 8: Type of non-content data retained by ESPs (in percentage of respondents)	50
Figure 9: Purpose for retaining subscriber data	55
Figure 10: Purpose for retaining identification data	56
Figure 11: Purpose for retaining traffic data (1).....	56
Figure 12: Purpose for retaining traffic data (2).....	56
Figure 13: Purpose for retaining location data	57
Figure 14: Frequency of access requests to non-content data in the course of a criminal investigation/prosecution, 2018 and 2019.....	65
Figure 15: Comparison of the frequency of access requests to non-content data in the course of a criminal investigation/prosecution, 2018 and 2019, by type of authority (police vs. public prosecutors)	65
Figure 16: Frequency of unsuccessful requests for non-content data reported by LEA survey respondents.....	67
Figure 17: Most frequent practice to request non-content data, LEA and ESPs combined.....	68
Figure 18: Share of LEAs using different type of data in over 60% of cases.....	69
Figure 19: Percentage of respondents using the type of data in at least 60% of cases, by type of crime	70
Figure 20: Percentage of requests, by type of communication in Estonia and Germany, 2018	71
Figure 21: Percentage of requests for non-content data, by age, Estonia, 2018.....	72
Figure 22: LEAs' internal procedures for requesting non-content data	83
Figure 23: LEAs' internal procedures to access non-content data received from ESPs	84
Figure 24: Key features of ESPs' management practices for access requests	85
Figure 25: ESPs' views of data retention-related costs.....	86
Figure 26: ESPs' views of data retention-related costs items	87
Figure 27: Reasons for ESPs being unable to provide the data requested.....	88
Figure 28: Practical arrangements between ESPs and LEAs	90
Figure 29: Frequency of access requests to non-content data from OTTs in the course of a criminal investigation/prosecution, 2018 and 2019	106
Figure 30: Success rate of requests sent to individual OTTs, January-June 2019	107
Figure 31: Stakeholders' assessments of the national schemes for data retention...	111

Figure 32: Stakeholders' assessments of cross-border procedures and systems for data retention	113
Figure 33: Ranking of technological challenges, LEAs and ESPs combined.....	114
Figure 34: Likely impact of new technological trends (such as 5G or IoT) on access to non-content data	116
Figure 35: In how many cases on average do you use this type of data? Respondents who answered in at least 60% of cases – by type of Member State	164
Figure 36: Number of requests sent to OTTs per 100 000 population in 2018 and in Jan-June 2019	174
Figure 37: Number of requests sent to OTTs vs number of accounts specified in Jan-June 2019.....	174
Figure 38: Successful vs total requests sent to OTTs between January and June 2019 in absolute numbers.....	175
Figure 39: Success rate of requests sent to OTTs between January and June 2019 in percentages	175
Figure 40: Successful vs total requests sent OTTs between January and June 2019 per 100,000 population	176
Figure 41: Successful vs total requests sent to individual OTTs between January and June 2019.....	176
Figure 42: Reasons for rejecting requests sent to Microsoft between January and June 2019	177

LIST OF TABLES

Table 1: Interviews conducted during the Study – EU level	36
Table 2: Interviews conducted during the Study – Member State level	36
Table 3: Overview of the current legal framework.....	39
Table 4: Overview of data retention periods, by type of purpose.....	52
Table 5: Overview of security requirements for the storage of data.....	57
Table 6: Overview of statistics available on non-content data requests.....	61
Table 7: Summary of the types of crimes for which non-content data can be requested, based on national legislative frameworks	73
Table 8: Overview of national authorities' competences in retention of non-content data by OTTs.....	102
Table 9: Total number of requests sent to OTTs, 2018 and January-June 2019.....	105
Table 10: Analysis framework for the Study	146
Table 11: Types of electronic communications non-content data.....	152
Table 12: Mapping of OTT services in scope	154
Table 13: Typology of relevant serious crimes	155
Table 14: Authorities authorised to access non-content data for law enforcement purposes based the national legislative frameworks	156
Table 15: Overview of competences of national authorities regarding retention of non-content data.....	160
Table 16: Subscriber data retained per Member State	163

Table 17: Identification data retained per Member State	163
Table 18: Traffic data retained per Member State	163
Table 19: Location data retained by Member State	164
Table 20: Types of crimes for which LEAs can access non-content data based on the national legislative frameworks.....	165
Table 21: Ex-ante authorisations required to access non-content data	168
Table 22: Ex-post supervision of access to non-content data by LEAs.....	173
Table 23: Comparing the state of play at the ESPs/OTTs and the needs of LEAs as to the types of non-content data	178
Table 24: Comparing the state of play at the ESPs/OTTs and the needs of LEAs as to the retention periods.....	179

LIST OF BOXES

Box 1: Legal uncertainty about the application of the current framework.....	41
Box 2: Fragmented institutional framework can result in legal uncertainty on the circumstances for access to non-content data.....	44
Box 3: Coordination initiatives in Slovenia	54
Box 4: Lengthy ex-ante authorisation procedures can prevent access to non-content data	81
Box 5: Functioning of the SPOC in France	82
Box 6: Shortcomings of quick freeze mechanism	97

ABBREVIATIONS

Acronyms and Abbreviations	Meaning
AG	Advocate General
AT	Austria
BEREC	Body of European Regulators for Electronic Communications
Budapest Convention	Council of Europe 2001 Convention on Cybercrime
B2B	Business-to-business
B2C	Business-to consumers
CG NAT	Carrier Grade NAT
CJEU	Court of Justice of the European Union
DE	Germany
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DG HOME	Directorate-General for Migration and Home Affairs
DPA(s)	Data Protection Authority(-ies)
DRD	Data Retention Directive
EC	European Commission
ECA	Estonian Electronic Communications Act
ECTA	European Competitive Telecommunications Association
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EE	Estonia
EECC	European Electronic Communications Code
EIO	European Investigation Order
ES	Spain
ECS(s)	Electronic communications service(s)
ESMA	European Securities and Markets Authorities
ESP(s)	Electronic communications service provider(s)
ETNO	European Telecommunications Network Operators' Association
EU	European Union
EuroISPA	Pan-European association of European Internet Services Providers Associations
e-Privacy Directive	Directive on privacy and electronic communications
e-Privacy Regulation	Proposal for a Regulation on Privacy and Electronic Communications
E2EE	End-to-end encryption
FB	Facebook, Inc.
FR	France
GSMA	GSM Association
IE	Ireland
IMEI	International mobile equipment identity
IMSI	International mobile subscriber identity
IOSCO	International Organization of Securities Commissions
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP(s)	Internet Service Provider(s)
IT	Italy
LEA(s)	Law enforcement authority(-ies)

Acronyms and Abbreviations	Meaning
MAC address	Media access control address
MEC	Multi-access edge computing
MS(s)	Member State(s)
NRA(s)	National telecommunication regulatory authority(-ies)
OTT	Over-the-Top
OTTs	Over-the-Top service providers
PIN	Personal Identification Number
PL	Poland
PNIJ	French National Platform for Judiciary Interceptions
PT	Portugal
PUK	Personal Unblocking Key
ROC	Registry of Enrolled Operators - <i>Registro degli Operatori di Comunicazione</i>
SI	Slovenia
SIENA	Secure Information Exchange Network Application
SIM	Subscriber Identification Module
SMS	Short Message Service
SPOCs	Single Points of Contact
TKG	German Telecommunications Act
VoIP	Voiceover IP
2000 Convention	EU Convention of 29 May 2000 on Mutual Assistance in Criminal Matters

EXECUTIVE SUMMARY

Background and context

Since the early 2000s, EU Member States have introduced compulsory retention schemes for electronic communications non-content data (non-content data, or data) as an important law enforcement tool for the investigation and prosecution of crimes. Mandatory data retention was harmonised in the EU in 2006 through Directive 2006/24/EC (Data Retention Directive, or DRD). After the invalidation of the DRD in 2014 by the Court of Justice of the European Union (CJEU), Article 15(1) of Directive 2002/58/EC (the e-Privacy Directive) provided the legal basis for data retention for law enforcement purposes. In this context, Member States either maintained, repealed or amended their national laws. A number of requests for preliminary rulings brought by national courts before the CJEU concerning these laws are now pending.

In addition to legal constraints, technological changes in the electronic communications sector are shaping the debate on data retention. The transition to Internet Protocol (IP) technology has enabled consumers to move away from traditional to online electronic communications services. This has triggered the emergence of new services and business models, such as Over-the-Top services (OTT services¹) provided by OTT service providers (OTTs). These services include instant messaging, email web-based and voice services.

Objectives, scope and limitations of the study

The Study's **overall objective** is to **collect information on the legal framework and practices for retention of and access to electronic communications non-content data in 10 EU Member States** (Austria, Estonia, France, Germany, Ireland, Italy, Poland, Portugal, Slovenia and Spain). It investigates the regulatory framework, practices, needs and challenges for electronic communications service providers (ESPs) and law enforcement authorities (LEAs). This Study was commissioned by the European Commission in response to a request of the Council of the European Union.

The scope of this Study does not address matters relating to the impact of national data retention rules on fundamental rights. The Study is limited to the factual collection and presentation of quantitative and qualitative information about the retention and access practices of ESPs and LEAs and whether these contribute effectively to preventing, investigating and prosecuting criminal offences.

Although the Study primarily covers a **period of 18 months**, from 1 January 2018 to 31 August 2019, it takes into account more recent data, where available.

The Study relied on **in-depth desk research at both EU and national level, online targeted surveys of LEAs and ESPs** active in the 10 EU Member States covered by the Study, and **interviews with EU-level representative organisations of ESPs and EU agencies (Europol, Eurojust), national stakeholders (LEAs, ESPs)** that replied to the online survey, **national telecommunications regulatory authorities (NRAs) and data protection authorities (DPAs), and selected OTTs**. Overall, the Study considered 34 valid (i.e. complete) replies to the LEA survey, and 13 valid replies to the ESP survey, from all 10 EU Member States covered. In addition, it included inputs from 47 interviews with the stakeholders listed above. Information collected through these channels was analysed and developed to reply to the key research questions of the Study.

The Study presents some **limitations**:

- It was not intended to analyse large-scale datasets but, rather, to collect limited representative qualitative and quantitative evidence on the practices and needs

¹ The term OTT refers to delivery of content or services over another platform that is 'Over-the-Top' of an ESP infrastructure. OTT services encompass any service available on the internet, such as video, audio, messaging or voice services.

of LEAs and ESPs. Therefore, the **sample of replies is not statistically representative** of all LEAs and ESPs in the 10 Member States. This is due to the limited response rate from stakeholders, as well as the Study's design.

- **Data gaps**, due to the reluctance (or inability) of stakeholders to share information on data retention, and the limited comparability of the data collected, given the differences in national definitions and practices.

The Study faced a number of **challenges**, such as the outbreak of the COVID-19 pandemic, which led to delays in the data collection tasks and thus to the analysis of the evidence collected. Additionally, the sensitivity of the topic of data retention affected the consultation process, as many stakeholders (LEAs, ESPs, OTTs) declined the invitation to participate, despite the guarantee of confidentiality and protection of the information provided.

Regulatory and institutional framework for data retention

The **regulatory and institutional framework for data retention in the 10 Member States included in the Study is fragmented**. Three of the 10 Member States currently have no legal obligation for ESPs to retain non-content data for law enforcement purposes (*de jure* Austria and Slovenia and *de facto* Germany, as its national data retention framework is not enforced). Seven Member States still – broadly – apply the national legislation transposing the DRD (Estonia, France, Ireland, Italy, Poland, Portugal, Spain). In three Member States with no mandatory data retention schemes (Austria, Germany, Slovenia), LEAs rely on the non-content data kept by the ESPs for their own commercial or business purposes.

Few alternatives exist to mandatory data retention. The main alternative solution available to LEAs is a request for the preservation of data, also known as '**quick freeze**', generally ordered by the police or Prosecutor's Office and requiring a judicial authorisation to obtain the data. However, only six Member States covered under the Study have expanded the data preservation mechanism beyond the range of cybercrime offences defined by the Budapest Convention on Cybercrime. As quick freeze concerns past data that is currently stored by the ESP, its success often depends on whether non-content data are even retained by the ESPs. Stakeholder consultations revealed that the usage of data preservation mechanisms is not considered a suitable alternative to general and mandatory data retention.

Seven Member States (Estonia, France, Germany, Ireland, Italy, Portugal, Slovenia) have ongoing legal or political proceedings regarding their data retention frameworks, and four of the 10 (Estonia, France, Germany, Ireland)² have pending requests for preliminary rulings before the CJEU. Such **legal uncertainty regarding the legal framework** on retention of and access to data is a primary challenge for both LEAs and ESPs in almost all Member States. Even if national laws on data retention are still valid, fears of convictions being overturned due to the inadmissibility of non-content data in criminal proceedings may prevent LEAs from requesting access to non-content data retained for law enforcement purposes.

In the majority of the Member States, the national legislative frameworks allow **access to non-content data by police authorities** (including military police, in some cases) **and judicial authorities** (public prosecutors and judges), as well as by the **intelligence agencies**. Many Member States, however, have also expanded the right to access retained non-content data to other types of national authorities, most commonly tax, customs or competition authorities. Although such authorities are not considered LEAs per se, non-content data can only be requested for law enforcement purposes, e.g. investigation of criminal offences that fall under the remit of the authority.

² Requests for preliminary rulings before the CJEU have also been filed by the courts in Belgium, which is not covered under this Study, and the UK, which is no longer an EU Member State.

In the 10 Member States covered by the Study, **competences with respect to oversight of data retention rules are shared** between NRAs and DPAs. Although this overlap of powers could potentially raise issues, the stakeholders noted no major problems. While DPAs are primarily responsible for ensuring that personal data are processed in accordance with the relevant rules and safeguards, NRAs are responsible for the oversight of ESPs' obligations under national data retention laws. This is logically the case for countries where national data retention rules are still in force. The situation is different in Portugal, where competences to oversee ESPs' data retention obligations are enshrined in the DPA remit, including inspection, supervision and imposition of sanctions.

Main findings on retention practices of non-content data

Overall, **the types of data** included under the data retention obligation are broadly the same across Member States with data retention laws. In addition, all ESPs consulted retain all types of non-content data for at least one internal purpose (e.g. business, commercial, invoicing, marketing, network security). However, national frameworks differ with regard to **the classification of non-content data and the retention period** of data for law enforcement and business and commercial purposes.

Based on the analysis of national frameworks, **non-content data can be classified into three groups: subscriber, traffic and location data**. This classification of data is important as, in some Member States, the conditions for accessing the data vary depending on the type of data requested. There is a broad consensus about the data points included within these three groups from one Member State to another, with the exception of certain specific data points – IP address, port number for dynamic IP addresses and subscriber identification module (SIM) and device identification numbers (e.g. international mobile subscriber identity (IMSI) or international mobile equipment identity (IMEI)). Some Member States consider these subscriber data, while others treat them as traffic data. For clarity, these data points are referred to as **identification data** within the Study.

The mandatory **data retention period** for law enforcement purposes is 12 months, except in Ireland (12 months for internet data, 24 months for telephone data) and Italy (*de facto* 72 months). Retention periods for data retained for business purposes are unclear, however. Some Member States (Germany, Italy, Portugal) set a maximum retention period of six months for business data, while others use one year (France). Within these limits, the periods vary from one operator to another, depending on their regulatory requirements and internal needs. Data retained for invoicing purposes generally have clearer and longer retention periods, due to legal thresholds for invoice contestation (on average three months). This means that for LEAs, the most reliable non-content data available within the internal databases of ESPs are those retained for invoicing purposes. Subscriber data are usually retained throughout the timeframe of the contract between clients and ESPs (as they are necessary for the subscription). This means that, in practice, subscriber data are often retained for several years. Most of the ESPs consulted retained traffic data for invoicing purposes. Identification and location data have limited business value and are retained for much shorter periods of time – in Germany, for example, they are deleted within seven days.

IP addresses, particularly **dynamic IP addresses** assigned to multiple users at the time through Carrier Grade (CG) NAT³, stand out as the **most challenging type of data for LEAs to obtain**. Port numbers are not retained in Estonia, Germany or Ireland, for example. Even when port numbers are retained, LEAs need very precise time stamps for ESPs to identify the user behind a connection.

³ CG NAT was adopted to ease the transition from IPv4 to IPv6. It is a collection of strategies for sharing addresses among a large pool of internet consumers and was necessary due to the lack of IPv4 addresses. A port number differentiates user connections linked to the shared IP address. ESPs need this port number along with precise time stamps in order to keep track of the subscriber to whom the IP address was assigned at a given moment in time. As such, if an LEA requests access to the information enabling the identification of the user behind a dynamic IP address, the port number and time stamp are necessary.

Security requirements for the storage of data are broadly the same across Member States, as they relate to requirements stipulated in the General Data Protection Regulation (GDPR) and remain technologically neutral. Some Member States (Germany, Italy, Portugal) require data retained for law enforcement purposes to be stored separately from data stored for business purposes. Other Member States (Estonia, Germany) also impose data localisation requirements. In Estonia, data must be retained in the EU, while in Germany, the data must be stored on the national territory.

Main findings on access to non-content data

In the absence of general reporting or transparency obligations for Member States or ESPs, **publicly available statistics on the number of requests for non-content data disclosures are very limited** and **stakeholders are reluctant** to share data, given the sensitivity of the issue (this is true even in cases where the publication of such data is not prohibited by law, e.g. Poland). It is therefore difficult to obtain a clear view on the frequency of requests for non-content data. Where statistics are available, there are a variety of methodologies used to record and count requests, making cross-country comparisons meaningless.

LEA survey responses suggest that **non-content data is requested frequently across the Member States**: over 50% of respondents stated that they have requested data in at least 60% of investigations over the last two years. Requests are most commonly targeted at a specific individual or device. Large-scale requests, linked to a cell tower for example, are rare and usually limited to urgent situations.

Requests from LEAs include all types of non-content data. The most frequent data points requested are telephone number, physical address, date and time of the communication and location of the equipment or line at start of communication. Generally, multiple data points are requested within the course of a single investigation, e.g. call records of a suspect that contain dates, times and location of communications, as well as the numbers called. Certain types of data are more frequently requested for certain types of crimes. For example, IP addresses are requested much more frequently for the investigation of online fraud, cybercrime, child sexual exploitation and other cyber-enabled crimes.

Requests for non-content data are rarely unsuccessful. The majority of both LEA and ESP respondents stated that requests are unsuccessful in less than 20% of cases. The most common reason is that non-content data is no longer retained. Portugal is an exception, where unsuccessful request rates are quite high due to differences in interpretation of the law between ESPs and LEAs.

It is difficult to obtain a consolidated picture of the average age of data requested due to the lack of statistics. Government statistics in both Estonia and Germany show that the majority of data requested are less than six months old. The type of crime investigated, however, plays a major role in the average age of the data needed. While some crimes are uncovered by victims within 24 hours, others - notably those committed via electronic means - may not be immediately visible and thus require older non-content data for effective and thorough investigation.

The legislation of **some Member States restricts access to data to cases involving certain types of crimes, either listed in the legislation (Germany, Portugal, Slovenia) or to the most serious crimes, based on the custodial sentence (Ireland, Spain)**. In other Member States (Estonia, France, Italy, Poland), non-content data can be requested in the context of any type of crime. However, stakeholders note that, in practice, non-content data are only requested when absolutely necessary, taking into account the severity of the crime and the availability of alternative evidence.

The extent to which **non-content data are decisive pieces of evidence in an investigation or prosecution varies according to the type of crime and type of LEA**. Non-content data are, for example, of particular importance in the investigation and prosecution of cybercrime, child sexual exploitation, and child pornography. For

these types of crime, non-content data are often the primary means of detecting the crime and act as key pieces of evidence.

Non-content data can also be valuable for investigations and prosecutions even where they are not used as primary evidence. For example, they can play an important role at the beginning of an investigation to help to obtain new evidence or identify additional victims and perpetrators. They can also be an important means of corroborating or invalidating other types of evidence relating to the facts of the case.

Main findings on the procedure to access non-content data

All Member States, apart from Ireland and Poland, **have some form of mandatory ex-ante authorisation** for LEAs to access non-content data. This is typically a judicial authorisation or an order by the Public Prosecutor (France, Italy). There are exceptions to this general requirement, based on:

- the type of non-content data (ex-ante requests are not necessary for subscriber data in Austria, Estonia, Germany, Spain);
- the type of offence investigated (Estonia). In Estonia, in case of misdemeanours, LEAs (except judicial authorities) always require judicial authorisation. For criminal offences, the authorisation from the Prosecutor's Office is required in pre-court procedures and judicial authorisation is required during court proceedings;
- the type of LEA making the request (Austria, Portugal). In Austria, criminal police authorities can access subscriber data with no ex-ante authorisation, but need authorisation from the Public Prosecutor to access traffic and location data, while security police authorities (*Sicherheitspolizei*) can access all types of non-content data without ex-ante authorisation.

ESPs process requests to access non-content data following different steps, which include the verification of the request, the extraction of the non-content data and their transfer to LEAs using secure protocols, IT platforms or pre-developed forms. In general, the requests from LEAs are managed internally by the ESP (often by a dedicated department) and necessitated the development of IT systems to store, extract and transmit the data.

Most of the ESPs interviewed carry out controls on the requests they receive from LEAs, which include a verification/vetting of the source, as well as a verification of the request itself, with varying degrees of automation.

ESPs have invested heavily in the development of IT platforms and process automation so as to reply to LEAs request efficiently. However, **the use of Single Points of Contact (SPOCs) by LEAs is not very widespread**. Among the Member States covered by the Study, France has recently implemented a SPOC (PNJI), which conveys the large majority of LEA requests to access non-content data.

ESPs would welcome increased standardisation of procedures and use of SPOCs from LEAs, which would increase the efficiency of the entire process and be cost-effective in the medium to long-term. Reimbursement schemes for ESPs, totally or partially covering the costs related to their data retention obligations, are not widespread and, where available, only partially cover the providers' costs.

Access procedures are particularly challenging in cross-border investigations. Several channels exist for cross-border exchange of non-content data in the EU, with the European Investigation Order (EIO) and Europol channels most widely used. Cross-border procedures raise challenges for LEAs, ESPs and OTTs. LEAs criticise the lack of harmonised rules, the excessive length of time to obtain non-content data and lack of knowledge of other Member States' regulations and practices. ESPs and OTTs offering cross-border services experience challenges related to different security requirements across the EU in the case of centralised storage of information (e.g. data localisation requirements) and different retention regimes.

Main findings on data retention by OTTs

The procedures described above for ESPs can be applied to some extent to OTTs, even in the absence of EU or national legal frameworks imposing a general data retention obligation for law enforcement purposes on OTTs. In response to a request for access, OTTs are able to provide LEAs with a number of non-content data, which they keep for their own business or commercial purposes.

Although OTTs do not have any obligation to report the number of access requests, they often do so in their **transparency reports**. In general, OTTs publish statistics on a six-monthly basis. Most of the requests come from Germany and France (in both absolute figures and in relation to their total population). Nevertheless, certain Member States (Portugal, Estonia) send a relatively high number of requests in relation to their total population. OTTs receive substantially fewer access requests than ESPs, with the exception of Germany.

OTTs have similar **rejection rates for requests** as ESPs and their reasons for rejection are alike. In most cases, the data requested was not found (e.g. data was never retained or was retained but the retention period has elapsed).

In terms of their procedures, like ESPs, OTTs have put in place **internal and centralised processes** for receiving, tracking, processing and responding to requests from LEAs. Such processes are described in their guidelines and actively promoted at training offered to LEA officers. An internal vetting system is used to check whether the requests to access non-content data are valid, i.e. from a legitimate source and with a legitimate legal basis. This vetting system is the most complex and labour-intensive part of the procedure to access non-content data. OTTs would welcome the use of SPOCs, whose requests have already been vetted and are thus automatically legitimate.

Main technological challenges

When asked about the most relevant issues for data retention for law enforcement purposes in the present and immediate future, stakeholders pointed to **end-to-end encryption (E2EE) and the use of dynamic IP addresses**, followed by the deployment of 5G and other related technology applications, such as Big Data, the Internet of Things (IoT) and blockchain. This increasing shift of communications from traditional telecommunication services to OTT services, which are often subject to E2EE, poses particular challenges for LEAs and heightens the importance of access to non-content data. The lack of skilled IT experts was frequently raised by LEAs.

An immediate consequence of the **introduction of 5G**, acknowledged by all stakeholders – and linking OTTs and NRAs - is **the large increase in information** potentially relevant for LEAs, with associated cost and infrastructure implications. 5G will likely use **encrypted interfaces and protocols**, meaning that non-content data normally available (especially identification data) would not be available to LEAs. In addition, due to the fragmented and virtual architecture of 5G, network and service providers may not have a complete copy of the information available, unless obliged to do so. This would present additional challenges for cross-border cooperation and procedures, in particular.

Challenges related to IoT services often stem from larger amounts of non-content data available and **the cross-border nature of such services** (e.g. the large volume of data generated by SIM cards in cars, which will be collected through several countries, as cars are likely to roam between Member States while the services related to the SIM cards are likely to be provided via one centralised platform). While ESPs struggle to assign data retention rules to their IoT services across different jurisdictions, LEAs experience difficulties in obtaining information through cross-border mechanisms. LEAs requesting data cross-border (usually via EIOs) are faced with longer waiting times for access, uncertainty about the availability of such data in another country (different national frameworks may have shorter retention periods or may not retain certain data points at all) and concerns about the legitimacy of such requests in another country.

Key conclusions

- In the absence of legal certainty of national legal frameworks on data retention, there is a risk that **LEAs cannot access important evidence needed to investigate and prosecute crimes**. Existing differences in national laws seem to raise issues for cross-border cases, where LEAs face different procedures and retention periods between countries.
- **Unclear and insufficient retention periods in the case of storage of data for commercial purposes**. This is particularly problematic in countries that do not have a legal obligation for ESPs to retain non-content data (Austria, Germany, Slovenia), as LEAs cannot know with certainty what non-content data will be available and for how long. On average, traffic, identification, and location data are retained for three months. These retention periods might not be sufficient for investigation of crimes with an online dimension (e.g. child sexual exploitation, child pornography, cyberattacks) or complex organised crime, which are often detected much later. As a result, some crimes committed via electronic means - particularly in Member States with no mandatory data retention - are not prosecuted and some crimes may not be detected at all.
- The categorisation of different types of data (subscriber, traffic and location data) is similar across Member States for many data points, which facilitates LEAs and ESPs in handling requests to access data. However, the classification of data points such as SIM and device identification numbers (e.g. IMSI, IMEI), IP address, and port number for dynamic IP addresses is more uncertain. **This ambiguity impacts the availability of these data points, especially dynamic IP addresses, which are the most challenging type of data for LEAs to obtain.**
- The classification or definition of data in some Member States affects the requirements for their access. For instance, requests to access subscriber data do not require ex-ante authorisation.
- In practice, **data are generally requested only for serious crimes** or where absolutely necessary, even in Member States where the legislation does not restrict access to data to certain types of crimes or to crimes with a minimum criminal sentence.
- **Oversight of retention of and access to data** is typically shared between the NRAs and DPAs. However, the scope of their respective competence over the OTTs is not always clear.
- Where ESPs and LEAs have developed **automated procedures and processes, such as IT platforms and SPOCs, these serve to facilitate secure access to data**. Several stakeholders would welcome further standardisation of procedures and use of SPOCs. **Ex-ante authorisations** are a commonly used safeguard against abuse of the system.
- **Access procedures are particularly challenging in cross-border investigations**. Differences in national data retention regimes, types of data and retention periods, and lack of knowledge of practices in other Member States are the main obstacles to investigation and prosecution of cross-border crime.
- **Quick freeze is often the only alternative** to data retention. However, it cannot fully replace data retention as it can only be applied from the moment a crime is detected or suspected and relies on data actually being stored by ESPs.
- **Certain providers of communication services are excluded from general data retention obligations**. OTTs are exempt from data retention obligations, despite the increasing share of communication passing through their services. The situation will likely change from 21 December 2020, when the e-Privacy Directive will be extended to OTTs. The extent to which Member States would have to enact this requirement in their legislation remains unclear, however.

- **Absence of common definitions, reporting obligations/practices and publicly available statistics** make it very difficult to understand the dimensions of the issue and to compare the (very limited) evidence across Member States. In addition, statistics from operators (both ESPs and OTTs) are not comparable, complicating the identification of trends across Member States and/or communications providers. The lack of comprehensive information, together with the limited response rate among stakeholders, limits the results of this Study and does not allow for a thorough assessment of the benefits and constraints of data retention.
- Existing technological challenges such as the retention of dynamic IP addresses remain unsolved, while **upcoming technological developments (such as 5G and IoT) will likely complicate some of the existing issues** for non-content data retention. For example, 5G is expected to increase the share of E2EE communication, which in turn is likely to reduce the volume of non-content data available to LEAs via data retention schemes (ESPs would no longer process – or retain – such data). 5G will also bring about new challenges, as its service-based architecture will make it harder for ESPs to provide certain types of data that are currently retained, such as IMSI numbers.
- Cross-border provision of communication services is expected to increase further with the implementation of 5G-enabled IoT applications. It will likely **broaden the need for cross-border investigations and LEA cooperation**, for which current procedures are not suitable. Upcoming technological challenges might raise further concerns and prompt the need for an EU-wide approach to the issue.

1. INTRODUCTION

This is the Final Report for the *Study on the retention of electronic communications non-content data for law enforcement purposes* (the Study).

1.1. STUDY OBJECTIVES AND SCOPE

The Study's overall objective is to collect information on the legal framework and practices for retention of and access to electronic communications non-content data (non-content data, or data) in a selected number of EU Member States. The information collected shall provide input for assessing whether and under which conditions data retention rules and practices contribute to preventing, investigating and prosecuting criminal offences.

The Study examines the national legislation and practices in respect of the following aspects:

- The identification of existing legal rules and practical arrangements on the retention of and access to non-content data by electronic communications service providers (ESPs) and law enforcement authorities (LEAs);
- Categories of data and data storage practices of ESPs and Over-the-Top communications service providers (OTT service providers, or OTTs), both for law enforcement purposes and for their own commercial and business purposes;
- Specific retention and access needs of LEAs, in particular, which non-content data they need and for which periods of time in order to prevent, investigate and prosecute criminal offences;
- Relevant technological developments (e.g. use of dynamic Internet Protocol (IP) addresses, introduction of 5G, encryption of data, Internet of Things (IoT)) and corresponding challenges for key stakeholders, as well as projected measures to address these challenges.

The scope of this Study does not address matters relating to the impact of national data retention rules on fundamental rights. The Study is limited to the factual collection and presentation of quantitative and qualitative information about the retention and access practices of ESPs and LEAs.

In terms of geographical scope, the Study covers a sample of 10 selected EU Member States - Austria, Estonia, France, Germany, Ireland, Italy, Poland, Portugal, Slovenia and Spain.

Although the Study primarily covers a period of 18 months, from 1 January 2018 to 31 August 2019, it takes into account more recent data, where available.

1.2. STRUCTURE OF THIS REPORT

This Final Report is structured as follows:

- **Section 1: Introduction.**
- **Section 2: Background and context of the Study.** This section outlines the legal and political background to data retention, as well as the challenges within the current regulatory and technological context.
- **Section 3: Methodology.** This section outlines the methodology used in the analysis, including national-level desk research, consultation strategy, data collection tools and analytical methods.
- **Section 4: Regulatory and institutional framework on retention of and access to non-content data for law enforcement purposes.** This section

summarises the current situation with respect to retention of and access to non-content data for law enforcement purposes in the 10 Member States covered by the Study.

- **Section 5: Retention of non-content data.** This section presents the categories of data retained and ESP data storage practices, including retention periods and storage and security requirements.
- **Section 6: Access and use of non-content data by LEAs.** This section presents the needs of the LEAs, specifying the types of non-content data requested and their average age, as well as the benefits of their use in preventing, investigating and prosecuting criminal offences.
- **Section 7: Procedure to access non-content data.** This section explains the procedure for requesting access to non-content data, with emphasis on cross-border procedures and other alternatives to the general data retention obligation.
- **Section 8: Retention of and access to non-content data from OTT service providers.** This section compares ESP and OTT practices for retention of and access to non-content data.
- **Section 9: Lessons learned and future challenges.** This section presents the upcoming technological developments and related challenges, together with the key findings of the Study.

In addition to the list of **references** collected during the Study, the report includes the following **annexes**:

- **Annex I** Analysis framework developed for the Study.
- **Annex II:** Key concepts and definitions relevant to the Study.
- **Annex III:** Detailed set of materials (including tables and graphs), compiling the evidence collected during the Study.
- **Annex IV:** Full results of the targeted survey of LEAs.
- **Annex V:** Full results of the targeted survey of ESPs.
- **Annex VI:** Full text of the targeted survey of LEAs.
- **Annex VII:** Full text of the targeted survey of ESPs.

2. BACKGROUND AND CONTEXT OF THE STUDY

This section describes the legal and political context of ESPs' data retention obligation for law enforcement purposes (section 2.1). It presents legislative and case-law developments at EU level and the response in the EU Member States. Lastly, it considers different challenges due to the current regulatory and technological context (section 2.2).

2.1. LEGAL AND POLITICAL CONTEXT OF DATA RETENTION

Since the development/rise of mobile telephony and the internet, individuals, including criminals, have increasingly used electronic communications networks and services to perform their daily activities and transactions. Apart from the content, such communications also generate non-content data, such as traffic and location data. Combined with data enabling the identification of the subscriber, the availability of such data is particularly important for the investigation, detection and prosecution of crimes.

Since the early 2000s, Member States have started to introduce compulsory retention schemes of electronic communications non-content data for law enforcement purposes.

Different approaches in the Member States to the legal, regulatory and technical provisions concerning the retention of non-content data resulted in the need for a harmonised approach at EU level⁴.

The Data Retention Directive (the DRD, or the Directive⁵) was adopted on 15 March 2006. The Directive introduced a general obligation to retain certain categories of non-content data for all users for the purpose of fighting serious crime, as defined by each Member State in its national law. The DRD obliged the providers of publicly available electronic communications services and/or publicly available communications networks to retain non-content data for a period of 6-24 months in order to ensure that the data are available for the investigation, detection and prosecution of serious crime. ESPs were obliged to make non-content data generated or processed by them available to LEAs on request. The DRD did not specify how data would be accessed and further used by the competent LEAs.

In 2014, the Court of Justice of the European Union (CJEU) in the *Digital Rights Ireland* case⁶ ruled that while the retention of data genuinely satisfies an objective of general interest in the fight against serious crime, the DRD did not pass the proportionality test, as the interference with fundamental rights was not limited to what was strictly necessary. Consequently, the DRD was declared invalid. The arguments put forward by the CJEU were that the DRD did not lay down clear and precise rules regarding the scope and justified limitations to the rights to privacy and personal data protection recognised by Articles 7 and 8 of the Charter of the Fundamental Rights of the EU. It also held that the DRD lacked sufficient procedural safeguards for the protection of the data.

After the invalidation of the DRD in 2014, Member States resorted to Article 15(1) of the 2002 Directive on privacy and electronic communications (the e-Privacy Directive⁷) as a legal basis for the general retention of non-content data for law enforcement purposes. Although the e-Privacy Directive was designed to offer users of electronic communications

⁴ Commission proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, COM(2005) 438 final, 21 September 2005, available at: [http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2005/0438/COM_COM\(2005\)0438_EN.pdf](http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2005/0438/COM_COM(2005)0438_EN.pdf).

⁵ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13.4.2006, pp. 54-63, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024>.

⁶ Joined cases C-293/12 and 594/12, *Digital Rights Ireland and Seitlinger and others*, 8 April 2014.

⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37-47, available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>.

services protection against risks to their personal data and privacy arising from new technology in the electronic communications sector, Article 15(1) enables Member States to introduce some exceptions to the principle of ensuring the confidentiality of communications and related non-content data. EU Member States are thus able to enact laws that require the storage of data for a range of public interest purposes, such as national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

In the 2016 ruling *Tele2 Sverige*⁸, the CJEU confirmed that EU law, in particular the e-Privacy Directive, precludes national legislation that prescribes general and indiscriminate retention of data. However, the CJEU also made clear that the e-Privacy Directive does not preclude national legislation from imposing the targeted retention of data for the purpose of fighting serious crime, provided that such retention of data is limited to what is strictly necessary.

The CJEU further construed safeguards that need to be respected when enacting national data retention laws, namely: (i) retention of non-content data should be the exception; (ii) the purpose should be restricted to fighting serious crime (so-called condition of 'seriousness of a crime'); (iii) the retention should be limited to what is strictly necessary; (iv) access to the data should be subject to prior review by a court or an independent authority; and (v) data should be retained only within the EU. The condition of 'seriousness of crime' was further specified in the C-207/16 *Ministerio Fiscal* case⁹, where the Court held that if access to certain types of retained non-content data does not represent serious interference with the fundamental rights to privacy and data protection, LEAs could access non-content data retained by the ESPs for crimes that are not serious.

A 2017 report by Privacy International 2017¹⁰ states that in most Member States, data retention regimes are still based on the annulled DRD and do not comply with subsequent CJEU case-law. The report states that national data retention regimes are often outdated and lack legal clarity, with some subject to long-lasting procedures before national Courts, exacerbating legal uncertainty.

Member States' responses to the development of CJEU jurisprudence remain diverse and can be summarised as follows:

- Member States in which the domestic law implementing the DRD remains in force;
- Member States that amended their legislation or enacted new data retention laws in line with the CJEU case-law;
- Member States whose national laws transposing the DRD were struck down and which now lack any data retention laws.

While a handful of Member States have repealed national transposing data retention laws (chiefly due to decisions of their respective Constitutional Courts), most Member States still apply the regime transposing the DRD. A few countries have set up new legal regimes to comply with the CJEU case-law.

Expert discussions have been taking place within the European Commission and the Council of the European Union (the Council), with support from the European Union Agency for Law Enforcement Cooperation (Europol) and the European Union Agency for Criminal Justice Cooperation (Eurojust), to identify the main aspects of data retention and to assist Member States in analysing the requirements of the relevant EU case-law.

In March 2017, the Council initiated a reflection process on mandatory data retention for the purpose of detection and prosecution of crime. The Conclusions of the European Council

⁸ Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson and Others*, 21 December 2016.

⁹ Case C-207/16 *Ministerio Fiscal*, 2 October 2018.

¹⁰ Privacy International (2017). National Data Retention Laws since the CJEU's *Tele-2/Watson* Judgment, September 2017.

of 23 June 2017¹¹ stress the importance of securing the availability of data in order to effectively fight serious crime, particularly terrorism. According to Europol, the requirements set by the CJEU do not reflect law enforcement reality, suggesting that rather than a system of targeted retention, which opens the door to discrimination, it is the access to retained non-content data that should be targeted instead.

The Council subsequently requested the Commission to carry out a comprehensive study into possible solutions for retaining data for law enforcement purposes, including the consideration of a future legislative initiative, and taking into account the development of national and EU case-law (Conclusions of the Council of 6 June 2019¹²). The present Study was commissioned in the context of that request.

2.2. CHALLENGES IN THE CURRENT REGULATORY AND TECHNOLOGICAL CONTEXT

The main challenge for national and EU legislators is to strike a fair balance between two opposite needs: (i) the individual's rights to privacy and data protection, and (ii) the need for law enforcement to access data for investigations and prosecutions, while taking into account the requirements of CJEU case-law.

The increased number of preliminary rulings referred by the Member States' (and UK) courts reveals the existence of profound doubts in the interpretation of the limits of Article 15 of the e-Privacy Directive. Requests for preliminary rulings before the CJEU have been filed by the courts in France¹³, Belgium¹⁴, Estonia¹⁵, Germany¹⁶ and Ireland¹⁷, as well as the UK¹⁸.

The preliminary questions coming from Belgium, France and the UK deal with the applicability of the *Tele2* requirements and Article 15 of the e-Privacy Directive in the field of national security and law enforcement, in particular whether the case-law of the CJEU should apply to instruments to safeguard national security and counter-terrorism. The recent opinions of the Advocate General (AG) on these references for preliminary rulings follow the previously established line of reasoning of the CJEU, stating that 'generalised retention' of non-content data for the security and intelligence agencies of Member States is not allowed, and that any access to such data must comply with the conditions established in the *Tele2* judgment¹⁹. The AGs recommend limited and discriminate retention (i.e. retention of specific categories of data that are absolutely essential for the effective prevention and control of crime and the safeguarding of national security for a determined period, adapted to each particular category) and limited access to that data (e.g. a prior review carried out either by a court or by an independent administrative authority). However, exceptions to such rules might be possible on an exceptional and temporary basis.

Similarly, the Estonian Supreme Court referred a question to the CJEU regarding the compatibility of their national law with Article 15 of the e-Privacy Directive. The Court asked the CJEU to clarify whether the type of non-content data and the duration of the period for

¹¹ European Council Conclusions, Brussels, 23 June 2017 (OR. En), EUCO 8/17, CO EUR 8 CONCL 3, available at: <https://www.consilium.europa.eu/media/23985/22-23-euco-final-conclusions.pdf>.

¹² European Council Conclusions, 6 June 2019, 10083/19, available at: <https://data.consilium.europa.eu/doc/document/ST-10083-2019-INIT/en/pdf>.

¹³ C-511/18 and C-512/18 *French Data Network, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs v Premier ministre, Garde des Sceaux, Ministre de la Justice*, 3 August 2018.

¹⁴ C-520/18 *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministres*, 2 August 2018.

¹⁵ C-746/18 *H.K. v. Prokuratuur*, 29 November 2018.

¹⁶ Joined cases C-793/19 and C-794/19 *SpaceNet a.o.*, 29 October 2019.

¹⁷ C-140/20 *Commissioner of the Garda Síochána and Others*, 25 March 2020.

¹⁸ C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, 31 October 2017.

¹⁹ Opinions of AG in Case C-623/17, Joined cases C-511/18 and C-512/18 and Case C-520/18, 15 January 2020.

which the access request was made are relevant in deciding the severity of the interference with fundamental rights. With reference to the *Ministerio Fiscal* judgment, the AG confirmed that the categories of data and duration of access are indeed relevant criteria in assessing the seriousness of the interference with fundamental rights²⁰.

The German preliminary ruling refers to the compatibility of the 2015 national law with Article 15 of the e-Privacy Directive. As this national law was adopted after the German Federal Constitutional Court annulled the first national law implementing the DRD, it sets more restrictive security and access rules (e.g. in terms of the period of retention).

The case-law of the CJEU has raised concerns among stakeholders as to the legal certainty of the current legislative frameworks, particularly among Member States and their LEAs, which are concerned about the impact on detection, investigation and prosecution of criminal offences, as well as judicial cooperation on cross-border cases. Legal uncertainty exists in respect of the use of non-content data as evidence in criminal prosecutions, as defence lawyers have challenged the admissibility of such data in many Member States covered under the scope of this Study²¹. ESPs also express concerns about the legal fragmentation and degree of uncertainty in the EU internal market.

In addition to the difficulties posed by diverse and to some extent unclear legal frameworks, the retention of non-content data faces challenges from current and upcoming technological changes in the telecommunications sector. The transition to IP technology has enabled consumers to move away from traditional to online telecommunication services. This has triggered the emergence of new services and business models, such as Over-the-Top services (OTT services). The term OTT refers to delivery of content or services over another platform that is 'Over-the-Top' of an ESP infrastructure. OTT services encompass any service available on the internet, such as video, audio, messaging or voice services (see Annex II for a more detailed definition).

The EU legislation on electronic communications networks and services²² has not kept pace with the evolution of OTT services. It was only on 25 May 2016 that the Commission published its Communication on Online Platforms and the Digital Single Market²³, which paved the way for simplifying EU telecommunication rules by suggesting maintaining only a limited set of communication-specific rules that would apply to all relevant and comparable services (including when provided by OTTs). On 4 December 2018, the Council of the EU formally adopted Directive 2018/1972 establishing the European Electronic Communications Code (EECC²⁴), updating the EU's rules for electronic communications services (ECSs).

The new EU electronic communications policy framework provides that the definition of ECSs should also cover OTT services²⁵. Recital 15 of the EECC explains that '*The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly substitute traditional voice telephony, text messages and electronic mail conveyance services by functionally equivalent online services such as voiceover IP, messaging services and web-based email services.*' Due to the cross-reference to the definition of electronic communications services in Article 2 of the e-Privacy Directive, the e-Privacy Directive will become applicable to certain OTT services (communication services) from 21 December 2020. This, in turn, means that the data retention obligations still in place in certain EU Member States could be extended to OTTs

²⁰ Opinion of AG in Case C-746/18, 21 January 2020.

²¹ Question on the admissibility is, for instance, raised in the recent Irish Case C-140/20 *Commissioner of the Garda Síochána and Others*, 25 March 2020.

²² In particular, the Framework Directive 2002/21/EC, the Access Directive 2002/19/EC and the e-Privacy Directive 2002/58/EC.

²³ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe, COM(2016) 288 final.

²⁴ Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

²⁵ <https://ec.europa.eu/digital-single-market/en/telecoms>.

that provide voice, instant messaging and email web-based services.

The proposed e-Privacy Regulation²⁶ maintains a similarly broad definition of ECSs, as well as the possibility to adopt data retention measures (Article 11 of the Commission proposal).

²⁶ Commission Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>.

3. METHODOLOGY

This section describes the methodology that guided the design and implementation of the Study. It presents the analysis framework (section 3.1) the overall methodological approach (section 3.2), the data collection strategy and its implementation (section 3.3), as well as the approach for the analysis and assessment of the information (section 3.4). Finally, it considers the limitations of the Study, the main challenges faced and the mitigation actions undertaken (section 3.5).

3.1. ANALYSIS FRAMEWORK AND KEY DEFINITIONS

In order to reply to the key research questions, the Study developed an analysis framework, which defines the indicators used to reply to each research question, the data collection tools and the stakeholders to be consulted for each of the research questions.

The development of the analysis framework followed an iterative process throughout the Study and was refined following desk research and scoping interviews in the inception and early data collection phases.

The final version of the analysis framework is provided in **Annex I**.

Following clarifications on the aim, purpose and scope of the Study during the inception phase, it appeared evident that various sources and stakeholders (as well as national frameworks and practices) have adopted different definitions for the key concepts of this Study. To clarify the scope of the Study, therefore, and to reduce the risk of misinterpretation by the stakeholders, the project team developed a list of the main concepts and definitions, which apply throughout the Study.

The list of **main concepts and definitions is presented in Annex II**. This includes the following concepts:

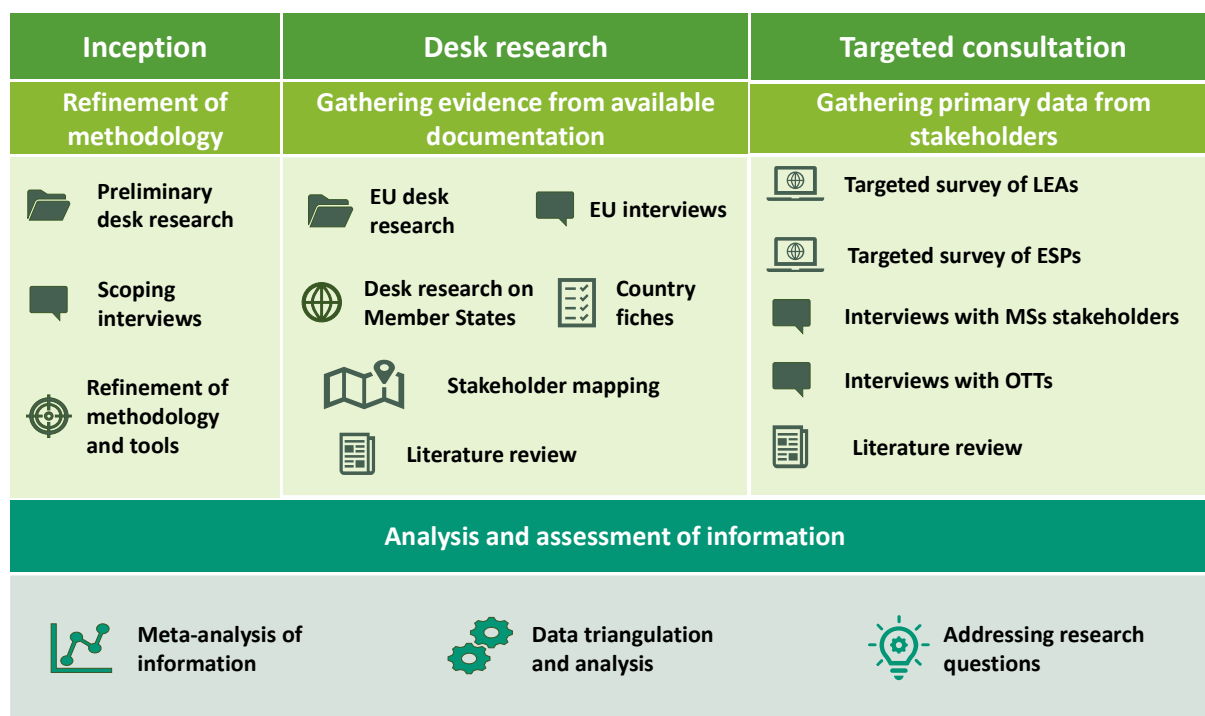
- Electronic communications non-content data;
- Electronic communications services (ECSs);
- Electronic communications service provider(s) (ESPs);
- Law enforcement authority(-ies) (LEAs);
- Law enforcement purposes;
- National security purposes;
- Over-the-Top communications services (OTT services);
- Over-the-Top services providers (OTT service providers, or OTTs);
- Serious crime.

The clarification of the concepts listed above was instrumental in the identification of the national stakeholders (especially LEAs).

3.2. METHODOLOGICAL APPROACH TO THE STUDY

The Study aimed to collect information on the legal frameworks and practices for retention of and access to non-content data in 10 selected countries (Austria, Estonia, France, Germany, Ireland, Italy, Poland, Portugal, Slovenia, Spain). The information collected provides input for assessing whether and under which conditions data retention rules and practices adequately take into account the general objectives of effectively preventing, investigating and prosecuting criminal offences.

The figure below provides an overview of the three main tasks of the Study, the tools used for data collection and the approach to analysing and assessing the information collected.

Figure 1: Methodological approach to the Study

Source: Milieu elaboration

The **inception task** aimed to better understand the context and define the scope of the Study, while refining the research questions, methodology and tools.

The **desk research task** gathered the publicly available information needed for the Study, mostly focusing on the legal framework, existing case-law and available data and statistics on the use of data retention in the 10 Member States. It included evidence from available documentation and additional sources identified during the inception task, at both EU and national level. As part of this task, **country fiches** were produced for each of the ten Member States covered by the Study. These provided detailed information on the legal framework for data retention in each case, which helped to finalise tools for primary data collection (online targeted surveys of LEAs and ESPs, interview guidelines) and for further analysis. The desk research also aimed to identify relevant stakeholders at national level (LEAs, ESPs, regulatory agencies) to be contacted for the targeted consultation task.

The **targeted consultation** complemented the data collection by gathering primary data and information from EU and Member State-level stakeholders. It included one online targeted survey of LEAs and one of ESPs, supplemented by follow-up interviews with (some of) the survey respondents. Additional interviews were conducted with national telecommunication regulatory authorities (NRAs) and data protection authorities (DPAs), as well as with selected OTTs.

The qualitative and quantitative information collected throughout the Study was analysed and assessed against available literature and discussed with thematic experts in order to validate the findings of the Study.

The following sections provide more detailed information about the data collection and analysis process, as well as on the limitations and challenges encountered by the Study.

3.3. DATA COLLECTION

Data collection was a key activity for the Study and was conducted through several channels:

- Desk research at EU and national level;
- Online targeted surveys of LEAs and ESPs active in the 10 Member States covered by the Study;
- Interviews of ESPs' representative organisations and relevant EU services (during the inception task), LEAs and ESPs that replied to the online survey, NRAs, DPAs, additional selected operators and selected OTTs.

More detailed information about each of the tools listed above is provided in the next sub-sections.

3.3.1. Desk research

Throughout the entire duration of the Study, desk research was used to collect the information relevant to the Study, primarily focusing on the legal framework, existing case-law and available data and statistics on the use of data retention in the 10 Member States covered.

Desk research at EU level, carried out by the core team, covered the legal framework, existing case-law and available data and statistics at EU and/or cross-border level, including, for instance, transparency reports from ESPs active in more than one EU Member State. It aimed to gain a better understanding of the legal framework at EU level (on data retention and other related issues, such as the general rules and exceptions set by the e-Privacy Directive and the EEC) and at national level, as well as of relevant stakeholders and their characteristics (e.g. evolution of services provided by ESPs and OTTs, and their impact on the data retention obligation).

Desk research in the Member States was conducted by national experts. This approach enabled a larger number of national sources to be analysed, as it was carried out in the national language. It followed a set of detailed research questions listed in a common template (the **country fiche**), prepared by the core team and agreed with the Commission. The country fiche allowed the core team to analyse and compare information across countries. The aim and scope of the national desk research and the structure of the country fiche were discussed with the national experts during a webinar, in order to ensure a common understanding of the task and reduce inconsistencies. The country fiche was revised and updated by the national experts during the last phases of the Study, based on the additional information gathered via interviews and other sources (e.g. reports from national authorities and/or ESPs).

The list of the EU and national sources collected and used for the Study is provided in the **References** section.

Desk research also aimed to allow a more **detailed stakeholder mapping**, identifying the organisations and (possibly) individual stakeholders to be contacted for the primary data collection (surveys and interviews). Conducted at both EU and national level, it identified the most relevant contacts among OTTs and business-to-business (B2B) ESP providers, national LEAs and ESPs, and national regulatory authorities.

3.3.2. Targeted surveys

The Study included two separate surveys, **one targeting LEAs** and the **other ESPs** active in the 10 Member States covered. The surveys aimed to collect information on the volume and type of non-content data retained, their use in investigations, prosecutions and crime detection, the implications (for technology, costs, security, etc.) of storing, requesting, accessing and analysing such data, relevant technological challenges to existing arrangements regarding retention of and access to non-content data and their implications for legal frameworks, technological solutions and costs.

The design of the surveys followed an iterative process, based on the refined understanding and approach from the inception task, as well as guidance and discussions with the Commission and the Senior Thematic Experts. Both surveys were designed in English, then translated and made available online to stakeholders in their national languages, with the choice of replying in either language. Although translating the surveys required additional time, it nevertheless facilitated stakeholders' participation by overcoming any potential language barrier. The surveys also included an introduction that clearly explained the objective and benefits of contributing to the Study, to incentivise participation.

The surveys were **distributed via email using several channels** to increase the chances of response. The **survey of LEAs** was disseminated to contacts identified via the EU and national stakeholder mapping and ad hoc communication from Europol and Eurojust. The initial list of contacts was then broadened via additional contacts provided both by Europol and Eurojust, national contact points and other relevant parties identified by the core team and national experts during the Study. The **survey of ESPs** was disseminated via email through several channels, including those identified via stakeholder mapping and provided by the representative organisations contacted during the inception task. For both surveys, the national experts carried out an intensive follow-up by email and direct calls (where possible) to increase participation and clarify specific questions.

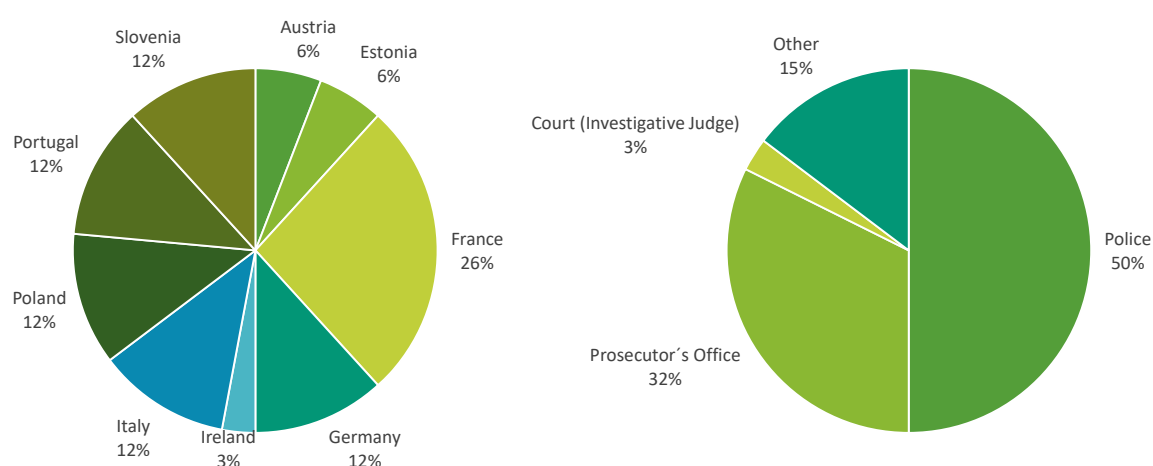
The full text of the targeted surveys is provided in **Annex VI** for LEAs and **Annex VII** for ESPs, while the full set of results are in **Annex IV** and **Annex V**, respectively. The survey targeting LEAs was published online from 1 March 2020, and the survey targeting ESPs from 11 March 2020.

The targeted surveys were not designed to have a large pool of respondents nor to collect a statistically representative sample of the entire national situation but, rather, to provide some qualitative and quantitative evidence on the needs and practices of LEAs and ESPs, ideally through statistics and concrete examples (see section 3.5 for more details).

Targeted survey of LEAs: respondents' profile

Overall, the targeted survey of LEAs had 34 valid (complete) replies, from all 10 Member States covered.

Figure 2: Replies to LEA targeted survey, by EU Member State and type of LEA



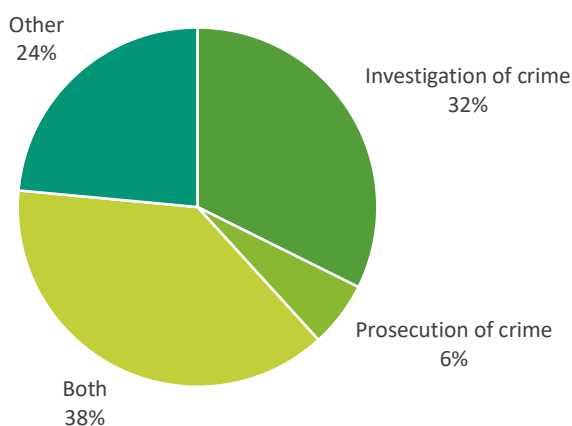
Source: Targeted survey of LEAs, Questions 1 and 5 (N=34)

Overall, while all LEAs in all Member States provided at least one reply, France is over-represented (26% of replies). Half of the respondents (50%) came from police bodies, about one-third (32%) from the Prosecutors' Office, and only one from a court investigative

judge. The remaining 15% came from other LEAs, including Ministry for Justice, tax and customs authorities and other central administrative authorities.

Most of the replies were from national/federal LEAs (65%), while only some (21%) were from regional LEAs and 15% from local LEAs.

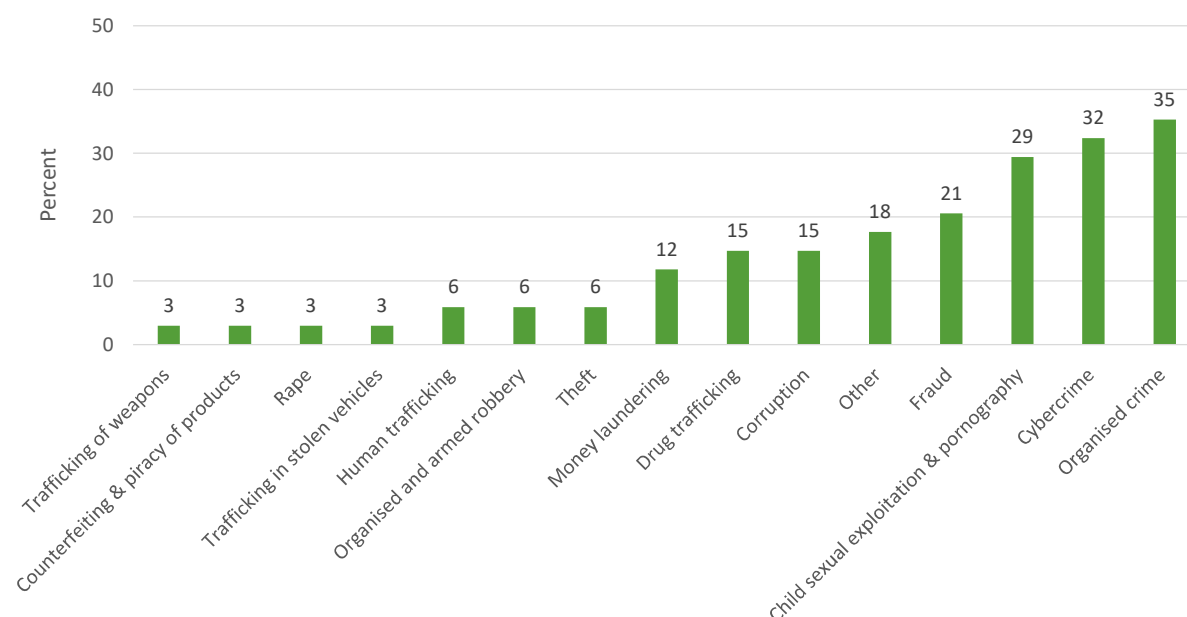
Figure 3: Replies to LEA targeted survey, by role in criminal procedure



Source: Targeted survey of LEAs, Question 4 (N=34)

About 32% of respondents work in LEAs involved in the investigation of crime and a small share in prosecution (6%), while the relative majority (38%) belong to authorities involved in both investigation and prosecution. The remaining respondents (24%) came from organisations supporting and coordinating LEAs and/or the actions of the State in matters of judicial interception of electronic communications, such as digital forensic investigators, and the Ministry of Justice.

Many of the respondents' organisations (80%) are **specialised in the investigation and/or prosecution of specific crimes**, with organised crime, cybercrime and child sexual exploitation and child pornography being the most frequent (35%, 32% and 29% of respondents, respectively). The category of 'other crimes', which ranked fifth, includes mostly financial crimes, such as corporate market abuse, bankruptcy and tax offences, or misappropriation of public funds.

Figure 4: Replies to LEA targeted survey, by area of crime

Source: Targeted survey of LEAs, Question 11 (N=34, multiple answers possible)

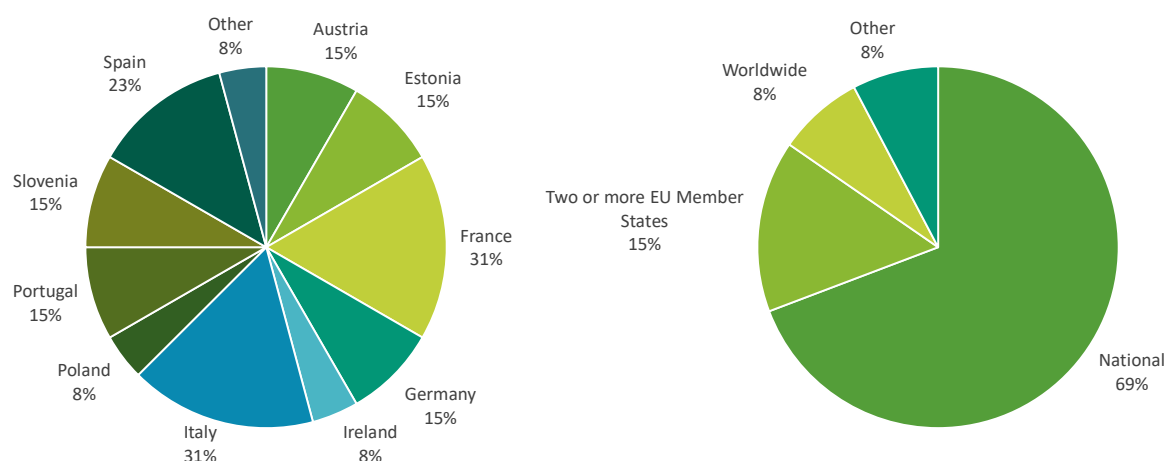
As the targeted survey was aimed at those LEAs that make use of data retention in their daily activity, the prevalence of these areas of specialisation among the respondents is in line with the aim of the exercise, i.e. collecting concrete and illustrative examples.

The Study expressly targeted law enforcement activities, while activities linked to national security were excluded for being outside the scope of the Study. Respondents (to both the targeted survey and the interviews) were thus identified among those LEAs that do not have national security functions. However, in many cases, LEAs cooperate with national security authorities. As such cooperation could potentially compromise the validity of the Study, respondents to the survey (29% of whom perform some national security activities) were asked to exclude such activities from their answers. The inputs collected thus reflect law enforcement functions of the LEAs consulted, and not their national security functions.

Targeted survey of ESPs: respondents' profile

Overall, the targeted survey of ESPs had 13 valid (complete) replies, from all 10 Member States covered²⁷.

²⁷ One survey reply arrived too late to be included in processing of the survey results. However, the input was taken into account in the analysis.

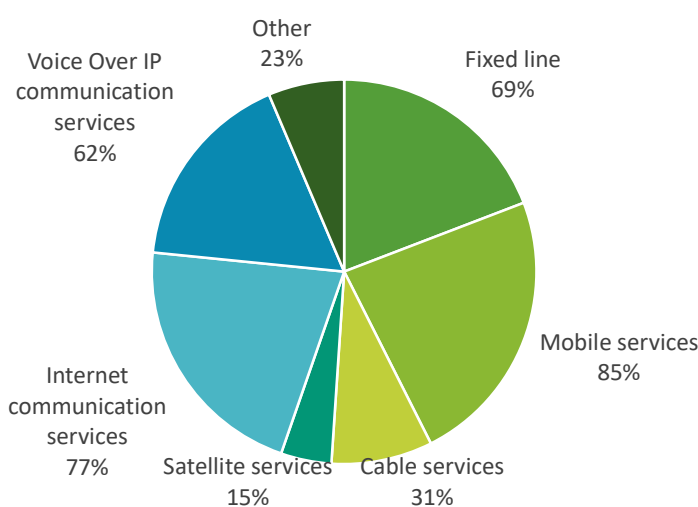
Figure 5: Replies to ESP targeted survey, by EU Member State and territorial activity

Source: Targeted survey of ESPs, Questions 2 and 3 (N=13)

The vast majority of the respondents (69%) were ESPs active only on the national market, while 15% were active in two or more Member States and a small minority worldwide and/or in one Member State and one or more third countries. However, even when present in more than one EU market, national branches operate with a large degree of autonomy, which includes the obligations and practices for data retention.

All but one of the respondents were large-sized businesses, with a staff headcount of 250 employees or more and/or an annual turnover above EUR 50 million.

The vast majority of the respondents (85%) provide both B2B and B2C (business-to-consumer) services, while only a small minority specialise in B2B and B2C services only (8% in each case). Most of the respondents provide fixed, mobile, and internet communication services (69%) and voiceover IP (VoIP) communication services (61%).

Figure 6: Replies to ESP targeted survey, by type of electronic communication service provided

Source: Targeted survey of ESPs, Question 8 (N=13, multiple answers possible)

Among the respondents, cable and satellite services were less frequent (31% of respondents provide them, in addition to fixed, mobile and internet communication

services, while the combination of cable/satellite and internet communication services is much less frequent among the ESPs consulted), while other services such as hosting, cloud computing services and wholesale access to infrastructure are provided by a small minority.

3.3.3. Targeted interviews

A set of interviews were conducted during the whole Study. During the inception task, the core team conducted a set of initial (scoping) interviews to get a better understanding of the legal, technical and technological context of the Study and to increase awareness of the Study and the forthcoming targeted consultation.

The vast majority of the other stakeholders' interviews were conducted in parallel with the desk research and targeted consultation tasks. These interviews aimed to complement the information collected through desk research and targeted surveys and to obtain a deeper understanding (and further evidence) of national practices, needs and stakeholder opinions.

The tables below provide an overview of the interviews conducted as part of the Study.

Table 1: Interviews conducted during the Study – EU level

Type of stakeholder	N. of interviews	Organisations
EU services/bodies/agencies	2	<ul style="list-style-type: none"> ■ Europol ■ Eurojust
ESPs' representative organisations	3	<ul style="list-style-type: none"> ■ European Telecommunications Network Operators' Association (ETNO) ■ European Competitive Telecommunications Association (ECTA) ■ Pan-European association of European Internet Services Providers Associations (EuroISPA)
OTTs	2 (and 2 follow-up interviews)	<ul style="list-style-type: none"> ■ Restricted information

Source: Milieu elaboration

Table 2: Interviews conducted during the Study – Member State level

Member State	LEAs	NRA/DPA	ESPs
Austria	2	1	0
Germany	3	2	0
Estonia	3	2	3
Spain	0	0	0
France	4	0	3
Ireland	2	0	0
Italy	0	2	2
Poland	3	1	0
Portugal	3	1	1
Slovenia	3	1	1
EU level	/	/	4
Total	23	10	14

Source: Milieu elaboration

All interviews were designed as **semi-structured interviews**²⁸ and followed guidelines prepared by the core team. Interview guidelines included general questions common to all

²⁸ Semi-structured interviews follow specific guidelines to ensure that relevant and comparable information is collected from all stakeholders, while leaving some flexibility for stakeholders to address specific points that may not have been foreseen initially but that add value.

interviewees, questions tailored to specific types of stakeholders and questions related to relevant national issues identified from the desk research and the analysis of the survey replies.

The targeted interviews in Member States aimed to collect in-depth knowledge about national practices and thus complement the information collected through the surveys. Comparison of the findings for each Member State enabled the detection of patterns specific to national contexts and/or cross-cutting issues common to different stakeholders.

3.4. ANALYSIS AND ASSESSMENT OF INFORMATION

The Study collected a large amount of evidence, including national and EU studies and reports, 10 country fiches, two targeted surveys and 52 interviews with stakeholders at EU and national level. The process used to analyse the evidence and elaborate answers to the research questions was based on **meta-analysis of information** and **triangulation of data**.

The **meta-analysis of information** involved tagging and coding all inputs to the analysis, as follows:

- Mark sections of country fiches/interview write-ups against the analysis framework and the related questions and indicators to identify all of the evidence relevant to the research questions;
- Identification of main themes, topics or categories;
- Mapping of the inputs (write-ups/fiches) against defined categories.

The meta-analysis included quantitative elements (e.g. number and type of requests for access to non-content data in the Member States covered by the Study, type of costs encountered by ESPs) and qualitative elements (e.g. national legal frameworks, rules and practices, stakeholders' views).

When carrying out the meta-analysis, the core team drew clear distinctions between:

- **Facts:** objective changes to a legal framework or exact data on numbers of cases, where available;
- **Estimates:** if no data were available on numbers of access requests or trends over the last few years, stakeholders were asked for their estimations. Their use is clearly highlighted in the analysis;
- **Actual** experiences: narratives of what happened and how, from stakeholders consulted (factual descriptions);
- **Opinions:** perceptions of the ease of access of the service.

Data triangulation sought to use different sources of information to increase the validity of the findings by confirming results with different sources. By combining the views and experiences of multiple stakeholders and empirical materials, such triangulation aimed to reduce the weakness or intrinsic bias associated with single method, single observer and single theory studies. It also constituted a tool for delivering evidence-based assumptions, if limited data is available on certain specific topics.

The data triangulation involved cross-checking consistency across different sources of data:

- **Comparing factual information from different sources**, e.g. major discrepancies between sources reporting the reasons for refusal of requests for access to non-content data between LEAs and ESPs in the same Member State and in the same time period. If required, additional data collection or review was carried out with stakeholders.

- **Taking stock of differences** in perspectives, experiences or opinions across information from different stakeholders.

The use of the data triangulation technique continued during the data analysis phase, allowing for more nuanced and accurate conclusions.

In addition, thematic experts were consulted throughout the Study, to fine-tune the data collection tools, integrate the stakeholder mapping and validate the key findings from the analysis.

3.5. CHALLENGES, LIMITATIONS AND MITIGATION MEASURES

The Study faced a number of challenges, including the sensitivity of the topic and the outbreak of the COVID-19 pandemic, which posed additional challenges to data collection and, subsequently, the analysis of evidence. A set of mitigation measures were implemented to address these challenges to the extent possible.

The **sensitivity of the topic of data retention** had repercussions for the stakeholder consultation activities. Many **stakeholders** (LEAs, ESPs, OTTs, across several of the 10 Member States) **declined the invitation to participate**, despite the guarantee of confidentiality and protection of the information provided. Refusals were communicated to the European Commission, together with the explanation provided by the stakeholder. **Mitigation measures** included offering stakeholders the option to partially complete the survey or to take part in the interview only, extended deadlines, and reiteration of the Study aims. Some organisations preferred to answer in writing instead of telephone interviews.

Despite numerous emails and telephone calls, some stakeholders did not respond to the communications sent by the core team and national experts. With a limited number of police bodies and law enforcement organisations using retained data and a limited number of ESPs in any country, it was not always possible to replace stakeholders. In order to minimise the risks of not reaching relevant stakeholders, the core team involved EU level representatives (Europol and Eurojust for LEAs and umbrella associations for ESPs) in outreach from the start of the project. Personal contacts were also used to boost participation.

Due to the **lockdown measures** in all EU Member States covered by the Study, stakeholders were not operational from February to the end of April 2020 or were overwhelmed with other pressing issues, such as the execution of restrictive measures to contain the spread of the virus (LEAs) and the facilitation of increased demand for telecommunication services (ESPs). To minimise the risks caused by the unavailability of stakeholders, the **duration of both surveys was prolonged**, from 31 March for LEAs and 8 April for ESPs, to Friday 12 June 2020 (close of business day). As an additional mitigation measure, interviews and follow-up interviews were conducted in parallel (before the closure of the survey) through the months of May and June 2020. For countries where there was little direct information from practitioners, the core team and national experts tried to accommodate late responses to interviews.

In addition to the challenges described above, the Study itself presents some limitations:

- The sample of replies is **not statistically representative** of LEAs and ESPs in the 10 EU Member States, due to the limited response rate among stakeholders, but also to the design of the Study, which aimed to collect statistics and circumstantial evidence;
- **Data gaps**, due to the reluctance (and in some cases inability) of stakeholders to share statistics on data retention;
- Extremely **limited comparability** of the few statistics collected, due to the differences in national definitions and practices, and to the absence of EU-level definitions and reporting obligations.

4. REGULATORY AND INSTITUTIONAL FRAMEWORK ON RETENTION OF AND ACCESS TO NON-CONTENT DATA FOR LAW ENFORCEMENT PURPOSES

This section maps the existing legal obligations and institutional frameworks in the 10 selected Member States covered under this Study on retention of and access to ESPs' non-content data for law enforcement purposes (section 4.1). The overview of legal rules presented below is factual and does not constitute an evaluation of these national laws. Finally, this section considers the role and function of national authorities, both NRAs and DPAs (section 4.2). The final section (4.3) summarises the key findings here.

4.1. CURRENT REGULATORY FRAMEWORK

This section describes the current regulatory framework for retention of non-content data by national ESPs. It focuses on two aspects:

1. Overview of the general legal framework for retention of non-content data by ESPs (section 4.1.1);
2. Overview of the institutional framework, describing the organisations involved in the retention of and access to non-content data (section 4.1.2).

The analysis in these sections is primarily based on the national-level legal research, which was complemented and verified during follow-up interviews with the stakeholders.

4.1.1. Overview of general legal framework for retention of and access to non-content data

Member States' responses to the annulment of the DRD diverged, with actions initiated at national level increasing the diversity of national data retention systems:

- Member States in which the **national laws transposing the DRD remain in force without any major changes** and for which there is a **legal obligation** for ESPs to retain non-content data (EE, ES, FR, IE, IT, PL, PT);
- Member States that **amended their legislation or enacted new data retention laws** following the CJEU case-law (DE²⁹);
- Member States whose **national laws were repealed** following the annulment of the DRD and for which there is currently **no legal obligation** for ESPs to retain non-content data (AT, SI).

The table below provides an overview of the current state of the legislative framework on data retention in the 10 Member States.

Table 3: Overview of the current legal framework

Country	Legal obligation to retain non-content data	Changes since annulment of the DRD	Ongoing legal changes, court cases or political processes
AT	×	National law repealed	×
DE	National legislation not enforced	New legal regime - not enforced	Request for CJEU preliminary ruling
EE	✓	No change	<ul style="list-style-type: none"> ■ Ministry of Justice currently drafting amendments to data retention law

²⁹ In Germany, a new legal regime on data retention for law enforcement entered into force in 2015 but is currently not enforced. As a result, there is *de facto* no data retention obligation in Germany. All of the information concerning the current legal framework in Germany used in this Study is thus based on the analysis of current practices.

Country	Legal obligation to retain non-content data	Changes since annulment of the DRD	Ongoing legal changes, court cases or political processes
			■ Request for CJEU preliminary ruling *
ES	✓	No change	
FR	✓	No change	Request for CJEU preliminary ruling
IE	✓	No change	■ Irish legislator drafting new legislation ■ Request for CJEU preliminary ruling
IT	✓	Minor changes to old legal regime	DPA advocates revision of national legislation
PL	✓	Minor changes to old legal regime	*
PT	✓	No change	Case before Constitutional Court
SI	*	Main articles of national law repealed	MPs filed a motion to review the constitutionality/legality of repealed articles

Source: Milieu elaboration based on desk research and stakeholders' input

Of the 10 Member States, seven (EE, ES, FR, IE, IT, PL, PT) still apply the national laws transposing the DRD, which have not been fundamentally altered in structure or substance since the annulment of the DRD. This means that retention of data in those countries is still general and not targeted, as required by CJEU case-law. In **Italy**, however, the legislator amended the national law in 2017, extending the length of the retention period to 72 months to deal with cases of serious crime. By contrast, in **Poland**, the data retention period has been shortened from 24 months to 12 months.

In three of the 10 Member States (AT, DE, SI), the national laws were either entirely or partially repealed following legal proceedings. In **Austria**, the Constitutional Court revoked the national acts on data retention, finding them unconstitutional³⁰, with retention of and access to non-content data for law enforcement purposes reverting to the practice in place before the transposition of the DRD. In **Germany**, a new legal regime³¹ on data retention for law enforcement purposes was adopted in 2015 to re-introduce mandatory data retention for ESPs from July 2017. However, in June 2017, following a decision of the Higher Administrative Court for North Rhine-Westphalia that the national legislation was contrary to EU law, the Federal Network Agency (*Bundesnetzagentur* or *BNetzA*) announced that it would abstain from enforcement measures until the case was concluded. The Federal Administrative Court subsequently made a request for a preliminary ruling to the CJEU in September 2019³². In **Slovenia**, the Slovenian Constitutional Court revoked the main articles in the legislation on data retention for law enforcement purposes in 2014³³. The Slovenian Supreme Court held that that decision does not interfere with the competence of the LEAs to access ESPs' non-content data stored for their commercial purposes, as access is based on a court order and does not mean upfront and indiscriminate non-content data collection³⁴. In 2019, a group of Parliament members filed a motion to reassess the constitutionality and legality of the

³⁰ Constitutional Court 27.6.2014, G 47/2017-49.

³¹ Act for the introduction of a retention obligation and a limited duration of retention for traffic data from 17 December 2015 (*Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*), bringing inter alia modifications to the German Telecommunications Act.

³² In Joined cases C-793/19 and C-794/19 *SpaceNet a.o.* the German Federal Administrative Court is asking the CJEU if the 2015 German legislation is in conformity with the e-Privacy Directive read in light of the EU Charter of Fundamental Rights.

³³ Judgment of the Constitutional Court of the Republic of Slovenia, case number U-I-65/13-19 of 3 July 2014.

³⁴ Judgments of the Supreme Court of the Republic of Slovenia, case numbers XI Ips 9569/2015-396 of 23 July 2015 and I Ips 90495/2010-500 of 9 June 2016.

provisions on access to non-content data³⁵, claiming that the conditions for access are defined too broadly.

In the three Member States whose national laws under the DRD were discontinued, both LEAs and ESPs voiced their concern, with LEAs arguing that this results in uncertainty about the amount and type of non-content data that will be available for investigations and prosecutions, while ESPs noted the uncertainty about their data retention practices and procedures for granting access to data to LEAs. **Consequently, LEAs need to rely on the non-content data maintained by ESPs for their own commercial or business purposes.**

All of the information concerning the current legal and practical arrangements in respect of retention of and access to non-content data for law enforcement purposes in Austria, Germany and Slovenia is thus based on the system of retention of non-content data for business purposes of the ESPs.

Box 1: Legal uncertainty about the application of the current framework

In Germany, the national legislation from 2015 that introduced changes to the Telecommunications Act (TKG) **is not currently enforced** due to alleged non-conformity with EU law in light of the relevant rulings of the CJEU (*Digital Rights Ireland* and *Tele2 Sverige*). The Federal Networks Agency decided to refrain from issuing instructions and other measures to ESPs to enforce the data retention obligations set out in Section 113b TKG. In 2019, the German Federal Administrative Court sent a request for a preliminary ruling to the CJEU and suspended the national proceedings.

These uncertainties have led to court cases and political actions. Due to fears of inadmissibility of non-content data as evidence in criminal proceedings, some courts refuse to order the collection of such data. The current practice, both in terms of retention of and access to non-content data in Germany, is therefore based solely on the provisions of the TKG, which prescribe operational storage of traffic data for the purpose of billing, detection, limitation and elimination of malfunctions and for the detection of misuse. To address this legal uncertainty, several German ESPs have expressed the need to trigger an overall debate on the need for data retention and a legal basis in conformity with EU case-law.

There is also legal uncertainty within the seven Member States that still apply laws transposing the DRD. As national legislative frameworks have, in most cases, remained unchanged, **defence lawyers in these countries have challenged the admissibility of non-content data as evidence in criminal proceedings.**

This is particularly true in **Ireland**, where the national legislation on data retention remains valid but is not used to its full extent by LEAs, out of concern that convictions will be overturned. This is due to a 2018 case in which the High Court found that large sections of the main articles of the 2011 Irish Communications (Retention of Data) Act were invalid in light of EU law³⁶. Subsequently, in early 2020, the Irish Supreme Court made a request for a preliminary ruling from the CJEU on the issues of: whether universal retention of non-content data is permissible under EU law; the access regime's review and supervisory processes (or lack thereof); and the retroactive effects of national legislation being declared invalid³⁷. Meanwhile, the Irish legislator is drafting new legislation on data retention for law enforcement purposes, which may introduce a differentiation in retention periods for different categories of non-content data, as well as a requirement for LEAs to obtain ex-ante authorisation to access data.

Court cases challenging the admissibility of non-content data have also taken place in Italy and Portugal. However, the courts in those Member States found that the national laws on

³⁵ https://www.sds.si/sites/default/files/Zahteva%20za%20oceno%20ustavnosti_hisnepreiskave_080519.pdf.

³⁶ *Dwyer v Commissioner of An Garda Síochána* [2018] IEHC 685; [2019] IEHC 48.

³⁷ C-140/20 *Commissioner of An Garda Síochána and Others*.

data retention were not contrary to the national constitutions. In a case in 2017³⁸, the **Portuguese** Constitutional Court was asked to review the constitutionality of certain provisions of the national law, which establish a legal obligation for ESPs to retain non-content data. In assessing the case, the Court decided that the provisions were not unconstitutional, as the restriction to the fundamental right to privacy was pursued for a constitutionally relevant purpose (i.e. safeguarding democratic legality and criminal prosecution). The Portuguese Constitutional Court concluded that it was adequate, necessary and proportional to satisfy this purpose. This position could be changed, however, as a case before the Constitutional Court is reviewing the constitutionality of some articles of the national data retention law following a request by the Portuguese Ombudsman in August 2019. In addition, the Portuguese Data Protection Commission has systematically alerted the legislator to the need to revise the law.

In **Italy**, two recent cases in front of the Court of Cassation³⁹ considered whether the current Italian legal framework for data retention (including the 72-month retention period for certain serious crimes (massacre, civil war acts, mafia type crimes, murder, aggravated robbery, aggravated extortion, kidnapping for ransom, terrorism, child pornography, participation in armed groups) is compatible with EU principles and rules, stating that these principles concern access to non-content data rather than the rules on retention. During a case in 2019⁴⁰, the defence lawyer argued that the Italian law on data retention was not compatible with the EU Charter of Fundamental Rights as interpreted by CJEU case-law. He argued that the Italian law would not fulfil the proportionality test, as: (1) it foresees access and retention of non-content data for any type of crime; and (2) the power to authorise access to data is granted to the Public Prosecutor instead of a judge or another independent authority. The Court of Cassation held that the Italian legislation is compatible with EU law, stating that: (1) the CJEU case-law concerns only those Member States that do not have legislation in place on data retention and access, whereas Italy has adopted specific rules on data retention⁴¹; and (2) the Italian legislation is proportional because the time limits are adequate and the Public Prosecutor is a sufficiently independent organ. No other notable court cases or legal changes were identified, although the Italian DPA adopted a critical stance towards the extension of the retention period to 72 months in several opinions issued in 2018. It advocates a revision of the national legislation to bring it in line with CJEU case-law.

National law in **Estonia** has faced important internal criticism and the Ministry of Justice is drafting amendments to the data retention law with the aim of creating a clearer legal framework. Although the draft is not yet published, one option is the differentiation of retention periods for different types of non-content data by considering the level of interference with the rights of the subjects and the purposes for which the non-content data are retained. The Estonian Supreme Court also sent a request for a preliminary ruling to the CJEU in 2018⁴².

In **France**, the French Council of State sent a request for a preliminary ruling to the CJEU in 2018, concerning the conformity of the French legislation with EU law⁴³. In **Poland and**

³⁸ Decision of the Constitutional Court of Portugal in case n°420/2017.

³⁹ Judgments of the Court of Cassation in cases no 36380/2019 and no. 5741/2020.

⁴⁰ Judgment of the Court of Cassation (criminal division) in case no 36380/2019.

⁴¹ This argument has been criticised in the legal literature on the grounds that the CJEU judgments in *Digital Rights Ireland* and *Tele2 Sverige* describe national regulations on data retention. The argument also states that even if the judgments had concerned Member States without data retention regulations, CJEU case-law clarified the requirements that must be respected not only by EU law but also by national laws. See Luparia, L. (2019). 'Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio', in *Diritto di internet*, Issue 4, p. 762.

⁴² In C-746/18 *H.K. v. Prokuratuur*, the Estonian Supreme Court asks the CJEU whether the type of non-content data and the length of the period of access to those data are relevant in deciding on the seriousness of the interference with fundamental rights.

⁴³ Case C-511/18 and C-512/18 *French Data Network, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs v Premier ministre, Garde des Sceaux, Ministre de la Justice*.

Spain (aside from the 2018 *Ministerio Fiscal* case⁴⁴) **no formal legal, court or political challenges to the current national data retention law have been identified.**

4.1.2. Overview of institutional framework for access to non-content data

The key stakeholders concerned by the retention of and access to electronic communications non-content data are the ESPs that retain such data and the LEAs that seek to access them (see **Annex II** for an explanation of these concepts).

In the majority of the Member States, the national legislative framework provides for access to non-content data by **police authorities** (including the military police, in some cases) and **judicial authorities** (public prosecutors and judges). Many Member States, however, have **expanded the right to access** retained non-content data to **other types of national authorities**, most commonly tax, customs or competition authorities. In these cases, non-content data can only be requested for criminal offences that fall under the remit of the authority, i.e. tax authorities can only request access to non-content data in relation to tax-related offences. In most Member States, based on the national legislative frameworks, the procedure these authorities must follow in order to access non-content data does not differ from that for police authorities (see section 7.1). While **intelligence agencies** can access non-content data in most Member States for national security purposes, this Study only includes intelligence agencies where they can also access data **for law enforcement purposes** (i.e. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and/or similar purposes). This is the case for intelligence agencies in four Member States (AT, EE, ES, PL). The specific crimes and procedures that must be followed by these different national authorities in order to access non-content data are discussed in sections 6.4 and 7.1.

Table 14 in **Annex III** provides an overview of the different types of authorities that can access non-content data in each Member State, along with the specific roles within those authorities authorised to submit requests. The list of authorities is standardised for comparison purposes, meaning that some national authorities combine the competences of several types of authorities.

In **Estonia**, access to non-content data is granted to several authorities and agencies. As the focus of this Study is on criminal law enforcement purposes, only the rules concerning access requests prescribed in the Estonian Code of Criminal Procedure and Code of Misdemeanour Procedure were analysed. Access requests in Estonia can also be made outside the scope of the aforementioned legislative acts by a variety of agencies and authorities and for a variety of purposes (e.g. courts in the course of civil proceedings). Some of the agencies and authorities listed in the tables below may also be permitted to submit access requests on the basis of other legislative acts (e.g. the Financial Supervisory Authority may also request access pursuant to the Securities Market Act), although the authorisation, control and supervision mechanisms may differ. The situation is especially complex in relation to security authorities. For example, the Estonian Internal Security Service can submit access requests on the basis of different legal acts, depending on which function it is fulfilling, and there may be partial overlap in applicable law that results in lack of legal clarity. Agencies and authorities not listed in the Code of Criminal Procedure and Code of Misdemeanour Procedure, or provisions permitting access requests for purposes other than those listed in the aforementioned acts are not covered by the Study. In **Italy**, access to non-content data is granted to defence lawyers in criminal proceedings. Article 132(3) of the Italian Data Protection Code gives the defence the right to request access to non-content data relating to accounts belonging to their client, who is a suspect or a defendant in a criminal proceeding, for a period of 24 months.

Based on publicly available information and stakeholder consultations, in most Member States, **any public prosecutor or judge working on the case** at hand can request access to non-content data. Rules on access to non-content data vary for police authorities, however. Only in three Member States (**AT, PT, SI**) **can any police officer working on**

⁴⁴ Case C-207/16 *Ministerio Fiscal*.

the case at hand request access to non-content data (having obtained prior judicial authorisation where applicable – see section 7.1). In other Member States, the **internal procedures are more hierarchical**, with specific rank requirements (**IE**), lists of positions (**EE**), lists of authorised agents (**FR**) or authorisations from Commanders in Chief (**PL**) necessary to access non-content data. In **France**, internal procedures depend on the type of authority. As a general rule, access requests can only be made by officers or agents of sufficient rank, who are authorised to do so by higher rank officials. Access requests often require authorisation from another authority or need to be transmitted through SPOCs. In **Poland**, the request to access data can be made by any operational officer (i.e. officer carrying out the investigation), provided the application is signed by a superior officer or a duty officer and transmitted through SPOCs. Exceptions exist for certain departments of Police Headquarters, the Central Investigation Bureau of the Police and the Regional Police Headquarters, where the application can be made directly by a police officer with authorisation of the Police Commander. In **Ireland**, where the national legislation is currently being scrutinised by the Supreme Court, efforts have been made to tighten the internal prior authorisation process within the police authorities. When accessing non-content data for the purposes of investigation and prosecution of criminal cases, the Irish police follow a more restricted access regime, for reasons of prudence.

In **Germany**, access to non-content data may only be ordered by the court upon the application of the Public Prosecutor or the investigative judge. The latter oversees the investigation and uses so-called investigative personnel (police or other law enforcement officers) to make an access request. Access to subscriber data can also be obtained directly by certain police officers (e.g. detectives) who have access to specific software without the need for authorisation. In **Italy**, the legislation does not expressly envisage a role for police authorities in accessing non-content data, as the police are 'at the service' of the Public Prosecutor⁴⁵. However, based on certain provisions in the law and practices in the field, it is evident that the police can access data for criminal investigations and proceedings but only with the authorisation and at the request of the Public Prosecutor. For the investigation of certain crimes (organised crime and terrorism), the respective Heads of authorities (e.g. Minister of Home Affairs, certain LEAs) can request access to non-content data but these data cannot be used in criminal prosecutions⁴⁶.

Due to the lack of survey responses and/or unavailability of stakeholders, it was not always possible to find publicly available information or to obtain more information on how such authorisations and delegations occur. This is particularly true for **Spain**.

Box 2: Fragmented institutional framework can result in legal uncertainty on the circumstances for access to non-content data

In Estonia, the situation is particularly complex. **Access to non-content data is granted to a large number of authorities and agencies**, with the rules to access non-content data specified in both the Estonian Electronic Communications Act (ECA) and in several laws that regulate the access requests for each authority and agency. Access to non-content data is most commonly requested by the Police and Border Guard Board, which conducts most of the criminal and misdemeanour proceedings (the other investigative bodies have limited competence, i.e. for investigating or assisting with the investigation of specific crimes).

The ECA does not clarify the roles within these authorities and agencies that may access non-content data nor provide any criteria that must be fulfilled to request access. As a consequence, rules on authorisation, control and supervision mechanisms differ by authority and are sometimes regulated in several sectoral laws or even in internal procedural rules and regulations.

Stakeholder input suggests that despite the general wording of the regulation on accessing non-content data, it is interpreted strictly in conjunction with the fundamental rights of individuals by the authorities making the request. **Access requests in criminal proceedings are made based on the *ultima ratio* principle**, the necessity of requests being initially assessed by the person

⁴⁵ Article 327 of the Criminal Procedure Code.

⁴⁶ Article 226(4) of Legislative Decree 271/1989.

conducting the proceedings, taking into consideration all circumstances of the case at hand, including the severity of the crime. Internal regulations often stipulate further conditions to access non-content data and technical and organisational measures are being taken to ensure compliance. The necessity of requests is assessed even more strictly in misdemeanour cases.

4.2. ROLE AND FUNCTION OF NATIONAL AUTHORITIES

This section presents an overview of the competences and responsibilities of NRAs and DPAs with respect to the rules on retention of non-content data. The analysis in this section is based on information collected through desk research and input from stakeholders, in particular interviews with national authorities.

The evidence shows that **competences and responsibilities in most Member States (AT, DE, EE, ES, IE, IT, PL, SI) are shared between the NRAs and the DPAs.** Although this overlap of competences could potentially raise issues, stakeholders tended to believe that the division of powers is clear. (See Table 15 in **Annex III** for an overview of the competences of different national authorities within each Member State and potential tensions due to overlap of those competences.)

In all 10 Member States, DPAs are primarily responsible for the protection of personal data. Their competences commonly include: handling complaints from individuals for violation of their personal data rights in respect of retention of and access to non-content data related to them, supervision of requirements for processing personal data, supervision of the use of non-content data, supervision of security requirements, oversight of notification requirements in cases of data breach, and receipt of reports on access requests.

As a general rule, **national DPAs are competent to supervise the actions of both ESPs and LEAs**, with the exception of national courts when acting in their judicial capacity⁴⁷. **Several Member States (AT, EE, IE) have given special institutions authority to exercise supervision of requests to access non-content data by LEAs.** In Estonia, such authority falls mainly on the Chancellor of Justice, while in Ireland, a High Court judge can ascertain whether LEAs are complying with the national rules on data retention. In **Austria**, a legal protection officer (with several deputies) within the Federal Ministry of the Interior supervises the use of surveillance measures, as the person affected cannot raise any legal remedies against themselves. In **Poland**, however, neither of the authorities is empowered to supervise access to data by the LEAs.

By contrast, the role of NRAs depends on the existence of national data retention rules. In countries with no general data retention obligation, NRAs do not have any power over the obligation of ESPs to assist LEAs in access requests. In countries where there is a legal obligation for ESPs to retain non-content data for law enforcement purposes, **NRAs are primarily responsible for the oversight of ESPs' obligations under national data retention laws.** In **France**, the situation seems unclear, as the NRA has indicated that it does not have any competence, stating that the competent authority for the telecommunication sector is the inter-ministerial Defence Electronic Communications Commissioner (*Commissariat aux communications électroniques de défense - CCED*), in charge of the implementation of the technical aspects of SPOCs and relations with ESPs.

In Estonia, Italy, Poland and Spain, NRAs have the authority to sanction ESPs for non-compliance with national obligations on general data retention. Despite this option, **sanctions remain a last resort**, chiefly due to overall compliance by the ESPs (EE, IT). In **Ireland**, no penalty is specified for non-compliance with a disclosure request.

In **Estonia**, the competences of the NRA are three-fold. The NRA exercises supervision of ESPs' obligations to retain non-content data and to delete data after the retention period elapses. ESPs thus submit annual confirmation of the deletion of non-content data.

⁴⁷ Article 55(3) GDPR and Article 45 of the Law Enforcement Directive 2016/680.

Although the NRA used to proactively check on ESPs, the latest inspection of ESPs' retention of necessary data was carried out in 2011 and the authority has not yet imposed sanctions. Finally, the NRA collects statistics from ESPs on non-content data access requests. The latter obligation has become obsolete due to the annulment of the DRD and the obligation to report those numbers to the European Commission. Despite the fact that the authority does not actively exercise this power, several ESPs still submit the data. The same is true for **Poland**, where the NRA supervises ESPs for compliance with legal requirements in the area of non-content data retention, in particular the types of non-content data that require storage. If legal requirements are not met or are improperly met (including the submission of incomplete data), the NRA may decide to exercise control over the ESP based on the Telecommunications Act or the administrative procedure (e.g. imposition of a fine). Proceedings are generally initiated based on reports of violations of obligations or based on a complaint by LEAs.

Although a data retention obligation exists in **Italy**, the NRA has more of a monitoring role. Its main function is the maintenance of the Registry of Enrolled Operators (*Registro degli Operatori di Comunicazione – ROC*), which includes all market operators receiving personal data. Nevertheless, the legislative framework also includes sanctions for ESPs that do not fulfil their obligations to support LEAs, including suspension or even loss of their licence and possible criminal sanctions.

In **Spain**, the current regime is unusual, with the competence to oversee ESPs obligations under national data retention rules shared between the DPA and the NRA, with the Ministry of Economy and Digital Transformation empowered to initiate proceedings and input to the resolution of the sanctioning procedure. National legislation lays down a sanctioning regime for ESPs, differentiating between very serious, serious and minor infringements⁴⁸. As a general rule, the NRA is the competent authority to verify whether any of these infringements has been committed, while the DPA is responsible for overseeing whether non-content data are retained for a sufficient period of time and if ESPs comply with the data protection and security obligations (where this does not constitute a serious breach).

The situation is different in **Portugal**, where **competence to oversee ESPs' data retention obligations is held by the DPA, including inspection, supervision and imposition of sanctions**. The DPA inspects the implementation of the following obligations of the ESPs: to guarantee the protection and safety of the data (e.g. security and deletion of data); to keep a constantly updated electronic record of persons specially authorised to access the data retention database; and to send (on a quarterly basis), the records of the data transmitted to the LEAs. Despite these broad powers, **in July 2017, the Portuguese DPA decided not to enforce data retention obligations due to claims of unconstitutionality of national law**. It thus refrains from sanctioning ESPs for non-compliance with the obligation to retain and provide access to non-content data. It does, however, exercise its other supervisory roles, including ensuring that security requirements are respected.

4.3. KEY FINDINGS

- Three out of the 10 Member States currently have no legal obligation for ESPs to retain non-content data for law enforcement purposes (*de jure* Austria and Slovenia and *de facto* Germany, as the national data retention framework is not enforced). In these three Member States, LEAs need to rely on the non-content data kept by the ESPs for their own commercial or business purposes. Seven of the 10 Member

⁴⁸ Article 10(1) of the Law on Data Retention provides that 'It is a very serious infringement not to retain the data referred to in Article 3 at any time'. Serious infringements are: (i) repeated or systematic failure to retain the data referred; (ii) retention of data for a period shorter than that laid down in law and; (iii) the deliberate failure to comply with the data protection and security obligations. Minor infringements are: (i) failure to retain the data, where this does not qualify as a very serious or serious breach; and (ii) failure to comply with the data protection and security obligations, where this does not qualify as a serious breach.

States still broadly apply the national legislation transposing the DRD (EE, ES, FR, IE, IT, PL, PT).

- Overall, there is legal uncertainty and confusion about the practices of non-content data retention and access, with ongoing legal or political proceedings in seven Member States (DE, EE, FR, IE, IT, PT, SI), four of which (DE, EE, FR, IE) have requests pending for preliminary rulings from the CJEU. In Ireland and Estonia, the national legislation is also being amended/redrafted.
- Legal uncertainty with respect to the current legal framework on retention of and access to data is a primary challenge for both LEAs and ESPs in almost all Member States. Even where national legislation on data retention is still valid, fears of convictions being overturned due to the inadmissibility of non-content data in criminal proceedings may prevent LEAs from accessing non-content data retained for law enforcement purposes. Pending cases in front of national courts and the CJEU amount to further legal uncertainty.
- In the majority of the Member States, the national legislative frameworks provide for access to non-content data for police authorities (including military police, in some cases) and judicial authorities (public prosecutors and judges), as well as to intelligence agencies. Many Member States have expanded the right to access retained non-content data to other types of national authorities, most commonly tax, customs or competition authorities. Although such authorities are not considered LEAs per se, non-content data can only be requested for law enforcement purposes, e.g. for criminal offences that fall under the remit of the authority.
- Estonia's fragmented institutional framework stands out. Here, access to non-content data is granted to a large number of authorities and agencies, with rules on access to non-content data specified in both general and sectoral laws. There is legal uncertainty with respect to who can access non-content data, for what purpose and under precisely which circumstances.
- As a rule, competences regarding rules on retention of non-content data are shared between the NRA and DPA. Although this overlap of powers could potentially raise issues, stakeholders noted no major problems.
- DPAs are primarily responsible for the protection of personal data, while NRAs are responsible for the oversight of ESPs' obligations under national data retention laws. This is logically the case for countries where national data retention rules are still in force. The situation is different in Portugal, where the competence to oversee ESPs' data retention obligations are enshrined in the DPA remit, including inspection, supervision and imposition of sanctions.
- National LEAs need to comply with rules on the processing of personal data, but NRAs do not have powers to oversee their actions related to access to non-content data. ESPs are subject to more stringent supervision by both DPAs and NRAs and can potentially face sanctions for non-compliance with data protection rules or national data retention obligations.

5. RETENTION OF NON-CONTENT DATA

This section presents the categories of non-content data that ESPs are legally obliged to retain for law enforcement and business purposes (section 5.1), a detailed analysis of the concept of IP address (section 5.2), retention periods (section 5.3), purposes for which data are retained (section 5.4) and the security requirements for storing the retained data (section 5.5). The final section summarises the key findings here (section 5.6).

The analysis is based on national-level legal research, complemented and verified through the targeted surveys and interviews with stakeholders.

5.1. TYPES OF NON-CONTENT DATA RETAINED

Non-content data can be categorised into three groups, which broadly contain the same type of information in all Member States:

- **Subscriber data:** the information enabling **identification of the sender** of a communication (e.g. name, address, username, phone number). In some countries (AT, ES, SI), this also includes information such as ID number, nationality and date of birth.
- **Traffic data:** the information necessary to identify the **type, date, time** and **duration** of a communication. It also includes any information enabling the **identification of the receiver(s)** or **attempted receiver(s)** of a communication.
- **Location data:** the information necessary to identify the **location of the communication equipment** (e.g. cell tower location; Wi-Fi hotspot).

While certain types of information are always classified as subscriber or traffic data across all Member States, there is no consensus on the classification of the following data points: IP addresses, SIM numbers, device identification numbers (e.g. IMSI, IMEI) and port numbers for dynamic IP addresses. In some Member States (EE, FR, IE⁴⁹), these data points are classified as subscriber data while others (DE, ES, IT, PL, SI) classify them as traffic data. This distinction is important as it impacts the conditions under which LEAs can access the data. In many Member States, access to subscriber data does not require judicial authorisation but it is mandatory for access to traffic and location data (see section 7.1.1.). The difference in access thresholds is linked to the level of interference with individuals' right to privacy. According to the jurisprudence of some courts, notably the CJEU⁵⁰ and the European Court of Human Rights (ECtHR⁵¹), retention and access to subscriber data is a less serious interference with privacy than access to traffic data. Subscriber data in themselves do not enable outside parties to draw precise conclusions in respect of the private lives of individuals⁵², unlike traffic data, which identifies where, when and with whom an individual has communicated. Some stakeholders argued that data such as port numbers for dynamic IP addresses or device identification numbers imply a greater interference with privacy rights and should therefore be subject to the same level of protection as traffic data. **Austrian law** classifies these data points within a **distinct category, 'access data'**, which are subject to higher levels of protection. In **Portugal**, there is disagreement between LEAs and ESPs over the legal classification of these data points. Personal Identification Number (PIN) and Personal Unblocking Key (PUK) numbers, for example, are considered traffic data by ESPs, yet public prosecutors consider them subscriber data (which do not require judicial authorisation for

⁴⁹ In Estonia, subscriber data are referred to as 'owner data'. Estonian LEAs can request subscriber data through the 'owner inquiries' procedure, for which no judicial approval is needed; Irish legislation does not make a clear distinction between subscriber and traffic data.

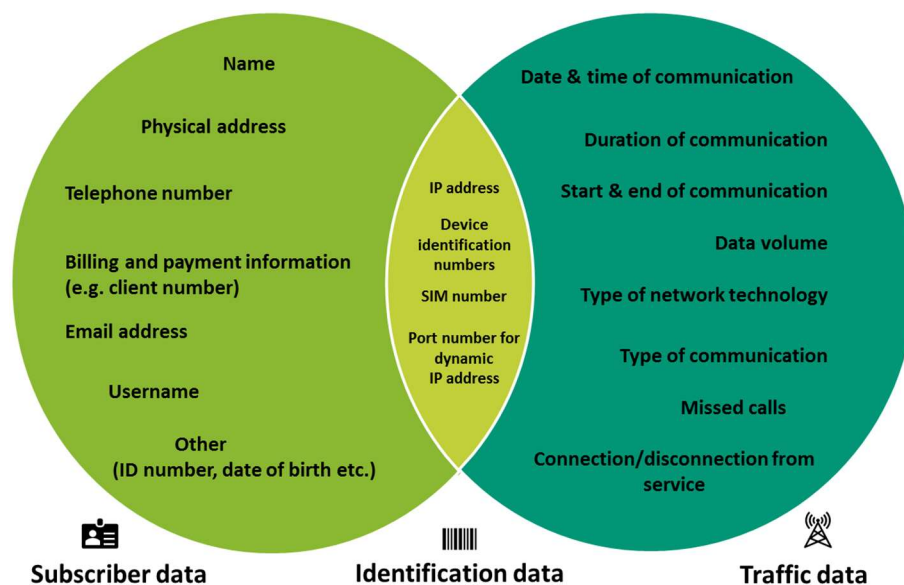
⁵⁰ Case C-207/16 *Ministerio Fiscal*, 2 October 2018.

⁵¹ *Benedik v. Slovenia*, Application No, 62357/2014, 24 April 2018.

⁵² Council of Europe (2018). *Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments*, Cybercrime Convention Committee, T-CY (2018)26.

access). According to Portuguese stakeholders, in many cases, unsuccessful requests from LEAs are due to differences in the interpretation of the applicable framework. **For the sake of clarity and precision, these overlapping data points will be referred to as 'identification data' within the Study** (see Figure 7). Where the terms subscriber and traffic data are used, they refer to the data always considered subscriber or traffic data in all Member States.

Figure 7: Classification differences between subscriber and traffic data







Source: Milieu elaboration

The types of data included under the mandatory data retention obligation are similar across Member States. A key difference is the amount of detail provided by the law specifying the types of data to be retained. Some Member States, such as Poland, Portugal and Spain, provide a detailed list of non-content data to be retained, while others, such as France, provide a broader non-restrictive definition of non-content data. Detailed tables on the types of data that must be retained in each Member State are available in **Annex III** (Table 16, Table 17, Table 18, Table 19).

In all 10 Member States, ESPs are authorised to retain data for business purposes (e.g. necessary for the provision of services, billing or marketing). In the Member States where there is no legal obligation to retain data for law enforcement purposes (AT, DE, SI), LEAs rely on the data retained by ESPs for business purposes. In practice, **the types of non-content data retained by each individual ESP for business purposes vary depending on their terms of use.** Stakeholder consultation and a review of the terms of use of the largest ESPs suggest that the non-content data retained for business purposes is broadly the same as the categories of non-content data described above. Key differences are the retention periods (see section 5.3) and certain data points, such as port numbers for dynamic IP addresses and missed calls, which are often not retained for business purposes, notably by German ESPs (see section 5.4).

Figure 8 below shows the types of data retained by ESPs (in percentage of survey respondents) for law enforcement purposes, business purposes or both. 100% of respondents retain information such as name, physical address, telephone number and billing information of a subscriber, along with the date and time of the communication.

Figure 8: Type of non-content data retained by ESPs (in percentage of respondents)

 Subscriber data		 Traffic data	
Name	100%	Date & time of communication	100%
Physical address	100%	Duration of communication	92%
Telephone number	100%	Start of communication	92%
Billing and payment information (e.g. client number)	100%	End of communication	92%
Email address	92%	Data volume of communication	92%
Username	69%	Type of network technology	92%
Other (e.g. ID number, date of birth)	23%	Type of communication	77%
 Identification data		Identifiers of the account/device to which the communication was sent.	62%
IP address	92%	Identifiers of the account/device to which the communication was forwarded or transferred.	54%
Device identification numbers (e.g. IMEI)	92%	Missed calls	54%
SIM number	85%	Connection to the service	46%
Port number for dynamic IP address	62%	Disconnection from the service	38%
 Location data		Identifiers of the account/device to which the communication was attempted to be forwarded or transferred.	23%
Location of the equipment or line at the start of the communication	77%		
Location of the equipment or line at the end of the communication	38%		

Source: Targeted survey of ESPs, Questions 10, 12, 14, 15 (N=13)

5.2. CONCEPT OF IP ADDRESS

IP addresses are a particularly challenging type of data for LEAs to obtain and use in criminal investigations and proceedings, despite their growing importance (particularly in the field of cybercrime). This section presents an overview of the key issues linked to IP addresses, which are referenced throughout the Study.

An IP address is a **unique numerical identifier** assigned to each device on a network. It serves a similar purpose to physical addresses or telephone numbers, i.e. to identify and locate devices. **IP addresses are necessary to connect to the internet, as they are the means by which devices communicate with one another**⁵³.

IP addresses can be either static or dynamic. Static IP addresses do not change over time, while dynamic IP addresses change periodically and are assigned to a user via Dynamic Host Configuration Protocol (DHCP) servers. **Most IP addresses assigned to users by ESPs are now dynamic**⁵⁴.

The increasing use of dynamic IP addresses creates a number of issues in the retention of and access to non-content data for law enforcement purposes. Unlike static IP addresses, which are stable and assigned to individual subscribers throughout the duration of their subscription with the ESP, **dynamic IP addresses change every few days or months** (for example every time a subscriber resets their router) and are **often assigned to multiple subscribers at the same time, using a CG NAT system**. CG NAT was adopted as a means to ease the transition from IP version 4 (IPv4) to IP version

⁵³ Vaughan-Nichols, S.J. (2020). *Static vs. Dynamic IP Addresses*, Avast Academy.

⁵⁴ *Ibid.*

6 (IPv6⁵⁵). It is a collection of strategies for sharing addresses among a large pool of internet consumers and was necessary due to the lack of IPv4 addresses. In these cases, a port number differentiates user connections linked to the shared IP address. ESPs need this port number together with precise time stamps in order to keep track of the subscriber to whom the IP address was assigned at a given moment in time⁵⁶. If an LEA requests access to information to identify the user behind a dynamic IP address, the port number and time stamp are both necessary. The **ESP may then need to analyse the traffic data of multiple users** to determine the identity and location of the specific user in question. The fact that ESPs need to look up and process traffic data is seen in some countries as an interference with the right to privacy⁵⁷, as **traffic data identifies where, when and with whom individuals have communicated**.

An ongoing debate in the field of data privacy is whether dynamic IP addresses should be considered subscriber data (like static IP addresses) or whether they fall into the category of traffic data and are thus subject to higher levels of protection. The 10 Member States covered by the Study **all require/allow retention of and access to static IP addresses, which are considered subscriber data**. The national legislation of four Member States (EE, DE, FR, SI) use the blanket term 'IP address' and make no legal distinction between static and dynamic IP addresses. Where a distinction is made, dynamic IP addresses are either considered both subscriber and traffic data (IE, PT), or traffic data only (ES, IT, PL).

Austria is the only Member State whose national legislation on non-content data retention and access contains a specific paragraph on IP addresses. Article 92 para 3 No 16 of the Austrian Telecommunications Act defines an IP address as '*a unique numerical address from an address block assigned by the Internet Assigned Numbers Authority (IANA) or a regional Internet registry to an Internet access service provider for the purpose of assigning addresses to its customers; a public IP address identifies a computer uniquely on the Internet and can be routed on the Internet.*' It further specifies that '*public IP addresses constitute access data as defined under Art. 92 para 3 No 4a Telecommunications Act. When a specific IP address is assigned to a subscriber for exclusive use for the duration of a contract, the IP address simultaneously constitutes master data as defined under Art. 92 para 3 No 3 Telecommunications Act [equivalent to subscriber data]*'. **In essence, when IP addresses are allocated exclusively to a subscriber, they qualify as subscriber data. If an IP address is assigned to multiple subscribers (dynamic IP addresses), it falls under the category of access data and is subject to higher protection under the Austrian national framework** (see section 7.1.1).

The Austrian legal act pertaining to criminal police authorities prescribes **a special procedure to access dynamic IP addresses** that requires judicial authorisation by the Public Prosecutor (judicial authorisation is not required to access static IP addresses). **It is not permitted to provide information about a dynamic IP address if its allocation would cover a large number of participants**. However, as this technical procedure is particularly common in the smartphone era, it is difficult in practice for Austrian LEAs to access non-content data related to dynamic IP addresses.

⁵⁵ IP addresses are primarily assigned using IPv4, which was released in 1978 and is the first IP version to be widely deployed. It standardises the way in which IP addresses are constructed, using a numeric 32-bit address scheme (e.g. 203.120.015), which can store over four billion unique IP addresses. However, at the beginning of the 1990s, growing demand and use of the internet meant that the supply of IPv4 addresses would quickly run out. Today, the supply is essentially exhausted and only a very limited number of addresses can be assigned using IPv4. IPv6 was developed in the 1990s to resolve the need for more internet addresses and is still in the process of being progressively deployed today. IPv6 addresses are alphanumeric and use a 128-bit scheme (e.g. 2001:0:9d35:6ab8:1c58:3a1c:a95a:b1c3), which means that IPv6 has a theoretical capacity of 340 undecillion (i.e. trillion trillion trillion or 10³⁶) unique addresses. Levin, S. L. and Schmidt, S. (2014). IPv4 to IPv6: Challenges, solutions, and lessons, Telecommunications Policy 38 (11), 1059-1068.

⁵⁶ Council of Europe (2018). *Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments*, Cybercrime Convention Committee, T-CY (2018)26.

⁵⁷ Council of Europe (2018).

Difficulties in obtaining the identity of a subscriber behind a CG NAT IP address (a dynamic IP address assigned to multiple users at the same time) **was frequently raised by stakeholders in all Member States.** Overall, **both LEA and ESP survey respondents ranked the use of dynamic IP addresses and CG NAT as the second biggest technological challenge in accessing/providing non-content data for law enforcement purposes** (Question 48 in Annex IV and Question 69 in Annex V – see section 9.2). In order for ESPs to identify the subscriber, police requests must be very precise, including the date and time (to the second) of the connection under investigation. The issue is particularly problematic in **Germany**, where, according to LEAs, ESPs rarely retain the port number that links an internet connection to a specific user, as this information is of little business value. One German LEA respondent stated that in approximately 90% of cases in which an initial suspicion of a crime becomes known to the police and in which the first and the only determination approach is the IP address (with time stamp), the investigations fail because ESPs do not retain the assignment of the IP connection. The situation is similar in **Ireland**, where ESPs do not retain port numbers, although LEAs argue that proper interpretation of the national data retention law should mean that ESPs retain port numbers.

In conclusion, while issues linked to CG NAT and dynamic IP addresses are not new (IPv6 became available in 1999), technical problems persist. The two systems, IPv4 and IPv6, continue to co-exist and ESPs find it very complex and costly to retain the information necessary to identify users via dynamic IP addresses (and do not retain them except under legal obligation).

5.3. RETENTION PERIODS FOR NON-CONTENT DATA

Differences are evident in the retention periods for non-content data:

1. between subscriber data and other types of data.
2. between Member States with and without mandatory data retention.

Table 4 presents an overview of the mandatory retention periods for law enforcement purposes (where applicable) and the retention periods for data retained by ESPs for business purposes.

Table 4: Overview of data retention periods, by type of purpose

	Business purposes		Law enforcement purposes
	Subscriber data	Traffic & location data	All types of data
AT	Timeframe of contractual relationship	Average of 3 months	x
EE	Timeframe of contractual relationship	Between 1 and 3 months	12 months
ES	Timeframe of contractual relationship	12 months (aligned with law enforcement purposes)	12 months
DE	Timeframe of contractual relationship	Maximum 6 months (but data often deleted after 7 days)	x
FR	Timeframe of contractual relationship	12 months (aligned with law enforcement purposes)	12 months
IT	Timeframe of contractual relationship	Maximum 6 months	<i>De facto</i> 72 months
IE	N/A*	N/A*	24 months for telephone communications 12 months for

	Business purposes		Law enforcement purposes
	Subscriber data	Traffic & location data	All types of data
			internet communications
PL	N/A*	N/A*	12 months
PT	Timeframe of contractual relationship	Maximum 6 months	12 months
SI	Timeframe of contractual relationship	Average of 3 months	x

*ESP stakeholders in Ireland and Poland declined to participate in the Study.

Source: Milieu elaboration, based on stakeholders' input

A clear trend across all Member States is **a longer retention period for subscriber data than for traffic, identification and location data**. As subscriber data are necessary for the service contract between clients and ESPs, these types of data are retained throughout the timeframe of the contract and, in some countries (AT, SI), several years after the contract has ended for taxation or invoice contestation purposes. In **Portugal**, as the retention period for subscriber data is not prescribed by law, LEAs can request access to this type of data within an indefinite period.

For the Member States in which there is a legal obligation to retain non-content data for law enforcement purposes (EE, ES, FR, IE, IT, PL, PT), the non-content data retention period for traffic, identification and location data is 12 months – except in Italy and Ireland. Italy and Ireland distinguish between non-content data stemming from telephone and internet communications. The former are retained for 24 months and the latter for 12 months. In Italy, an additional distinction was introduced in 2017⁵⁸, whereby non-content data must be retained for 72 months to be accessed in case of terrorism or other serious crimes (see section 6.4). In practice, however, as ESPs in Italy cannot know the types of crime data that might be requested in the future, they retain all non-content data for 72 months by default. For non-serious crimes, requests for access must be made within the time limits set by the national legislation on data retention⁵⁹.

In these Member States, ESPs can also retain traffic, identification and location data for internal purposes (e.g. commercial, marketing, invoicing). Most of the ESPs consulted declined to provide precise information on the length of time for which non-content data are used, citing business confidentiality reasons. Broadly speaking, in **France** and **Spain**, non-content data can be used for internal purposes during the same timeframe as the retention for law enforcement purposes. In **Italy** and **Portugal**, the maximum legal retention period for internal purposes is six months. **Estonian** stakeholders stated that non-content data are retained for internal purposes, on average, between one and three months. It was not possible to obtain this information for **Ireland** and **Poland**, whose ESPs declined to participate in the Study.

Retention periods for traffic, identification and location data is more complex and unclear within Member States without a legal obligation for ESPs to retain non-content data (AT, DE, SI). The main basis for data retention within these Member States is for the purpose of billing and the provision of services. Non-content data can also be retained for marketing purposes but only with the approval of the subscriber (typically via a service contract) which the subscriber can rescind at any time. As such, the retention periods can vary from one ESP to another, based on their terms of use. In **Austria**, for instance, traffic data can only be retained for a maximum of three months, which is the legal threshold for the contestation of a bill (this can go up to three years if a timely objection is raised). Subscriber, traffic, identification and location data in Austria, however, can also be retained for longer periods of time (it is unclear for how long) with the approval of the subscriber, for marketing purposes, or, in case of an ongoing investigation, until the end of the period prescribed by order of the Public Prosecutor. The situation is similar in

⁵⁸ Law No. 167/2017.

⁵⁹ Article 132 of the Data Protection Code (Legislative Decree 196/2003) and Article 3 of Legislative Decree 109/2008.

Slovenia, where non-content data can be retained up to the point where it is no longer necessary for billing or technical purposes, with a maximum of one year. Slovenian stakeholders stated that the average retention period for traffic, access and location data is around three months. Slovenian ESPs may also retain all non-content data for marketing purposes – with the approval of the subscriber – but it is unclear for how long.

The national laws of these Member States provide different retention periods for each retention purpose and legal exception, sometimes with variations by type of non-content data. As such, even the stakeholders consulted were unable to identify clear data retention periods. When requesting access to the non-content data retained by ESPs, LEAs cannot know with certainty what non-content data will be available. Stakeholders in both countries, however, stated that traffic, identification and location data are retained for three months, on average.

Box 3: Coordination initiatives in Slovenia

In **Slovenia**, coordination initiatives have been launched, with ESPs asked to list the non-content data they retain, along with the retention periods in each case, in order to provide clarity to LEAs. The intention is that LEAs will know in advance which data are likely to be available and adapt their practices accordingly (reducing the number of unsuccessful requests).

In **Germany**, the 2015 national law set a different retention period depending on the type of non-content data. Traffic data was to be retained for 10 weeks and location data for four weeks. As the national legislation is not being enforced, the situation in Germany is similar to Austria and Slovenia, where retention periods vary from one provider to another and LEAs cannot know in advance what data will be available. The Federal Commissioner for Data Protection and Freedom of Information (*BfDI*) and the Federal Network Agency (*BNetzA*) published guidelines for ESPs in 2012 that set a maximum data retention period for traffic data retained for business purposes to six months after invoicing⁶⁰. In practice, however, many German ESPs retain data for much shorter periods of time.

Based on publicly available information in their terms of reference, the largest ESPs operating in Germany, Deutsch Telekom and Vodafone, appear to retain internet traffic data for a maximum of seven days after the communication and to retain telephone traffic data for a maximum of three months after the invoice was sent to the consumer⁶¹. Telefonica retains traffic data for a maximum of six months after invoices were sent to consumers⁶². This was confirmed through interviews with German LEAs, which stated that traffic data are often retained for less than a week or up to three months for billing purposes. According to German stakeholders, location data are frequently deleted within a week, as they are not necessary for ESPs' internal purposes.

In conclusion, retention periods for non-content data retained for business purposes vary from one ESP to another within the maximum data retention periods prescribed by the national legislation - data are retained on an as-needed basis by ESPs. For the purposes of LEAs, the most reliable non-content data available within the internal databases of ESPs

⁶⁰ Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und der Bundesnetzagentur (BNetzA) (2012). *Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten*: available at: https://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenZumSpeichernVonVerkehrsdaten.pdf;jsessionid=4679E8E4892CBA54285CAC6C7C609E76.1_cid319?_blob=publicationFile&v=4.

⁶¹ Vodafone, *Datennutzung vor Vertragsschluss*, available at: <https://www.vodafone.de/unternehmen/verantwortung/datenschutz-fuer-telefon-internet.html> and Deutsch Telekom, *Verdict: The European Court of Justice overturns data storage directive*, available at: <https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/archiv-datenschutznews/news/verdict-the-european-court-of-justice-overturns-data-storage-directive-360432>.

⁶² Telefonica, *Häufige Fragen*, available at: <https://www.telefonica.de/unternehmen/datenschutz/haeufige-fragen.html>.

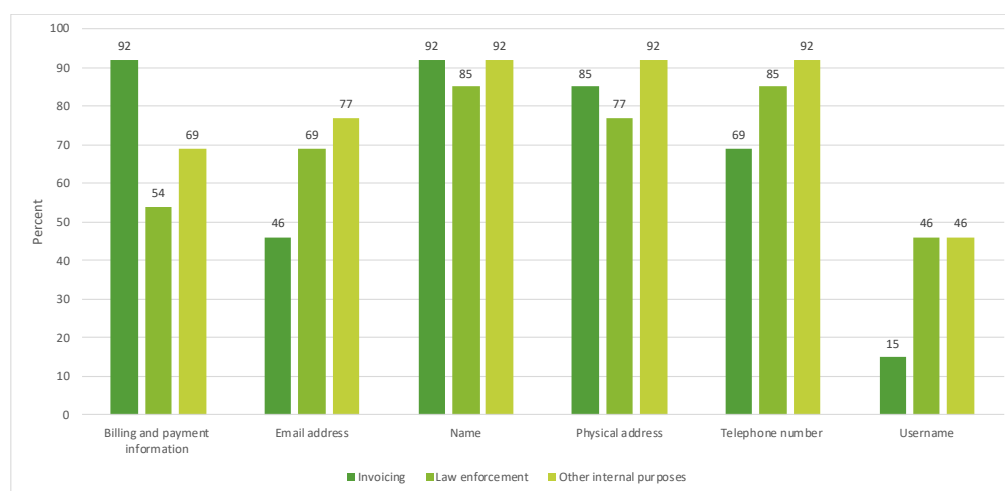
are those retained for invoicing purposes. Longer and clear data retention periods can be identified for invoicing purposes due to the legal thresholds for invoice contestation.

5.4. PURPOSES FOR WHICH NON-CONTENT DATA ARE RETAINED

Non-content data are retained by ESPs for purposes other than law enforcement. These include national security, and internal and commercial purposes, such as invoicing, marketing, network security and taxation. For the purposes of law enforcement, **the types of data retained for invoicing purposes can be more reliably requested by LEAs, as these seem to have clearer and longer retention periods than the retention periods for other internal purposes.** This is due to the legal thresholds for bill contestation, which means that the data retained for invoicing purposes will be retained at a minimum during this contestation period by all ESPs operating in the country, as opposed to the retention periods for other internal purposes, which vary from one ESP to another (see section 5.3).

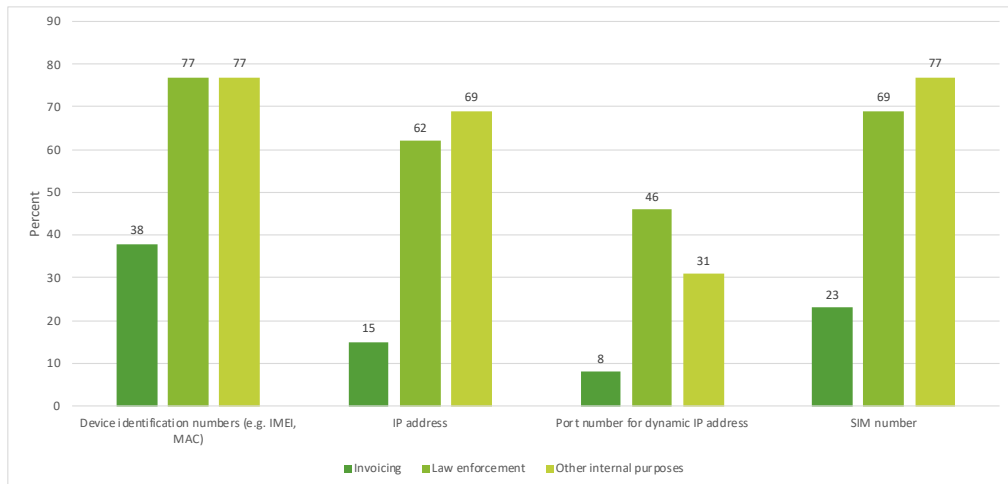
The following graphs show the percentage of ESP survey respondents who stated that they retain different types of data for one or more of the following purposes: law enforcement, invoicing or other internal purposes (commercial, marketing, network security and taxation purposes). A breakdown by each type of purpose is available in **Annex IV**.

Figure 9: Purpose for retaining subscriber data



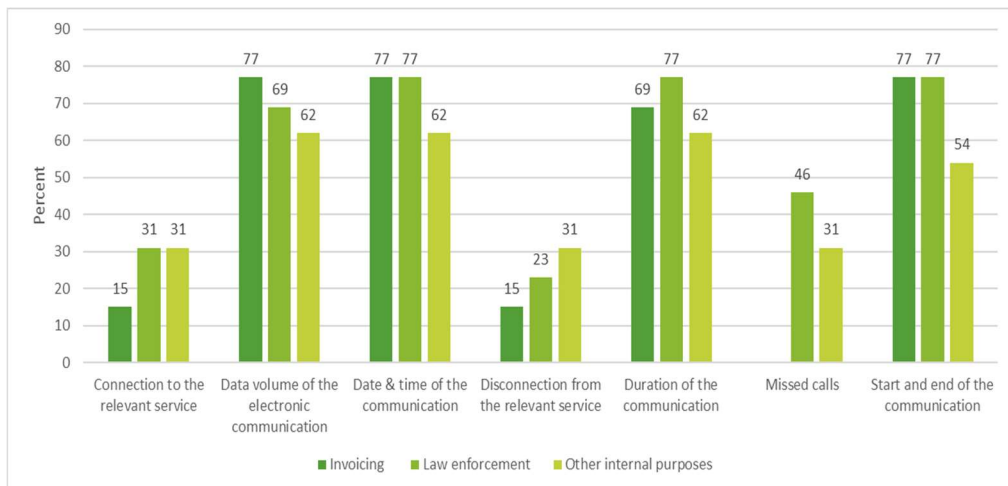
Source: Targeted survey of ESPs, Questions 11, 13, 14, 15 (N=13, multiple answers possible)

Figure 10: Purpose for retaining identification data



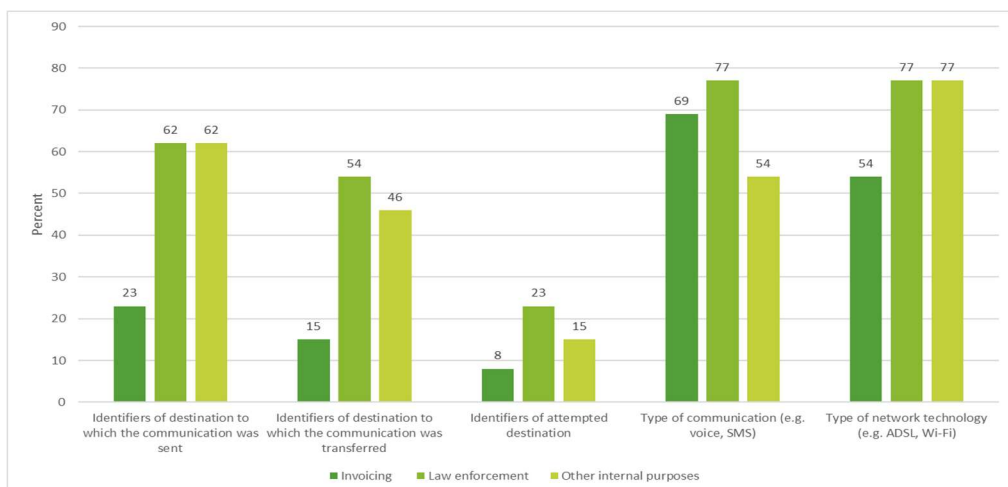
Source: Targeted survey of ESPs, Questions 11, 13, 14, 15 (N=13, multiple answers possible)

Figure 11: Purpose for retaining traffic data (1)

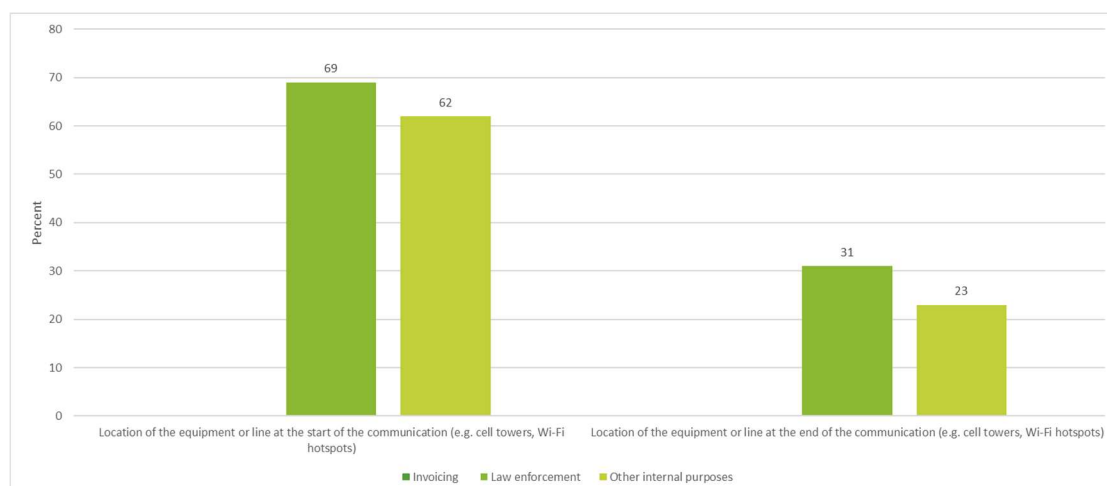


Source: Targeted survey of ESPs, Questions 11, 13, 14, 15 (N=13, multiple answers possible)

Figure 12: Purpose for retaining traffic data (2)



Source: Targeted survey of ESPs, Questions 11, 13, 14, 15 (N=13, multiple answers possible)

Figure 13: Purpose for retaining location data

Source: Targeted survey of ESPs, Questions 11, 13, 14, 15 (N=13, multiple answers possible)

Overall, all types of non-content data are retained for law enforcement purposes and at least one internal purpose. Subscriber and traffic data are retained for both law enforcement and invoicing purposes in most of the 13 ESPs that responded to the survey. On the other hand, **identification and location data are retained for invoicing purposes by less than 40% of respondents.** The port number for dynamic IP addresses, for instance, is retained by 46% of respondents **for law enforcement purposes** but only by **8% for invoicing purposes**. Port numbers are required to be retained for law enforcement purposes under the data retention laws of France, Italy, Poland, Portugal and Spain. They are not required under the Estonian data retention law and there are different interpretations of the Irish law. Among the ESP stakeholders consulted, port numbers are either not retained for internal purposes or they are retained only for short periods of time, usually for network security purposes. In the Member States without data retention obligations, LEA stakeholders indicated that port numbers are not retained long enough to be accessed for investigations and prosecutions. **None of the ESPs consulted retain location data for invoicing purposes or the number of missed calls.** This finding was confirmed through interviews with both ESPs and LEAs. Several ESP respondents stated that location data have less business value than other types of data and are therefore only retained due to the mandatory obligation. The experience of LEAs from the Member States without mandatory data retention also show that the types of data not retained for invoicing purposes must be requested within less than three months if it is to be available for use in criminal investigations.

5.5. STORAGE AND SECURITY REQUIREMENTS

Overall, the security requirements imposed on ESPs for storing the retained non-content data are similar in all 10 Member States covered under the scope of the Study.

Table 5: Overview of security requirements for the storage of data

MS	General security requirements linked to the GDPR	Localisation requirement	Separate storage of data retained for business and law enforcement purposes
AT	✓	x	x
DE	✓	✓ (National)	✓
EE	✓	✓ (EU)	x
ES	✓	x	x

MS	General security requirements linked to the GDPR	Localisation requirement	Separate storage of data retained for business and law enforcement purposes
FR	✓	x	x
IE	✓	x	x
IT	✓	x	✓
PL	✓	x	x
PT	✓	x	✓
SI	✓	x	x

Source: Milieu elaboration based on desk research and stakeholders' input

The national laws of all Member States include **a general reference to ensuring the security, protection and integrity of the non-content data retained by ESPs**. This entails taking all measures necessary to **prevent any use of the data not foreseen by the law**. ESPs must ensure that no damage, loss or alteration occurs to the data and that only authorised personnel are involved in their processing. These requirements are **in line with Article 32 of the GDPR** on the security of personal data. ESPs must also ensure that access requests made by LEAs can be met without delay and that the **destruction of the data occurs upon the expiry of the prescribed retention period**. The legislation of **most Member States remains technologically neutral** and does not describe exact security measures. In **Germany** and in **Italy**, however, the German Federal Networks Agency and the Italian Data Protection Authority, have published catalogues that specify the legal requirements for the technical aspects of data management and security⁶³.

The national laws of some Member States specify **additional requirements**. In **Estonia** and **Germany**, the storage of non-content data is subject to data localisation requirements - in Estonia, the non-content data must be retained within the EU, while in Germany, the non-content data must be retained within the national territory. In **Germany**, **Italy** and **Portugal**, non-content data retained for law enforcement purposes must be retained separately from non-content data retained for other technical/commercial purposes.

In practice, the most common security measures implemented by ESPs (91% of the 13 survey respondents, Question 52 in **Annex V**) **are strict access controls that limit the personnel who can access the database**. One ESP stated that only three people in the entire company have access to the database containing the non-content data retained for law enforcement. In addition, several ESPs use biometric technology to control access to the database. In **France**, there is no legal obligation to retain law enforcement data separately from business data. However, several French ESPs stated that location data are stored separately from other data to prevent easy linkage between a communication and its geolocation. Although French ESPs can use the data retained for law enforcement purposes for internal purposes, when data are used commercially, they must be pseudonymised. **Many ESPs (64%) also stated that the non-content data are encrypted although there is no legal obligation to do so.**

ESPs have internal audits and controls in place to ensure continuous high security standards and are occasionally subject to external controls from DPAs (although these controls are linked to ensuring compliance with the GDPR rather than data retention). The DPAs interviewed for the Study reported that security breaches are rare and ESPs take all adequate measures to ensure the security and integrity of the retained data.

67% of the ESP survey respondents stated that the security requirements were more stringent for law enforcement purposes than for business purposes, while 33% stated that the requirements were the same (ESP survey question 62 in **Annex V**). The main reasons for more stringent requirements are separate storage for law

⁶³ Italy: Security of telephone and telematic traffic data - 17 January 2008 [1482111] and Measures regarding the conservation of telephone and telematic traffic data for the purpose of ascertaining and suppressing crimes - September 19, 2007 [1442463]. Germany: Catalogue of technical arrangements and other measures to implement the law on storage obligation and maximum storage period for traffic data from 10.12.2015 (BGBl. I S. 2218).

enforcement than for business purposes (IT, PT), stringent access controls, and the need for regular data backups in case of technical failure. For Member States in which there is no legal obligation to retain non-content data, some ESPs nevertheless stated that the requirements were more stringent, citing the storage requirements linked to data preservation (quick freeze) requests.

Many ESPs pointed to the high additional costs incurred from the retention of data for law enforcement purposes - even without mandatory data retention. 42% of survey respondents stated that they incur major additional costs and 33% substantial additional costs (ESP survey question 26 in Annex V). The main reason for these costs is the infrastructure, tools and IT equipment necessary to ensure secure storage of data and timely responses to LEA requests. 50% of ESP respondents also mentioned staff costs (see section 7.2.1). Staff members responsible for dealing with requests from LEAs need training on data security and processing requests to ensure that the data are only transferred to legitimate LEAs using the correct legal basis. Only ESPs in **Austria** and **France** are partially reimbursed for these costs. The ESPs highlighted the need for cost recovery mechanisms, arguing that they perform a public interest mission that requires high investment with no business return.

5.6. KEY FINDINGS

- The types of non-content data included under the data retention obligation are broadly the same across Member States with data retention laws. All ESPs consulted also retain all types of non-content data for at least one internal purpose (e.g. business, commercial, invoicing, marketing, network security).
- Non-content data can be classified into three groups: subscriber, traffic and location data. In some Member States, the conditions for accessing data vary depending on the classification of data requested. While there are some data points that are always considered subscriber or traffic data in all Member States, there is no consensus on the classification of IP address, port number for dynamic IP addresses, and SIM and device identification numbers. Some Member States consider these subscriber data, while others treat them as traffic data. The Irish legislation does not categorise non-content data. For clarity, these data points are referred to as identification data within the Study.
- The mandatory data retention period for law enforcement purposes is 12 months, except in Ireland (12 months for internet data, 24 months for telephone data) and Italy (*de facto* 72 months). Retention periods for data retained for business purposes are unclear. Some Member States (DE, IT, PT) set a maximum retention period of six months for business data, while others use one year (FR). Within these limits, the periods vary from one operator to another, depending on their internal needs. Data retained for invoicing purposes generally have clearer and longer retention periods due to legal thresholds for invoice contestation (on average three months). For the purposes of LEAs, the most reliable non-content data available within the internal databases of ESPs are those retained for invoicing purposes. Subscriber data are usually retained throughout the timeframe of the contract between clients and ESPs (as they are necessary for the subscription). This means that, in practice, subscriber data are often retained for several years.
- Most traffic data are retained for invoicing purposes. Identification and location data are generally not retained for invoicing, as they have limited business value for ESPs. These data points are thus retained for much shorter periods of time – in Germany, for example, they are deleted within seven days.
- IP addresses, particularly dynamic IP addresses assigned to multiple users at the time through CG NAT, stand out as the most challenging type of data to obtain for LEAs. Port numbers are not retained in Estonia, Germany or Ireland, and even in

Member States where they are retained, LEAs need very precise time stamps for ESPs to identify the user behind a connection.

- Security requirements for the storage of data are broadly the same across Member States, as they related to GDPR requirements and remain technologically neutral. Some Member States (IT, PT, DE) require data retained for law enforcement purposes to be stored separately from data stored for business purposes. Other Member States have data localisation requirements - in Estonia, data must be retained in the EU, while in Germany, data must be stored on the national territory. Overall, ESPs have invested heavily in infrastructure, IT equipment and staff training in order to meet these requirements and ensure the security of data. The majority of ESPs consulted highlighted the high costs involved, which are not systematically reimbursed.

6. ACCESS TO AND USE OF NON-CONTENT DATA BY LAW ENFORCEMENT AUTHORITIES

This section provides an overview of how frequently non-content data are accessed and used by LEAs (section 6.1), the types of data requested (section 6.2) and their average age (section 6.3), along with the types of crimes for which data are used (section 6.4). Section 6.5 focuses on the extent to which non-content data advance criminal investigations and proceedings. Section 6.6 presents the key findings.

The analysis in this section is based on the national-level legal research, complemented and verified through the targeted surveys and follow-up interviews with stakeholders.

6.1. DIMENSIONS OF THE ISSUE

This section looks at the frequency with which non-content data are requested and used by LEAs in the 10 Member States covered by the Study. However, given the limited availability of statistics and the variety of methodologies used for recording requests, only an incomplete view of the situation is possible. LEAs do not keep reliable or precise records of the number of requests sent, ESPs have no reporting obligations, and many governments do not disclose statistics due to the sensitivity of the issue. The following sub-sections compile the different types of information that could be gathered: section 6.1.1 gives an overview of the statistics available for each Member State, section 6.1.2 presents the views of the LEAs consulted and section 6.1.3 focuses on the frequency of and reasons for unsuccessful requests.

6.1.1. Statistics on the number of requests

Table 6 presents the available information on the number of requests for non-content data in each Member State. It was not possible to obtain official data for all Member States and the numbers come, variously, from official government statistics, police reports and ESPs' transparency reports. The numbers for some Member States reflect the requests received by a single ESP and there are variations in the way requests are recorded across countries. The comment column describes what each number represents and how it should be interpreted.

Table 6: Overview of statistics available on non-content data requests

MS	Year	Number of requests	Source	Comments
AT	2017	5,527	Official statistics ⁶⁴	These numbers only include requests for traffic data (not subscriber data). Numbers are based on the number of warrants sent out to ESPs (one warrant can cover multiple individuals or multiple devices; one individual can be covered by multiple warrants).
	2018	5,899		
DE	2015	26,265	Official statistics ⁶⁵	These numbers only include requests for traffic data (not subscriber data). Numbers are based on the number of warrants sent out to ESPs (one warrant can cover multiple individuals or
	2016	25,640		
	2017	22,929		

⁶⁴ Bundesministerium Verfassung, Reformen, Deregulierung und Justiz, *Sicherheitsberichte*, available at: <https://www.justiz.gv.at/home/justiz/daten-und-fakten/berichte/sicherheitsberichte~2c94848525f84a630132fdbd2cc85c91.de.html>.

⁶⁵ Bundesamt für Justiz, *Telekommunikationsüberwachung*, available at: <https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html>.

MS	Year	Number of requests	Source	Comments
EE	2016	5,100	Statistics from the Consumer Protection and Technical Regulatory Authority	multiple devices; one individual can be covered by multiple warrants).
	2017	5,780		The numbers do not show the full picture. The Consumer Protection and Technical Regulatory Authority disclosed statistics for the past three years, which aggregate the number of requests received by ESPs. However, as there is no obligation for ESPs to submit such statistics to the Authority, it is unclear whether all relevant ESPs provided statistics, and there may be inconsistencies in the way the number of requests are recorded across ESPs. The numbers provided by ESPs may not differentiate between requests from LEAs and non-law enforcement authorities for purposes which are excluded from the study (e.g. civil proceedings). These statistics should therefore not be considered official government statistics.
	2018	4,151		
ES	2017	53,751	Vodafone Transparency report ⁶⁶	This number only shows the requests sent to one operator. The number is based on the number of warrants received (one warrant can cover multiple individuals or multiple devices; one individual can be covered by multiple warrants).
FR	2017	2,000,000	Official government press release ⁶⁷	The French state does not allow the disclosure of precise statistics. However, an official press release states that some two million requests for data go through the automated national system (PNIJ) each year. French LEAs must submit a separate request per target and type of data (several separate requests can target one individual).
IE	2015	20,540	Department of Justice statistics ⁶⁸	Statistics obtained by an Irish newspaper following a Freedom of Information (FOI) appeal. No precise information is provided on how requests are recorded.
	2016	17,706		
	2017	16,001		
IT	2017	131,067	Vodafone transparency report ⁶⁹	This number only shows the requests sent to one operator. The number is based on the number of warrants received (one warrant can cover multiple individuals or multiple

⁶⁶ Vodafone Group Plc (2017). Country by Country Disclosure of Law Enforcement Assistance Demands 2016-17, available at: https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/vodafone_dr_law_enforcement_disclosure_country_demands_2016-7.pdf.

⁶⁷ Ministère de la Justice (2017). *La plateforme nationale des interceptions judiciaires en chiffres*, Communiqué de presse, available at: <http://www.presse.justice.gouv.fr/communiqués-de-presse-10095/archives-des-communicés-de-2017-12858/la-plateforme-nationale-des-interceptions-judiciaires-en-chiffres-30997.html>

⁶⁸ O'Keeffe, C. (2018). *Personal data shared 92,000 times to State agencies by phone and internet firms*, The Irish Examiner, available at: <https://www.irishexaminer.com/breakingnews/ireland/personal-data-shared-92000-times-to-state-agencies-by-phone-and-internet-firms-891004.html>

⁶⁹ Vodafone Group Plc (2017).

MS	Year	Number of requests	Source	Comments
	2018	1,198,576	Survey response from a large ESP operating in Italy	devices; one individual can be covered by multiple warrants)
	2019	1,467,178		These numbers only show the requests sent to one operator. Requests are recorded as one request per target and per type of data (several separate requests can be targeted towards one individual).
	No statistics available – the disclosure of statistics on the number of requests is unlawful			
PL				
PT	2017	33,914	Vodafone transparency report ⁷⁰	This number only shows the requests sent to one operator. The number is based on the number of warrants received (one warrant can cover multiple individuals or multiple devices; one individual can be covered by multiple warrants).
SI	2017	437	Official police annual report ⁷¹	These numbers only represent requests made by the police for traffic data (they do not include requests for subscriber data). In addition, requests can also be made from investigative judges and public prosecutors.
	2018	486		
	2019	393		

Note: The official German statistics for 2018 were excluded, as five of the 16 German Länder (states) are missing from the report and the numbers are not comparable with previous years.

Source: Milieu elaboration, based on desk research and stakeholders' input

It is difficult to extrapolate total numbers of requests based on the statistics available in the transparency reports of ESPs. Any such extrapolation would have to be based on the market share of the ESP, yet the assumption that the number of requests received by an ESP is proportional to its market share is unreliable, as this will depend on the overall structure of the national telecommunications market and the presence of smaller operators. Some stakeholders highlighted that criminals are more likely to use smaller, less established operators, which have less developed infrastructure to respond to police requests in a timely manner. These smaller operators may therefore receive a disproportionate number of requests. In addition, there is no information on how many of the requests involve fixed versus mobile communications, for which ESPs have different market shares. Several LEA respondents provided statistics on the average number of requests they send out on a yearly basis but these numbers are not comparable and were thus excluded (some numbers represent the requests made by a single officer while others represent those of units or sub-units).

It can be concluded that **cross-country comparisons are meaningless without a homogenous reporting system**. Requests for non-content data are recorded in a variety of ways and the methodology used is often not clearly explained. Requests can be recorded as: one request per individual or identification number, one request per data point, or one request per warrant (which can cover multiple individuals or devices). As such, **statistics do not depict the total number of individuals affected by non-content data disclosures**. One individual can often be targeted by multiple separate requests - for different investigations, by different authorities, or because the individual possesses several telephone numbers or electronic devices that produce different identifiers (yet relate to the same person). In Slovenia in 2019, for example, the police sent out 393 requests for traffic data to ESPs, targeting 199 individuals. The official statistics of the

⁷⁰ Vodafone Group Plc (2017).

⁷¹ Ministrstvo za Notranje Zadeve, Policija, Služba generalnega direktorja policije (2019), *Letno poročilo o delu policije 2019*, available at: https://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2019_popr.pdf.

Austrian and German governments and the Slovenian police only show the requests for traffic data, while the numbers for other countries include requests for all types of data, including subscriber data. The numbers for Germany could be significantly higher, as there is an automated system for LEAs to request subscriber data, greatly facilitating this type of request⁷².

Although the time period covered (two-three years) is too short to draw longer-term conclusions, it be observed that **while some Member States have seen an increase in the number of requests in recent years, others have seen a decrease.**

Statistics and stakeholder input from **Austria, France, Italy** and **Spain** pointed towards a general perception of **increasing requests**. This can in part be linked to the recent introduction of automated request systems (e.g. France) and the increase in criminal offences committed via electronic means. Interestingly, the number of requests for traffic data sent by Austrian LEAs increased by 6.7% between 2017 and 2018 despite the lack of mandatory data retention.

In **Estonia, Germany, Ireland** and **Slovenia**, however, requests for non-content data appear to have decreased. In **Ireland**, the number of requests has decreased at an annual rate of 12% since 2015. One possible explanation for this decrease is the ongoing debate over the validity of the national data retention law since the invalidation of the DRD by the CJEU in 2014. Irish law enforcement interviewees highlighted that they are not using the legislative scheme to the full extent, to avoid challenges to the admissibility of evidence. Challenges to the current legal framework for data retention in **Estonia** could also explain the decrease in requests between 2017 and 2018. In **Germany** and **Slovenia**, stakeholders stated that they have perceived a decrease in the number of requests in recent years. The official statistics of the German Federal Office for Justice show that the number of requests for traffic data decreased at an annual rate of 7% since 2015, coinciding with changes in the national framework.

6.1.2. Frequency of use of non-content data

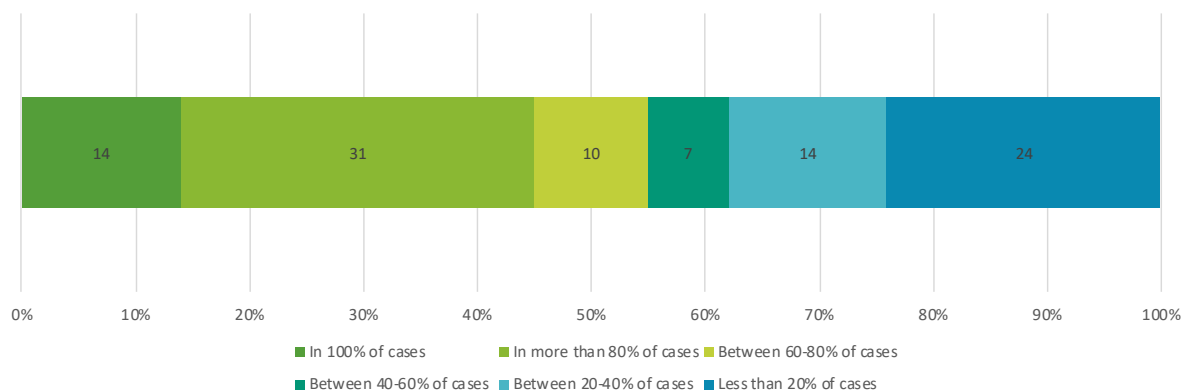
Given the limited availability and reliability of statistics, the LEAs consulted were also asked to estimate how frequently they request and use non-content data in the course of criminal investigations and proceedings. **Based on their assessment, non-content data appears to be used frequently across all Member States.** Over 50% of respondents stated that they have requested data in at least 60% of cases over the last two years (see Figure 14 below). There are no notable differences between Member States in terms of the frequency of requests reported by respondents, although French LEAs reported more frequent use of non-content data than other Member States, with all six French respondents having requested non-content data in over 80% of cases in recent years. Respondents from Slovenia reported the least frequent use of non-content data, with three out of four Slovenian respondents having requested data in less than 20% of cases over the past two years. Differences in the frequency of use of non-content data are primarily linked to the type of authority (police vs. public prosecutor) and the types of crimes investigated. Among the sample of LEAs consulted, police authorities request non-content data more frequently than public prosecutors – 65% of police respondents request data in at least 60% of cases compared to 36% of public prosecutors (see Figure 15 below). Interviews also highlighted that specialised authorities (e.g. focusing on environmental

⁷² Based on Article 112 TKG, the Federal Networks Agency has put in place an automated information procedure (the AVV - *Automatisiertes Auskunftsverfahren*), which consists of a secure IT platform that enables LEAs and other authorised bodies to query customer data such as name, address or phone number around the clock. The Federal Networks Agency's IT system is based on the databases of all participating ESPs (116 companies in total are obliged to participate). The system automatically forwards the requests to the telecommunications companies as a query, merges the answers obtained and returns the information to the authorised body as a result.

Bundesnetzagentur, *Automatisiertes Auskunftsverfahren* (§ 112 TKG). Available at: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/AutomatisiertesAuskunftsverfahren/Automatisiertesauskunftsverfahren-node.html.

crimes or revenue offences) request non-content data to a lesser extent than police and public prosecutors. LEAs investigating cybercrimes, paedophilia and fraud reported a higher need to request non-content than those investigating other types of crimes.

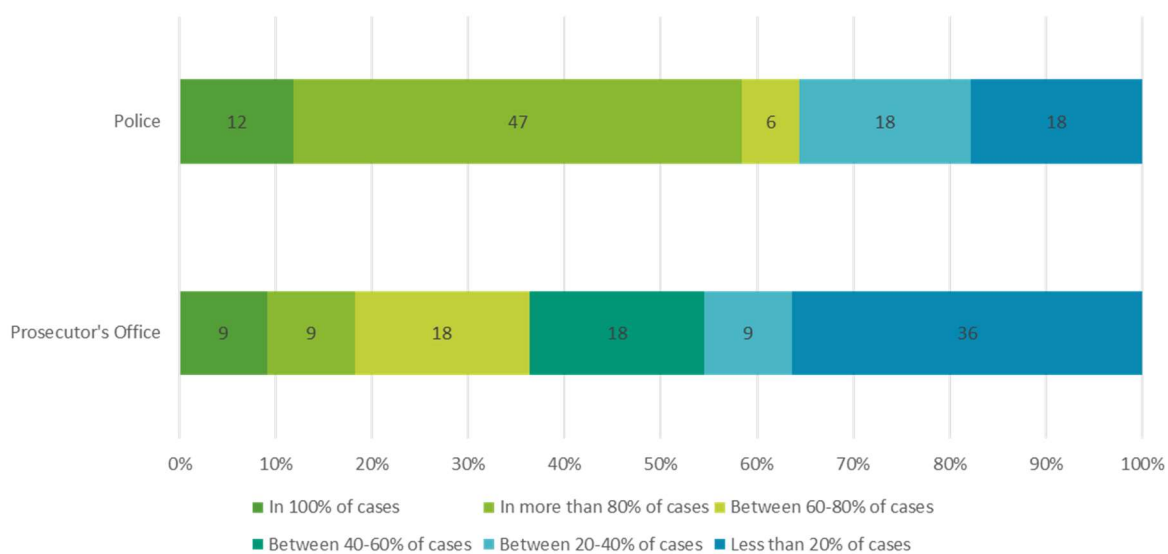
Figure 14: Frequency of access requests to non-content data in the course of a criminal investigation/prosecution, 2018 and 2019



Note: The figure shows only police and public prosecutor responses. Other types of respondents were excluded as they either do not request non-content data (not investigative or prosecution bodies) or do so only rarely.

Source: Targeted survey of LEAs, Question 14 (N=29)

Figure 15: Comparison of the frequency of access requests to non-content data in the course of a criminal investigation/prosecution, 2018 and 2019, by type of authority (police vs. public prosecutors)



Note: The figure shows only police and public prosecutor responses. Other types of respondents were excluded as they either do not request non-content data (not investigative or prosecution bodies) or do so only rarely. Number respondents per type of authority: police - 17; public prosecutors - 11.

Source: Survey of LEAs, Question 14 (N=29)

6.1.3. Unsuccessful requests

The overall impression from the available statistics and stakeholders' responses is that non-content data are frequently requested and used during criminal investigations and proceedings. However, it is also interesting to examine how often requests to access data

are unsuccessful. Stakeholder consultation highlighted that LEAs and ESPs have different views of what constitutes an unsuccessful request. For LEAs, unsuccessful requests are requests for which none or only part of the data requested are disclosed and usable. ESPs, by contrast, often consider all processed requests as successful, regardless of whether or not data were provided to LEAs. For many ESPs, an unsuccessful request is a request they were unable to process internally.

Aside from the internal reasons that may prevent an ESP from processing a request (e.g. technical failures, insufficient human resources), a variety of structural reasons can underpin an unsuccessful request where the full amount of data was not disclosed, for example:

- ESP no longer retains the requested non-content data;
- ESP can only provide part of the non-content data requested due to the unavailability of some of the data or technical issues;
- ESP refuses to disclose data due to procedural requirements (e.g. incorrect legal basis used);
- Request sent to the wrong ESP;
- Data obtained cannot be read due to technical difficulties.

The majority of stakeholders consulted (both LEAs and ESPs) stated that requests for non-content data were rarely unsuccessful. 56% of LEA respondents and 92% of ESP respondents stated that requests are unsuccessful in less than 20% of cases (LEA survey question 36 in Annex IV and ESP survey question 53 in Annex V). Although the survey question specified that unsuccessful requests should be understood as requests that did not result in the disclosure of the full amount of data requested by LEAs, the difference in the reported success rate between LEAs and ESPs may be due to different interpretations of an unsuccessful request. 68% of both LEA and ESP respondents cite the non-content data no longer retained as the main reason for an unsuccessful request.

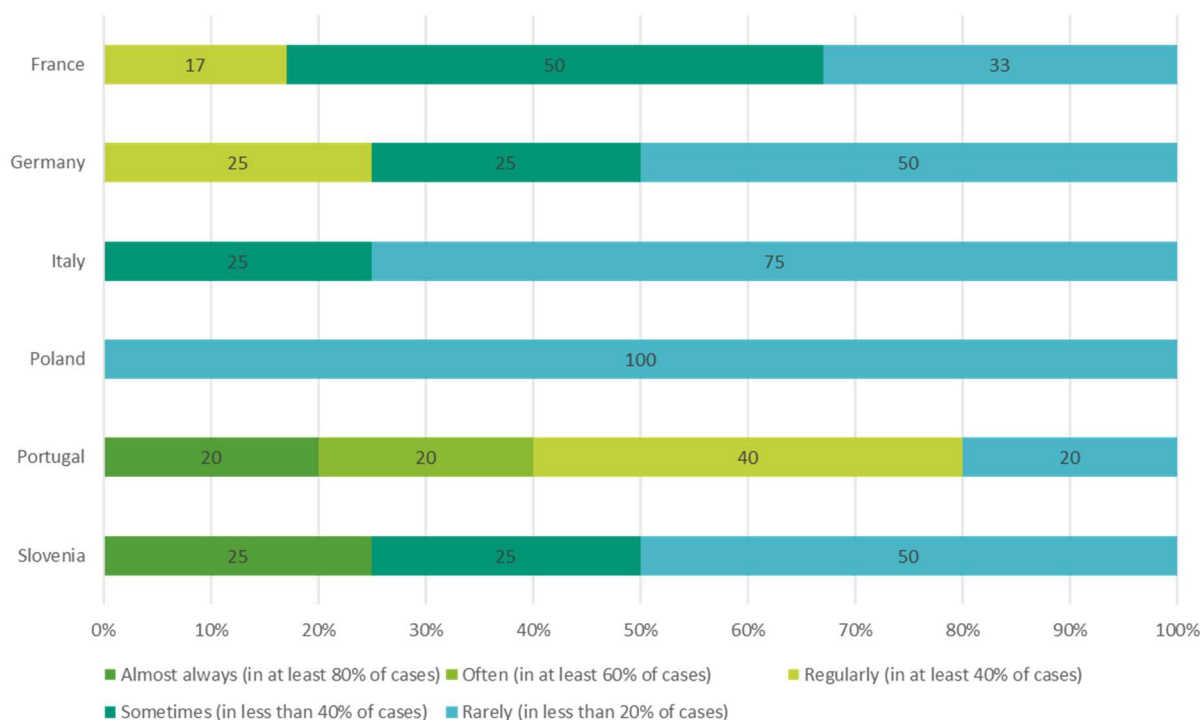
The tendency seems to be confirmed by the official statistics available, although the number of unsuccessful requests in Germany increased substantially from 2017 to 2018. The statistics from the **German** Federal Office for Justice show that 21% of requests for traffic data sent in 2017 were unsuccessful due to partial or complete unavailability of non-content data (18,014 successful requests for traffic data in Germany, which led to 15,361 procedures). In 2018, the percentage of unsuccessful requests due to the absence of data increased to 42% (five Länder are missing from the 2018 statistics). In **Estonia**, the statistics from the Consumer Protection and Technical Regulatory Authority show that 37% of requests were unsuccessful in 2018.

Among LEA survey respondents, only slight variations can be detected between respondents from Member States with and without mandatory data retention, with the latter reporting slightly higher rates of unsuccessful requests (see Figure 16 below). Many respondents from these countries (AT, DE, SI) explained that, overall, they have low levels of unsuccessful requests, as they simply do not request data when they believe that it will no longer be retained by ESPs. As an illustrative example, a German officer explained that they have managed to adapt procedures and are generally able to obtain judicial approval and access non-content data within one week.

The most striking variation is evident in Portugal, where 80% of LEA respondents stated that their requests are unsuccessful in at least 40% of cases (see Figure 16). Follow-up interviews revealed that the high rates of unsuccessful requests are due to differences in the interpretation of the law between ESPs and LEAs. This is mostly due to the existence of different frameworks for retention of and access to data – one pertaining to access to business data and the other to data retained for law enforcement. Stakeholders reported that where LEAs ask ESPs for data beyond six months (the maximum retention for business purposes), ESPs refuse to transfer the data, arguing that they were retained for business purposes and are thus deleted – despite the fact that Portugal has a mandatory

data retention scheme of one year. Although the data retention law in Portugal is still in force, there is no arbitration between ESPs and LEAs since 2017, as the DPA is no longer settling disputes nor sanctioning ESPs for failing to retain data for law enforcement purposes (it argues that the national data retention law is incompatible with CJEU case-law). There is also disagreement over the classification of identification data, which are considered subscriber data by public prosecutors (which do not require judicial authorisation), but treated as traffic data by ESPs (requiring judicial authorisation), further contributing to higher numbers of unsuccessful requests.

Figure 16: Frequency of unsuccessful requests for non-content data reported by LEA survey respondents



Number of respondents per country: Austria and Estonia were excluded as there were only 1 and 2 respondents, respectively; France - 6; Germany - 4; Italy - 4; Poland - 3; Portugal - 5; Slovenia - 4.

Source: Targeted survey of LEAs, question 36 (N=29)

Most of the negative replies from ESPs stemming from unavailability of the data at the time of the request come from LEAs investigating organised crime, corruption, fraud and money laundering. For these types of crime, investigations often take a long time (even years) to be completed, which means that non-content data can be deleted even despite comparatively long retention periods.

6.2. TYPES OF NON-CONTENT DATA REQUESTS

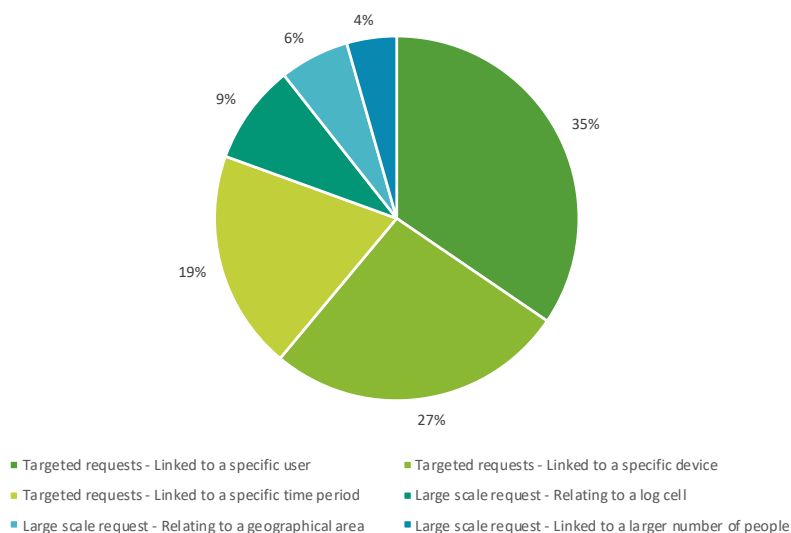
This section focuses on the types of requests sent by LEAs, notably:

1. frequency and context of targeted vs. large-scale requests;
2. types of non-content data most frequently requested.

6.2.1. Targeted versus large-scale requests

Requests for non-content data can be either targeted or large-scale. Targeted requests are requests for non-content data associated with a specific person, a specific device or a specific period of time. For example, LEAs may request the call records of a specific suspect using their name or they may seek to identify the owner of a specific phone number or device. Requests can also be large-scale, meaning that they do not target a specific person/device but, rather, relate to the logs of a cell tower or a geographical area, thus disclosing non-content data of multiple individuals simultaneously. Interviews with all types of stakeholders showed that **the majority of requests are targeted rather than large-scale**. Both LEAs and ESPs were asked for an estimate of the proportion of targeted versus large-scale requests in 2019 (LEA survey question 17 in Annex IV and ESP survey question 46 in Annex V). Responses from both types of stakeholders suggest an average of 80% targeted requests and 20% large-scale requests. In addition, the official statistics for Austria show that, in 2018, the majority (71%) of court-approved requests for traffic data targeted a named suspect. During the interview phase, respondents explained that **large-scale requests are limited and only occur in urgent situations**, such as a terrorist attack or a missing person. Large-scale requests most often pertain to the data contained within a cell tower at a specific point in time. In those situations, LEAs will request the numbers of all telephones connected to a cell tower at a certain time. These are generally cases where LEAs do not know what they are looking for. For example, the police only know that the suspects have fled in a specific direction and attempt to follow them through cell towers. However, **large-scale requests are limited by practical considerations** and are formulated in a limited way in terms of time or area. This is due to the considerable amount of data that results from such requests and the difficulty in finding relevant evidence within broad datasets. In dense urban areas, their utility is particularly limited.

Figure 17: Most frequent practice to request non-content data, LEA and ESPs combined



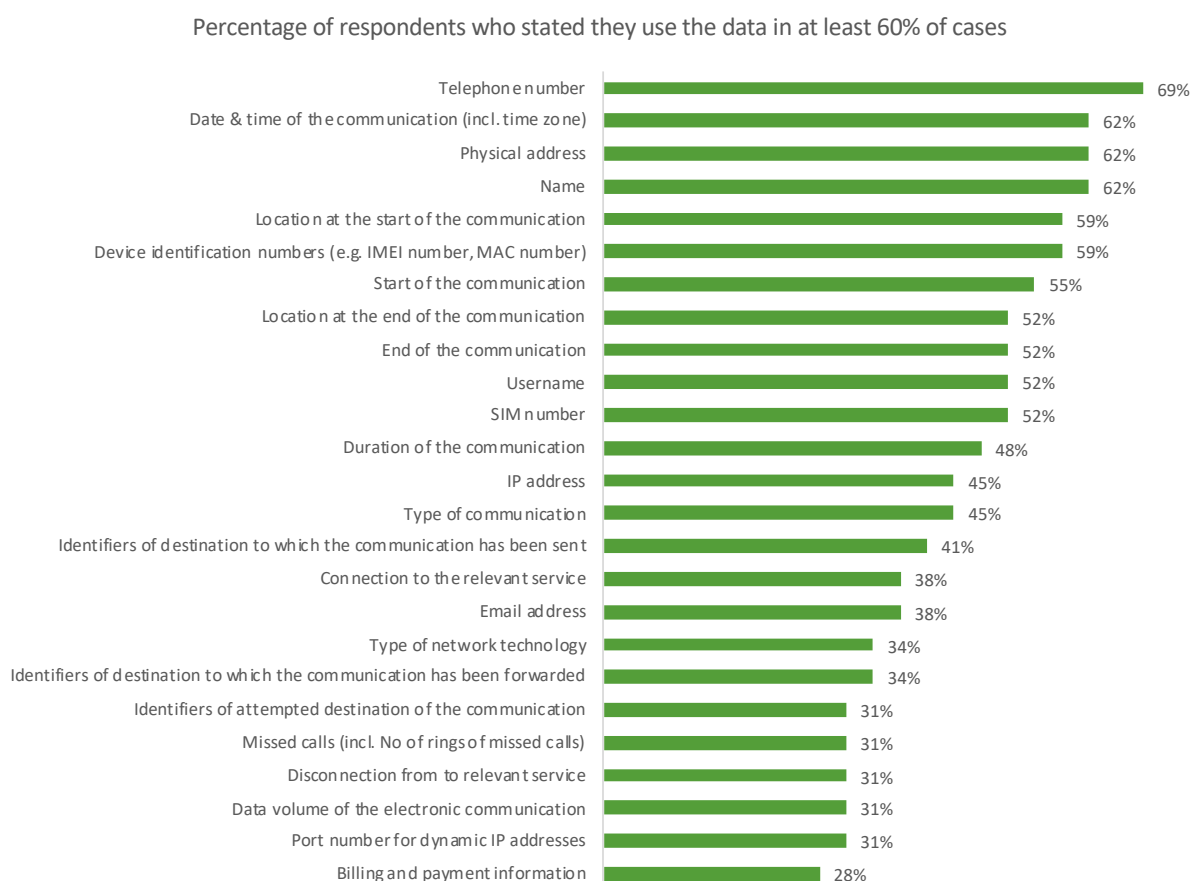
Source: LEAs survey question 17, ESPs survey question 46 (N=47)

6.2.2. Types of data most frequently requested

A large majority of LEA stakeholders reported making use of all types of data. The non-content data most frequently requested are telephone number, physical address, date and time of the communication, and location of the equipment or line at start of communication. Figure 18 shows that 62% of respondents use the physical address, name and date and time of a communication in at least 60% of cases. Although these figures represent the personal assessments of survey respondents, they are in line with the

information obtained in follow-up interviews with ESPs and national regulatory authorities. Overall, subscriber data appear to be most frequently requested by LEAs, followed by traffic and location data. Several stakeholders highlighted that **non-content data are usually requested as a package**. For example, in the course of a single investigation, LEAs will often request both the name and address of a person behind a specific identification number, or the call records of a suspect, which group data on the dates, times, duration and numbers called. Traffic and location data are typically requested in combination, e.g. the location of the equipment at a specific point in time.

Figure 18: Share of LEAs using different type of data in over 60% of cases



Note: The figure shows police, public prosecutor and investigative judge responses. Other types of respondents were excluded as they either do not request non-content data (not investigative or prosecution bodies) or do so only rarely.

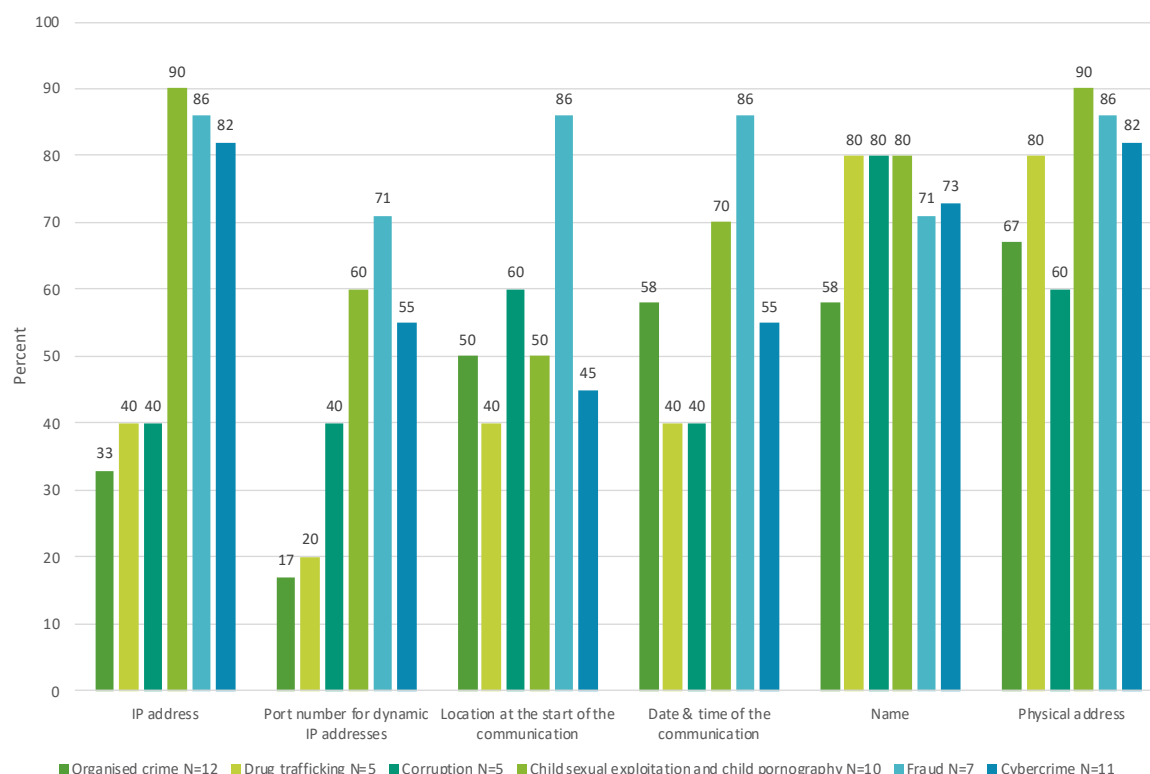
Source: Survey of LEAs, question 22 (N=29)

However, there are two important points to note, **(1) data points less frequently requested may nevertheless be of great importance in certain investigations, and (2) some types of data are less frequently requested in some Member States, as they are generally not retained by ESPs**. This is notably the case for port numbers for dynamic IP addresses, which were requested by only 11% of respondents from Member States without mandatory data retention in at least 60% of cases. This percentage increases to 40% of respondents in those Member States with mandatory data retention (see Figure 36: Number of requests sent to OTTs per 100 000 population in 2018 and in Jan-June 2019 in Annex III).

Survey responses and interviews highlighted that non-content data are used in the investigation of all types of serious crimes. **Subscriber and traffic data appear to be**

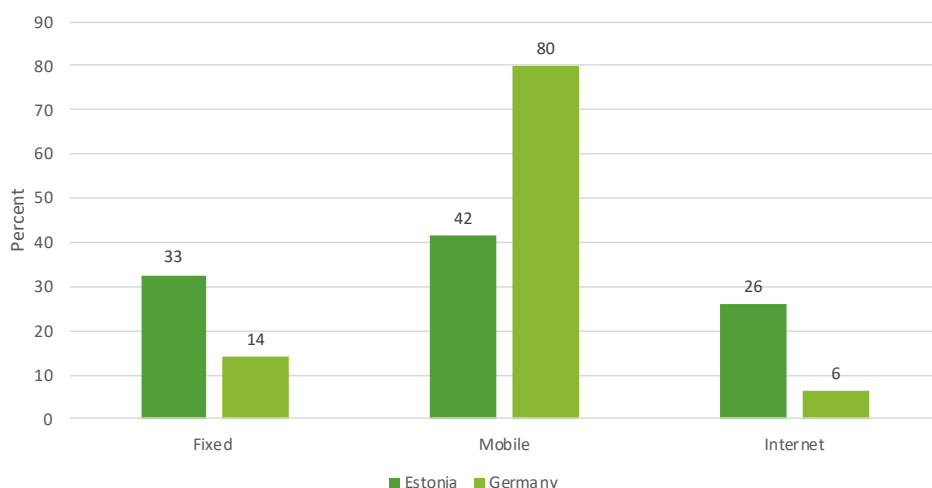
requested at a similar frequency for different types of crimes. Unsurprisingly, however, respondents who investigate crimes committed via electronic means (fraud, paedophilia, cybercrime) reported higher use of non-content data and higher use of certain types of data, such as IP addresses. Figure 19 shows that IP addresses are requested by 90% of respondents who investigate child sexual exploitation and child pornography in at least 60% of cases, while the same is true of 40% of respondents investigating drug trafficking. Name and physical address are requested at a similar frequency for all types of crimes shown in Figure 19.

Figure 19: Percentage of respondents using the type of data in at least 60% of cases, by type of crime



Source: Survey of LEAs, question 22 (N=29)

It is interesting to consider the types of communication for which non-content data are most frequently requested, whether fixed-line, mobile or internet communication. Statistics pertaining to this, however, are only available for Estonia and Germany for 2018. In both countries, the proportion of requests for mobile communication data is the largest (EE 42%; DE 80%), followed by fixed communication data (EE 33%; DE 14%) and internet communication data (EE 26%; DE 6%).

Figure 20: Percentage of requests, by type of communication in Estonia and Germany, 2018

Source: Milieu elaboration from data provided by the Estonian Consumer Protection and Technical Regulatory Authority and the official statistics of the German Federal Office for Justice

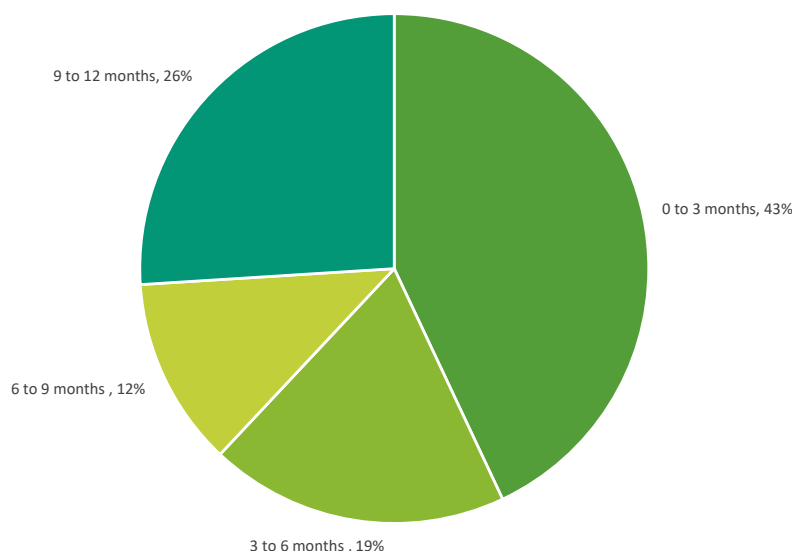
6.3. AVERAGE AGE OF REQUESTED NON-CONTENT DATA

This section focuses on the average age of the non-content data requested by LEAs. The average age of data is based on the time period between which the data are generated and retained by ESPs (e.g. when the communication took place) up to the point that they are requested by LEAs.

It is difficult to obtain a consolidated view of the average age of the data requested by LEAs due to the limited statistics available. Based on the results from the LEAs survey, respondents from Member States with mandatory data retention stated that they most frequently request data up to one year old, which corresponds to the maximum data retention period prescribed by the law. Similarly, the majority of respondents from Member States without mandatory data retention stated that they most frequently request data three to six months old. German respondents most frequently request data within one week of the communication. Again, this corresponds to the average period for which ESPs retain non-content data for business purposes.

Statistics showing a differentiation by age of data requested are available for two Member States: **Estonia** (mandatory data retention) and **Germany** (no mandatory data retention).

In **Estonia**, the statistics from the Consumer Protection and Technical Regulatory Authority show that in 2017, 61% of requests were for data up to six months old (36% for data up to three months old). In 2018, the proportions remained stable, with 62% of requests for data up to six months (43% for data up to three months old). In **Germany**, the statistics from the Federal Office for Justice show that in 2017, 63% of requests were for data of less than one month old and 84% of requests were for data less than six months old. **These Member States have very different legal frameworks on data retention, yet the statistics highlight that the majority of requests are for non-content data of up to six months old.** The extent to which this conclusion can be generalised to other Member States is uncertain, however. Beyond data retention laws, other factors such as general culture and practices linked to investigation and prosecution of crimes are also likely to play a role.

Figure 21: Percentage of requests for non-content data, by age, Estonia, 2018

Source: Statistics provided by the Estonian Consumer Protection and Technical Regulatory Authority (N = 4,151)

The stakeholder consultation highlighted that the age of the non-content data requested depends on the type of crime investigated, as some types require older data than others. For example, the absence of mandatory data retention has impacted LEAs in Germany to varying extents. For those investigating crimes such as thefts and robberies, the absence of mandatory data retention does not appear to be a fundamental issue. They highlighted that these types of crimes are generally discovered by victims within 24 hours, which gives enough time to request and access data. For German stakeholders focusing primarily on crimes with an electronic dimension (e.g. paedophilia), the current short retention periods are detrimental to investigations. **Many crimes committed via electronic means may not be immediately visible to victims and take longer to uncover.** One stakeholder gave the following real-life example: a cyberattack was carried out on an automated data processing system and remained undetected for two years. The attack only became visible after the activation of ransomware long after the initial attack. Similarly, investigations into organised crimes can last several years and new suspects may only become apparent through the course of the investigation. Many LEAs, notably French stakeholders, advocate longer data retention periods. Other types of stakeholders, such as the Portuguese DPA, believe that a six-month data retention period is sufficient.

6.4. TYPES OF CRIME FOR WHICH LEAS CAN REQUEST ACCESS TO NON-CONTENT DATA

Two broad categories of Member State can be identified with respect to the types of crimes provided in the national legislation for which LEAs can request access to non-content data:

1. Member States where **access and use of non-content data is more permissive**, as data can be requested for **any type of crime**.
2. Member States where access and use of non-content data is **strictly limited to specific types of crimes**.

In all Member States, national authorities such as tax or competition authorities can only request data for criminal offences that fall under the remit of that authority, i.e. tax authorities can only request access to non-content data in relation to tax offences.

Table 7 provides an overview of the types of crimes for which non-content data can be requested in each Member State covered by the Study. Table 20 in **Annex III** differentiates by type of LEA.

Table 7: Summary of the types of crimes for which non-content data can be requested, based on national legislative frameworks

MS	Types of crimes
AT	No crime threshold to access subscriber data. For access to other types of data, the crime thresholds depend on the type of LEA making the request. The Security Police can access all data with no crime threshold, while other types of LEA can only access data for specific crime thresholds specified in the legislation
DE	Only crimes of considerable significance, to be decided on a case-by-case basis by the Courts
EE	No crime threshold but <i>ultima ratio</i> principle applies
ES	Only for serious crimes
FR	No crime threshold
IE	Only for serious crimes
IT	Serious crimes for access to data within 72 months. Any type of crime for access to data within 12 months (internet data) and 24 months (telephone data)
PL	No crime threshold
PT	Only for serious crimes listed in the legislation for access to data retained for law enforcement purposes. A broader list of crimes applies for access to data retained for business purposes
SI	Only for specific crimes listed in the legislation

Source: Milieu elaboration, based on desk research and stakeholders' inputs

Four out of the 10 Member States included in the Study (EE, FR, IT, PL) fall under the first category, where non-content data can be requested from ESPs for **any type of crime, including misdemeanours**. The **Estonian** Code of Criminal Procedure and the Code of Misdemeanour Procedure state that the *ultima ratio* principle must be applied, i.e. LEAs can access non-content data only if accessing such data is strictly necessary for achieving the purpose of the criminal or misdemeanour proceedings. In **France**, police and judicial authorities can request access to non-content data for any type of crime and no threshold is prescribed in the national legislation. By contrast, tax authorities can only access data in relation to fraud on tax information, competition authorities in cases of anti-competitive behaviours, and financial authorities only for market abuse, with no specific thresholds prescribed. In **Italy**, there are no crime limitations for public prosecutors to request access to the non-content data of internet and telephone communications, within 12 and 24 months, respectively, from the date of the communication. Italian public prosecutors can, however, access the non-content data of communications that occurred before these periods (and within a maximum of 72 months) in cases of serious crime. These include massacre, civil war acts, mafia type crimes, murder, aggravated robbery, aggravated extortion, kidnapping for ransom, terrorism, child pornography and participation in armed groups.

In practice, however, stakeholders from these Member States highlighted that **non-content data is only requested when absolutely necessary for the investigation of the case at hand**. For the investigation of simpler, less serious offences, non-content data is usually not requested at all. The circumstances of the case, along with the severity of the crime and availability of alternative evidence, are taken into consideration before requesting non-content data. Stakeholders in Estonia, for example, indicated that while non-content data can be requested for misdemeanours, it is not common practice. Requesting data for misdemeanours is more difficult in Estonia, where necessity is assessed more strictly. **Practical considerations also play a role in limiting requests for non-content data to more serious cases**. Requesting, accessing and analysing non-

content data is costly and time-consuming for LEAs. Some datasets can be difficult to read and require specialised technical skills to analyse (see section 9 for further discussion).

In five of the 10 Member States (DE, ES, IE, PT, SI), LEAs can only request access to non-content data to prevent, detect, investigate and prosecute **specific types of crimes**.

The **German** and **Portuguese** national frameworks make an **explicit distinction between access to data retained for business purposes and data retained for law enforcement purposes** (although the mandatory obligation to retain data for law enforcement purposes is not enforced in Germany). In **Germany**, in order to access data retained for business purposes, the crime must be of 'considerable gravity', which is determined on a case-by-case basis. In order to access data under the mandatory obligation, the crime must also be of 'considerable gravity' and within a specific list of crimes⁷³. In **Portugal**, access to non-content data retained for law enforcement purposes is strictly for serious crimes⁷⁴. Access to non-content data for business purposes, however, is regulated under the Code of Criminal Procedure, which provides a broader list of offences for which data can be requested⁷⁵, including insults or threats committed via electronic means. In **Ireland** and **Spain**, non-content data can only be accessed for the **most serious crimes** foreseen by the national framework. In **Ireland**, this refers to criminal offences (including tax and competition offences) for which a five-year prison sentence is prescribed under the national law, or for certain crimes within a closed list, which have a penalty of less than five years⁷⁶. In **Spain**, serious crimes are defined under the national Criminal Code and include all crimes punishable by a prison sentence of five years or more⁷⁷. They also include crimes that lead to other types of penalties, such as *an absolute professional disqualification; the suspension from employment or public office for more than five years; or the deprivation of parental authority*⁷⁸. In **Slovenia**, access to non-content data is linked to specific types of crimes but these are not necessarily the most serious crimes defined under national law. A distinction is made for access to past non-content data available within the commercial databases of ESPs, for which a list of crimes is provided⁷⁹. In order to access current non-content data from ESPs, there must be a suspicion of a crime for which the law prescribes one or more years of imprisonment.

Access to non-content data in Austria is regulated under three different legal acts, each of which applies to different types of LEAs: (1) the Code of Criminal Procedure, which applies to the criminal police authorities and judicial authorities; (2) the Security Police Act, which applies to the federal and state security police authorities⁸⁰; and (3) the Police State Protection Act, which applies to the Federal Office for the Protection of the

⁷³ In Germany: organised crime, human trafficking, child pornography, corruption, fraud, money laundering, cybercrime, murder, kidnapping, organised and armed robbery, rape, incitement to racial hatred, forgery.

⁷⁴ Serious crimes in Portugal are: terrorism, violent crime, highly organised crime, illegal restraint kidnapping, personal integrity crimes, national security and counterfeiting.

⁷⁵ Crimes to access business data in Portugal are: criminal offences to which a custodial sentence with a maximum limit over three years applies, drug-related offences, possession of a prohibited weapon and illicit trafficking in weapons, smuggling offences, insult, threat, coercion, disclosure of private life and disturbance of the peace and quiet, whenever committed by means of a telephone device, threatening the commission of a criminal offence or abuse.

⁷⁶ Other crimes in Ireland for which data can be accessed: identifying, or impeding the work of a member of the Criminal Assists Bureau, a perjury-type offence of making a false statement in a certificate admitted in evidence in a criminal trial, poisoning, bribery, false reporting of child abuse, and the market abuse offences of insider dealing and market manipulation.

⁷⁷ Article 13(1) Spanish Criminal Code.

⁷⁸ The other penalties in Spain are: disqualifications for a period exceeding five years, deprivation of the right to drive motor vehicles and mopeds for more than eight years, deprivation of the right to keep and bear arms for more than eight years, deprivation of the right to reside in or use certain places for more than five years, prohibition of approaching the victim or those of their family members or other persons as determined by the judge or court for more than five years, prohibition on communicating with the victim or their relatives or other persons as determined by the judge or court for a period exceeding five years.

⁷⁹ The list of crimes in Slovenia includes every crime for which the law prescribes a prison sentence of five years: false imprisonment, kidnapping, stalking, abuse of personal data, pornography, drug trafficking, blackmailing, fraud, polluting drinking water, torture of animals.

⁸⁰ Organs of the public security service are, in particular, members of the federal police guard and members of the municipal guard. The highest security authority is the Federal Minister of the Interior. State police departments and district administrative authorities provide security administration in the federal states.

Constitution and the Fight against Terrorism. Each of these acts establishes specific procedures to access non-content data for the LEAs, with differentiations based on the type of non-content data requested. As such, **the thresholds in terms of crime depend on the type of authority requesting access to data and the type of data requested.** For criminal police authorities, there is no threshold in terms of crime in order to access subscriber data (master data). Criminal police authorities can access other types of data (traffic data, access data and location data) by order of the public prosecutor (and with judicial authorisation) for specific thresholds of crime. That is, either in case of an urgent suspicion of kidnapping, or where there is suspicion of a crime for which the law prescribes at least a one-year prison sentence. In case of suspicion of a crime for which the law prescribes a prison sentence of less than six months, the subscriber in question must give their consent for the authorities to access the non-content data. In exceptional cases, criminal police authorities can request data without a public prosecutor's order but only in case of imminent danger. The security police authorities do not have restrictions in terms of crimes for which they can access non-content data. The Austrian State Protection Office (intelligence agency) can only access non-content data for the investigation of 'advanced hazards' and the prevention of attacks that threaten the constitution, for which the law prescribes a one year prison sentence, at a minimum. This is linked to specific types of crime, primarily the fight against terrorism, group and armed violence or treason. Tax authorities are limited in the type of data they can access and are only allowed to access subscriber data for tax-related crimes without a specific threshold. In order to access the traffic data linked to an IP address, the value of the penalty for the specific financial offence (e.g. smuggling) must exceed EUR 10,000. For other financial offences the penalty must exceed EUR 33,000.

6.5. BENEFITS OF THE USE OF NON-CONTENT DATA FOR INVESTIGATION AND PROSECUTION

LEA survey respondents were unable to provide precise and reliable statistics on the number of cases for which non-content data were determinative evidence during investigations and prosecutions. However, qualitative information obtained through interviews helped to identify some specific needs fulfilled by non-content data (see section 6.5.1), highlighting their indirect value even when they are not used as primary evidence (section 6.5.2), and helped identify general points of interest on the admissibility of data before courts (section 6.5.3).

6.5.1. Evaluation of the decisive character of non-content data

The question whether non-content data are determinative in an investigation or for the prosecution of a case was extensively discussed with the law enforcement authorities throughout the consultation. However, extensive and reliable statistics could not be obtained. Determinative non-content data are defined as data without which criminal proceedings would be dropped.

A first finding is that the relative importance of non-content data depends on the type of crime at hand. For LEAs dealing among others with **cybercrime, child sexual exploitation, and child pornography**, the reported number of cases for which data was determinative is very high - **often above three quarters of the cases** in 2019. Some Portuguese, French and Slovenian Police respondents even estimate that these types of crime require access to electronic communications' non-content data in almost 100% of cases. This can be explained by the nature of the crimes, which are committed or facilitated by means of electronic communications, in particular Internet connections.

On the other hand, LEA respondents dealing primarily with **theft, organised and armed robbery and trafficking of stolen vehicles** reported a lower percentage of cases in which non-content data were determinative. However, the sparse statistics obtained through the survey are insufficient to generalise this finding. During follow-up interviews, some

stakeholders highlighted that even for crimes that are not committed via electronic means, an increasing amount of evidence nonetheless stems from electronic communications, due to the increasing use of mobile devices. **Overall, it appears that while non-content data is almost always crucial to the investigation of certain types of crimes, such as cybercrimes, for crimes such as theft or organised crime, the value of non-content data greatly varies depending on the facts of the case.**

Data on the location of devices proves to be particularly valuable for LEAs, as it can, for instance, corroborate the location of a suspect in the area of a crime scene, or trace journeys.

The weight of non-content data can be significant for **specific types of LEAs**, as indicated by two respondents, specialised in market issues and environmental crimes. In cases of insider misconduct, for example, non-content data constitutes the bulk of the evidence in 50 to 70% of the evidence materials. Similarly, identification of devices from communications issued through specific cell towers can be the only evidence for LEAs investigating environmental crimes, for instance in cases of forest arsons.

Regarding cases that have been dropped due to the lack of access to non-content data, the stakeholders' consultation is inconclusive in all Member States due to the absence of statistics held by the LEAs on the success of investigations or of prosecutions. Stakeholders highlighted that such statistics would be practically impossible to collect since this would require an analysis of each individual court proceeding and police investigation case. Estimations and numbers on this topic are thus based entirely on anecdotal evidence. Data from interviews suggest that the investigation and prosecution of crimes committed via electronic communication are particularly at risk in the absence of access to non-content data, the issue being particularly important in countries which do not have a legal data retention obligation.

6.5.2. Indirect value of non-content data

Stakeholder consultation shows that non-content data does not solely serve as evidence. Interviews conducted with LEAs suggest that most of the time, non-content data constitute either the **first step in finding more substantial evidence** through the identification of more elements, such as a device, a person, or the location of a crime. Data can also serve as a **means to clarify facts** (e.g. location of the suspect at a certain time, proven communication with other suspects) or as a means for **corroboration or negation** of allegations and testimonials, in order to reinforce a case and other pieces of evidence. Non-content data can also be used to identify correspondents of a suspect and detect other potential perpetrators.

The **absence of non-content data** can also serve as evidence. A German LEA, for example, stated that when non-content data show that the mobile phones of suspects of a shooting have been turned off for a certain period of time before and after the criminal facts, this may reinforce suspicions or consolidate other sources of evidence.

Non-content data can also serve at an earlier stage of a criminal procedure, during the investigation to **exclude suspects**, which is not reflected in the statistics. Non-content data can also be useful in cases of organised crime, terrorism or child pornography, which typically involve a high number of accomplices. LEAs can **identify more victims and potential perpetrators** beyond the case at hand, which is only possible by obtaining data going sufficiently back in time. More generally, having access to data from the past allows for the investigation and prosecution of crimes for which the effects only become apparent at a later stage, such as infiltration into information systems as described in Section 7.5.2.

6.5.3. Admissibility of non-content data

The admissibility of non-content data in court proceedings is also **difficult to evaluate**, because of the absence of statistics held by the LEAs. Furthermore, **public prosecutors filter evidence** to ensure that only legally conforming pieces of evidence are presented to the judge and sometimes **prior verification and approval of the evidence by the**

judge is even required. Therefore, potentially inadmissible evidence is rarely used before courts.

The potential issues linked to the admissibility of non-content data are procedural in nature, such as the non-observation of the conditions for access or the request touching on data that should not be accessible according to the national legal framework or case-law, as is the case in Ireland. Another issue related to the substance of the evidence is the potential inaccuracy of a **location** based on the connections to a cell tower: a user can be transferred to a cell tower located in a further location if this cell is congested at a precise point in time or the connection to the next tower can be delayed for technical reasons when a user is moving, reducing the **accuracy of the geographical location** at different times.

Nevertheless, several stakeholders highlighted that non-content data **rarely constitutes the sole evidence in a court case** but is often used to corroborate or contradict other findings. Member States consultations did not uncover specific issues with the admissibility of non-content data nor any examples suggesting issues in this regard. Finally, the information provided through non-content data is generally considered incontestable.

6.6. KEY FINDINGS

- Publicly available statistics on the number of requests for non-content data disclosures are very limited and many governments are unwilling to share data, given the sensitivity of the issue. This makes it difficult to obtain a clear view of the frequency of requests for such data. Where statistics are available, a variety of methodologies are used to record and count requests, rendering cross-country comparisons meaningless.
- LEA survey respondents estimate that they request non-content data frequently, across all Member States. Over 50% of respondents reported requesting data in at least 60% of cases over the last two years. Unsuccessful requests are rare and chiefly stem from non-content data no longer being retained by ESPs. Portuguese respondents reported higher rates of unsuccessful requests, due to different legal frameworks for retention of and access to non-content data, combined with disagreements between LEAs and ESPs over the interpretation of the law.
- The most common form of requests are targeted requests towards a specific individual or device. Large-scale requests, linked to a cell tower for example, are rare and limited to urgent situations.
- All types of non-content data are requested by LEAs. The most frequent data points requested are telephone number, physical address, date and time of the communication and location of the equipment or line at the start of communication. Generally, multiple data points are requested within the course of a single investigation, e.g. call records of a suspect, which contain dates, times and location of communications, as well as the numbers called. Certain types of data are more frequently requested for particular types of crimes, e.g. IP addresses are requested much more frequently for the investigation of fraud, cybercrime and child sexual exploitation than for organised crime.
- A lack of statistics makes it difficult to obtain a consolidated picture of the average age of the non-content data requested. Government statistics in both Estonia and Germany show that the majority of data requested are less than six months old. The type of crime investigated plays a major role in the average age of the data needed. While some crimes are uncovered by victims within 24 hours, others - notably those committed via electronic means - may not be immediately visible and thus require older non-content data for investigations. The same is true for more complex crimes, which require longer investigations and thus older data.
- The legislation in some Member States restricts access to non-content data to certain types of crimes, either listed in the legislation (DE, SI, PT) or the most

serious crimes foreseen by the national frameworks (IE, ES). In other Member States (EE, FR, IT, PL), non-content data can be requested for any type of crime. Stakeholder consultation highlighted that, in practice, non-content data is only requested when absolutely necessary, depending on the severity of the crime and the availability of alternative evidence. In Austria, the thresholds in terms of crime depend on the type of authority requesting access to the data and the type of data requested.

- The extent to which non-content data are determining evidence in an investigation or prosecution varies according to the type of crime and type of LEA. Non-content data are of particular importance in the investigation and prosecution of cybercrime, child sexual exploitation and child pornography. For these types of crime, non-content data are often the primary means of detecting the crime and act as key pieces of evidence. Non-content data can also be indirectly valuable for investigations and prosecutions even if they are not used as primary evidence. They can play an important role at the beginning of an investigation to help to obtain new evidence or identify additional victims and perpetrators. They can also be an important means of corroborating or invalidating other types of evidence relating to the facts of the case. Issues in the admissibility of non-content data are anecdotal, as non-content data is generally considered incontestable.

7. PROCEDURE TO ACCESS NON-CONTENT DATA

This section focuses on the procedures and practical steps implemented by LEAs and ESPs to issue, process, and monitor requests to access non-content data. More specifically, it describes the procedures, steps and shortcomings when LEAs request access to non-content data for law enforcement purposes (section 7.1), those implemented by ESPs to reply to the requests received (section 7.2) and the ex-post monitoring and control procedures implemented by LEAs and national authorities (section 7.3). It also describes how requests to access non-content data from another Member State are treated (section 7.4). Finally, the section looks at quick freeze and other alternatives to data retention used by LEAs (section 7.5). Section 7.6 presents the key findings.

The analysis in this section is based to a large extent on stakeholders' inputs, complemented and verified by available public information.

7.1. LEA PROCEDURES FOR REQUESTING ACCESS TO NON-CONTENT DATA

This section describes the rules, procedures and practical steps implemented by LEAs when requesting access to non-content data for law enforcement purposes, particularly:

1. Whether or not some form of ex-ante authorisation is required before LEAs can access non-content data;
2. Whether or not SPOCs are used by LEAs to present the requests, related procedures and other tools and procedures in place;
3. Whether or not there are specific rules and procedures for LEAs to request non-content data once the ex-ante authorisation is obtained, and to access non-content data once the request is fulfilled.

For each element, the analysis is based on information from the legal research, online survey of LEAs and follow-up interviews in the 10 Member States.

7.1.1. Ex-ante authorisations for LEAs to access non-content data

Based on the information collected, the national legislation of **eight Member States (AT, DE, EE, ES, FR, IT, PT, SI)** provide for some form of ex-ante authorisation before LEAs can access non-content data.

These EU Member States foresee an ex-ante authorisation for police forces, usually in the form of an order from the Public Prosecutor's Office or, more rarely, an investigative judge. In **seven (DE, EE, ES, FR, IT, PT, SI), an ex-ante authorisation is required by public prosecutors and/or investigating or other judges**. A detailed overview of the ex-ante authorisation requirements in each Member State for LEAs to access non-content data is provided in Table 21 in **Annex III**.

In six Member States (AT, DE, EE, ES, PT, SI), judicial authorisation is required (in Portugal and Slovenia, specifically by order of an investigative judge). In **Germany** and **Slovenia**, the request for access must specifically come from the public prosecutor. In **France** and **Italy** (the other two countries requiring ex-ante authorisation), access to non-content data is controlled by the **public prosecutors**. **French** police authorities must obtain the authorisation of the public prosecutor to access non-content data and judges can also only request non-content data by mandate of the public prosecutor. The French competition and financial authorities, however, must obtain authorisation from a magistrate from the Council of State or Court of Cassation. In **Italy**, the situation is similar: in all cases, the public prosecutor must request access to non-content data, and other LEAs can only act with the authorisation and upon request of the public prosecutor. The Italian legislation is alone in expressly acknowledging the right for the investigated person or the defendant in criminal proceedings (and their lawyers) to access metadata. The law

introduces the right for the lawyer to access metadata for phone/internet lines owned by the investigated person/defendant for a period of 24 months⁸¹.

Access to subscriber data is less strict than access to other types of non-content data in Austria, Germany, Estonia, Portugal and Spain. In **Germany** and **Estonia**, subscriber data can be accessed without prior authorisation when necessary for criminal or misdemeanour proceedings. In **Portugal**, LEAs do not need to obtain a previous judicial authorisation to request access to subscriber data. In **Spain**, police authorities require judicial authorisation to access all types of data, however, judicial authorities can request subscriber data directly from ESPs when necessary.

In addition to the partial exception for subscriber data mentioned above, the analysis also highlighted **exceptions to the general rule of ex-ante authorisation depending on the type of offence investigated.** In **Estonia**⁸², the Estonian Code of Criminal Procedure and Code of Misdemeanour Procedure **differentiates between data requested for misdemeanours or for criminal offences.** For misdemeanours, LEAs always require judicial authorisation. For criminal offences, the authorisation from the Prosecutor's Office is required in pre-court procedures and judicial authorisation is required during court proceedings.

Austria is an **exception to the general rule of ex-ante authorisation based on the type of LEA making the request.** For **criminal police authorities**, access to **subscriber data** can be granted without ex-ante authorisation or ex-post supervision. For other types of non-content data (traffic and location data), criminal police authorities can only access the data by order of the public prosecutor, with judicial authorisation. For the **security police authorities**, access to all types of non-content data is less strict and does not require prior ex-ante authorisation. Security police authorities, however, must report all access requests and use of non-content data to the legal protection officer in the Ministry of the Interior, who is responsible for reviewing practices. Based on annual information published by the legal protection officer on their work, the supervision appears to work in practice. In the 2018 issue, the officer stated that the security police authorities make very responsible use of their powers and carry out the considerable effort that comes from legal protection control in a constructive spirit⁸³. **The State Protection Office** (intelligence agency) requires the authorisation of the legal protection officer (who verifies the grounds for access) in order to access non-content data. For all types of LEAs, access to non-content data is directed only towards specific suspects or specific crimes and can only occur if the non-content data is necessary for the purposes of the investigation. As Austrian LEAs can only access non-content data retained for business purposes (there is no mandatory data retention), and as the type of non-content data and the length of the retention period may vary from one ESP to another, LEAs may need to resort to alternative solutions (such as data preservation) to obtain more stable and reliable non-content data (the same applies to Germany and Slovenia, see section 7.5).

Somewhat similarly, in **Portugal**, LEAs need ex-ante authorisation from an investigating judge to request access to traffic and location data (but not subscriber data), while public prosecutors do not need previous approval to request access to data. Interviewed stakeholders pointed out that in Portugal, public prosecutors benefit from a wide degree of autonomy within their investigations and are responsible for their own decisions. There is some disagreement between LEAs and ESPs about the classification of certain data points (such as IP addresses), leading ESPs to reply negatively to LEA requests. Stakeholders suggest, however, that LEAs and ESPs recently reached a shared understanding on the interpretation of the legislative framework, which will likely increase the success rate of future requests.

⁸¹ Article 132(3) of the Italian Data Protection Code.

⁸² Lõhmus, U. (2016). *The saga on retention of electronic communications data was resolved, but not yet in Estonia (Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte)*, Juridica X/2016, pp. 698–708, p. 701.

⁸³ Berka, W. and Trappel, J. (2019). *Internet Freedom*, Manz, Vienna, p. 41.

Looking more closely at the procedures for obtaining ex-ante authorisations, the request is generally presented to the investigative judge or public prosecutor by the police investigating office. The information collected did not point to any formal authorisation from a superior police officer, although requests are often discussed and agreed within the investigating team and authorised by the officer's superiors. The actual requests are presented in a variety of forms (from standardised forms to ad hoc requests) and via different tools (from common IT platforms to certified emails to faxes). Overall, this part of the procedure does not seem automated or standardised.

Two of the 10 Member States (PL, IE) do not require ex-ante authorisations for LEAs to access non-content data. As such, LEAs can request data directly from ESPs. However, Poland and Ireland foresee ex-post supervision through general reviews of the practices of LEAs in accessing non-content data (see section 7.3).

In **Ireland**, an appointed High Court judge has a supervisory role, verifying whether access to non-content data is compliant with the national legislation. The judge has the power to investigate any disclosure request and may access and inspect any official document or records pertaining to the request. In Ireland, LEAs sometimes use the traditional procedure of requesting District Court warrants (normally used to obtain physical evidence) for content and non-content data. This alternative approach is adopted in cases of serious crimes (leading to five or more years' imprisonment as a maximum sentence), despite being more cumbersome. Irish LEAs noted that while appreciating the speed of access granted by the national data retention legislation, they refrain from using it as much as they would like, and have strengthened their internal authorisation process as a way of insulating cases and convictions against the potential fall-out from the challenge to the 2011 Act⁸⁴. Although ex-ante judicial authorisation is not mandatory, Irish LEAs essentially use ex-ante authorisations as a sort of prudent conduct, to prevent or reduce the risk of investigations or sentences being overthrown because of the way evidence was acquired.

In **Poland**, while there is no ex-ante authorisation required by law, the request to access non-content data by the investigating officer needs to be authorised and signed by the officer's supervisor or by the duty officer.

Overall, interviews point to comparatively quick procedures and reduced waiting time to receive the ex-ante authorisation, ranging from a few hours up to one week, with no major repercussions for the investigation. However, there are cases where the length of the procedures can be detrimental (see Box 4 below).

Box 4: Lengthy ex-ante authorisation procedures can prevent access to non-content data

In **Portugal**, while access to subscriber data is quick, access to traffic and location data is more complex. The ex-ante authorisation process is long, sometimes requiring weeks. Despite the legislative provisions to create⁸⁵ an electronic platform for requesting and accessing data (i.e. a SPOC), this has not been implemented. In the absence of an automated process, the request is made by the criminal police in writing and is sent to the public prosecutor by regular post. The public prosecutor receives the request and forwards it to the judge for judicial authorisation. This procedure is time-consuming and it can happen that by the time of its completion, the data retention period has expired and ESPs cannot reply to the request. It was explained that in some cases it is necessary to use the measure of preservation of data (quick freeze) to overcome this problem.

⁸⁴ The CJEU ruling on the 2011 Irish Communications (Retention of Data) Act requested in early 2020 by the Irish High Court is pending. Meanwhile, the Irish legislator is drafting new legislation on data retention for law enforcement purposes.

⁸⁵ Order 469/2009.

7.1.2. Use of SPOCs

When transmitting an access request for non-content data to ESPs, LEAs can use several channels. The most common procedure is the use of certified emails (coupled with some sort of pre-authorisation or vetting of the user presenting the request), and, for a small minority of requests, **fax. The use of SPOCs is not very widespread, with only two of the 10 Member States (France and Germany) implementing the procedure.** Some countries (such as Portugal) are considering developing a SPOC.

Box 5: Functioning of the SPOC in France

In **France**, the National Platform for Judiciary Interceptions (*PNIJ*) was established in 2014. It is managed by the National Agency for digital judicial investigations (*Agence nationale des techniques d'enquêtes numériques judiciaires - ANTENJ*) since 2017. It works as an intermediary between LEAs and ESPs and includes data on mobile phone lines, fixed and IP addresses from French internet service providers.

Its use is, in principle, obligatory for both LEAs and ESPs, even if LEAs can still present requests through other channels. The PNIJ conveys about 80% (in volume) of the requests for non-content data and enables officers of the judicial police to connect and submit requests in a standardised format. There is no human intervention, the whole verification process, extraction and transmission of data is automated – generally officers receive data within 24-72 hours. The majority of requests are identification requests, as these can be automated. The remaining requests are received by fax or even, in very small numbers, via traditional mail. Requests via fax require manual processing, as the ESPs need to verify that the fax references the correct legal basis and that the legal basis fits the type of request. A similar, if more time-consuming, verification process is necessary when requests arrive via post. Some large ESPs are considering developing a messaging system to improve the functioning of the system. Replies to requests are sent via the same medium used to present the request.

The platform is subject to the obligation of secrecy for police and judicial investigation and only the requesting judge or prosecutor has direct access to these data. Other LEAs must request access from this same judge or prosecutor to access data stored by the PNIJ or make their own requests on their own available legal bases.

Germany has a SPOC but its use is not mandatory, despite providing advantages for both LEAs and ESPs.

In **Estonia**, LEAs and ESPs have a common set of forms and standards for presenting and replying to data access requests, which are exchanged in a secure manner via X-Road, a centrally managed standardised and secure integration layer between information systems⁸⁶. LEAs and ESPs have agreed the requests (usually most frequently requested data) and their submission format and ESPs reply electronically. ESPs have developed IT applications that extract the relevant data from databases and then forward the results via X-road. Only the major national ESPs are connected to this system, as it is an expensive solution. If the requests from LEAs concern data not included in the agreement, requests need to be submitted in writing. While this system cannot be considered a SPOC, it provides a high level of automation in the processing of requests, standardisation of data formats and close cooperation between LEAs and ESPs, replying on existing IT infrastructure.

The **platform was developed to improve the efficiency and effectiveness of the process** of requesting access (for LEAs) and providing access (for ESPs) to non-content data, while strengthening security. The use of a centralised platform enables the storage and exchange of common forms, standards and formats. This simplifies the storing and extraction of data by ESPs and the request and analysis by LEAs, reducing the time and costs for processing requests. SPOCs are also intended to increase the security of the

⁸⁶ Started in 1998 as a pilot project under the Ministry of Economy and Communications, it has become the backbone of the Estonian IT infrastructure for public sector services and integrates several functionalities that require direct interaction with private sector providers. See: <https://e-estonia.com/solutions/interoperability-services/x-road/>.

system for exchange of non-content data.

Access to SPOCs (when applicable) is permitted for all LEAs that would have access to non-content data retained for law enforcement purposes and is subject to the same ex-ante authorisation procedures foreseen by the legislative framework. In the two examples reported, the use of the SPOC is not mandatory but the vast majority of the requests are processed through the platform.

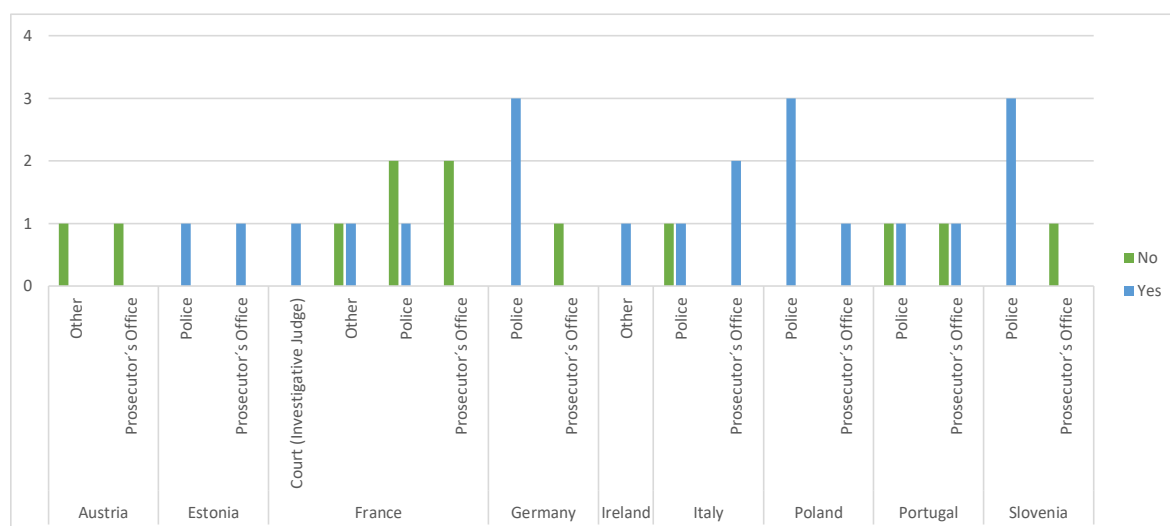
Replies to the LEA survey show some misunderstanding on the existence and functioning of SPOCs in EU Member States. In many cases (EE, PL, PT, PL), while responses from police officers about the existence and functioning of the SPOC were consistent with its definition, prosecution officers confused the SPOC with IT platforms developed by ESPs to process requests to access non-content data. This result seems to indicate that prosecution officers are in fact more detached from those practical aspects of the investigation, while police officers carry out most of the practical actions, including requesting and processing data.

Notwithstanding the apparent confusion about the exact role and functioning of SPOCs, the stakeholders agreed on the relevance of more automation and standardisation in the request and processing of non-content data, which would be provided by the SPOC. 62% of LEA survey respondents consider the SPOC 'fully relevant' for their work, with no noticeable differences across Member States and type of crime (see Question 61 in Annex IV).

7.1.3. Rules and procedures for LEAs to request and access authorised non-content data

Once the ex-ante authorisation is provided (where necessary), LEAs often have procedures to forward the request to ESPs. Data from the online survey show that 62% of the respondents from eight of the 10 Member States have internal procedures to request non-content data.

Figure 22: LEAs' internal procedures for requesting non-content data



Source: Online survey of LEAs, Question 63 (N=34)

In all Member States, the **investigating officer is responsible for forwarding the request to access non-content data to ESPs.**

As a general rule, the request is presented directly to the providers in a variety of forms: through standardised forms, certified emails or requests via IT platforms set-up by the ESPs (non-digital tools such as faxes and traditional mails are rare, but still used). The **identification of the provider** is facilitated by the existence of databases that register

existing phone lines (fixed and/or mobile) and some of the basic data of the owner(s) of those lines (e.g. telephone number, name and address of the line owner, date of birth (if natural person), address of the line (if landline), the number of the mobile phone if provided with the line, starting date of the contract). Other databases allow LEAs to identify the ESPs responsible for that line(s).

For instance, this is the system in place in **Germany**, where the Federal Networks Agency is in charge of the registration of numbers with a person and some of their data. The manual request for information concerns all other data, in particular traffic data, or IP addresses, which are not registered by the Federal Networks Agency. They are requested directly from the ESPs through an IT system that must be established by ESPs with more than 100,000 customers.

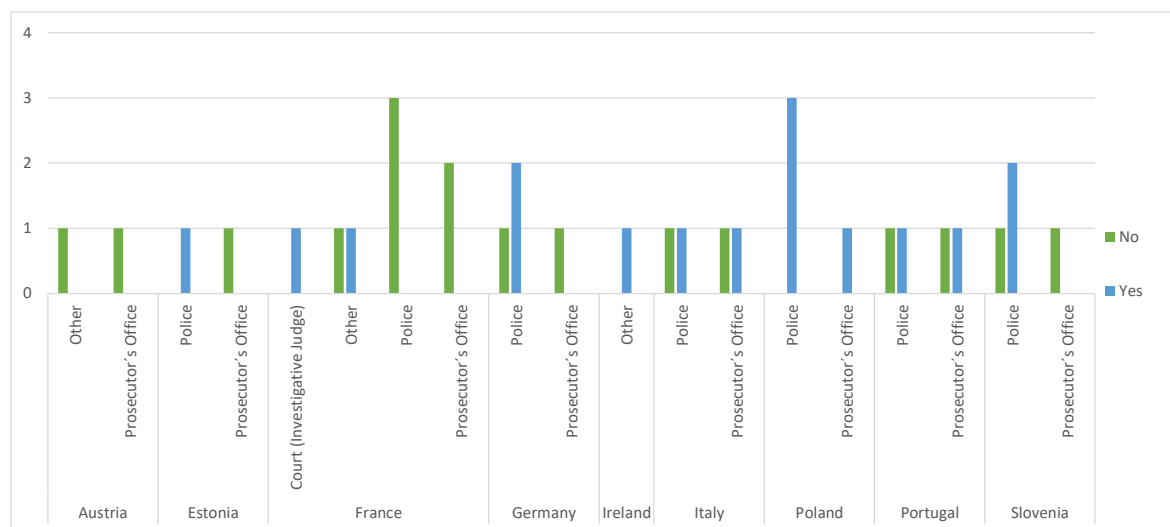
A similar system is in place in **Italy**, where the Unified Database (DBUnico), managed by the Ministry of the Interior, registers existing phone lines and some basic information about their owners, and the Registry of Enrolled Operators (ROC) (managed by the NRA), which enables the identification of the relevant ESP.

The use of SPOCs is limited to two Member States (FR, DE), and to specific types of non-content data. In those countries, the use of SPOCs requires one additional step: the investigating officer forwards the request and the authorisation (where needed) to the desk officers authorised to access the SPOCs, who in turn input the request to the system and forward the reply from ESPs to the investigating officer. The procedure used in Estonia is similar.

Interestingly, most of the negative replies to the questions on the use of SPOCs and ESPs platforms came from prosecution officers, which is consistent with the finding that it is police officers who forward requests to access non-content data. Prosecution officers are in fact more detached from those practical aspects of the investigation. In some countries (AT, PT), there is the possibility for prosecutors to directly request non-content data from providers (for instance, if they consider it useful but the police have not initiated the access request procedure). However, based on the findings from the survey and the interviews, these options are used very rarely. In most cases, the prosecutors access the data once it has been received by the police investigating officers.

Once the non-content data is received, LEAs usually have procedures in place that determine who can access the data. About 47% of the respondents to the online survey, from eight of the 10 Member States, stated that they have internal procedures to regulate access to non-content data obtained from ESPs.

Figure 23: LEAs' internal procedures to access non-content data received from ESPs



Source: Online survey of LEAs, Question 65 (N=34)

Overall, access to data received is restricted to the investigating officer and team, and the prosecution officer following the investigation. The general principle applied is that non-content data is sensitive information and access should be limited for the reasons for which the request to access was presented (i.e. the investigation or judicial proceeding) and to the personnel directly involved. Again, most of the negative replies came from the prosecution offices, which is consistent with the finding that it is police officers who are most involved with the analysis and use of non-content data and the practical elements of the investigation.

7.2. MEASURES FOR ESPS TO PROCESS REQUESTS FROM LEAS

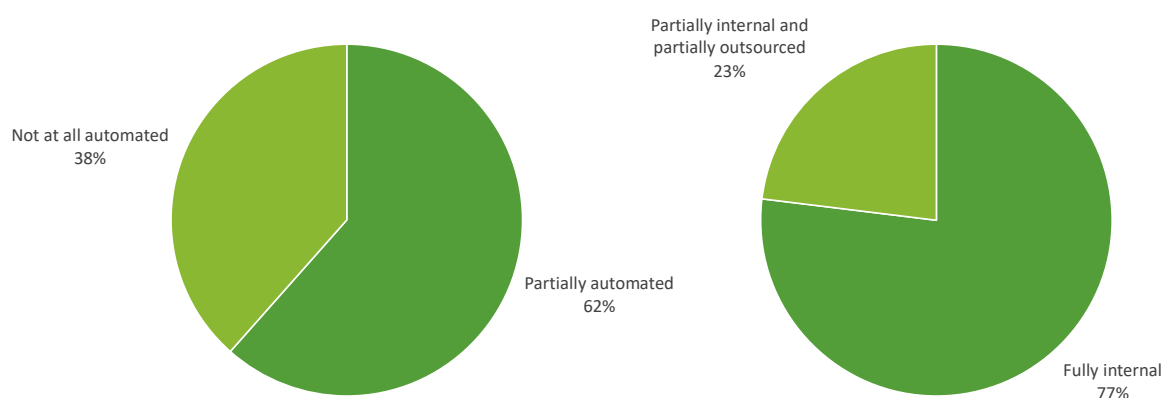
In order to comply with their obligation to cooperate with law enforcement, ESPs have set-up structures within their organisations to ensure that such obligations are discharged efficiently and effectively. These structures include personnel (legal counsellors, IT staff), IT infrastructure, training for internal staff and for LEAs interacting with ESPs' infrastructures.

This section describes the management practices implemented by ESPs, their main costs and implications (section 7.2.1), the vetting process to provide access to non-content data platforms (section 7.2.2), the use of platforms to reply to requests (section 7.2.3) and other tools and measures put in place (section 7.2.4).

7.2.1. Management practices to process requests to access non-content data

All of the ESPs consulted during the Study have designed and implemented management practices to process requests to access non-content data. Those practices include the verification of requests, extraction of non-content data and their transfer to LEAs, the development of technical solutions and related costs.

Figure 24: Key features of ESPs' management practices for access requests



Source: Targeted survey for ESPs, Questions 5 and 42 (N=13)

The procedure to respond to LEAs' requests for access to non-content data is carried out fully internally by the vast majority of the respondents (77% of the ESPs replying to the targeted survey). Where partially outsourced (23%), the parts of the procedure outsourced mostly concern the actual extraction of the data, while the verification of the requests is carried out internally by the ESPs, as is the reply to LEAs via a secured channel. Their sub-contractors have no direct contact with LEAs. The subcontractors provide a platform that automatically manages data, together with the necessary technical support and services.

The platform is located in a 'safe room' (limited access and security requirements) at the ESPs' premises. The results of the data collection activities do not highlight any major differences in these general practices across the different types of ESPs (whether B2C, B2C provider, or both) and the types of services provided. As the sample of respondents is primarily comprised of large operators, it is possible that small ESPs have different procedures (e.g. less automation, and/or largely outsourced).

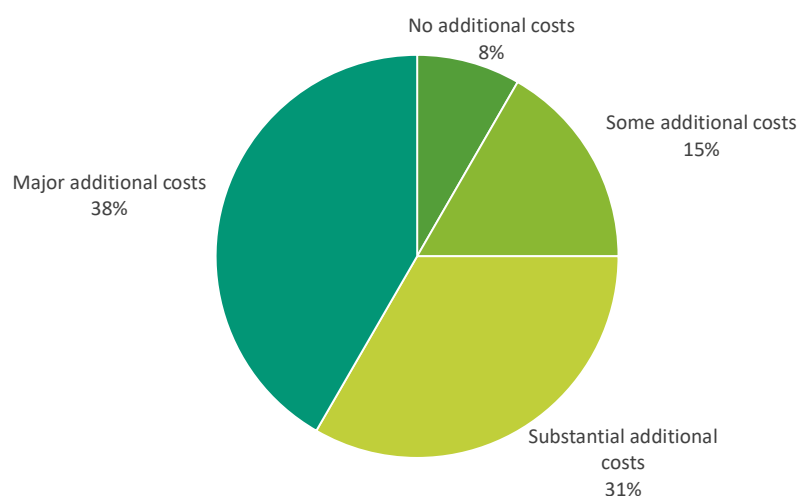
62% of ESPs reported that their management practices benefit from partial automation (see question 51 in Annex V). The automation is applied to the extraction and treatment of the non-content data requested, while the verification of the requests is carried out manually by the ESPs' legal staff.

While it is often a legal obligation for ESPs to designate a responsible person for such obligations, **ESPs have created ad hoc departments for compliance, for legal and functional reasons.** Based on the stakeholders consulted (chiefly large providers), such departments average 15-25 full-time staff (up to 70 staff in one case), including both legal and IT staff, dealing with data retention and other obligations (e.g. interceptions and content-related data retention are treated by the same departments and via the same personnel). In all likelihood, small ESPs will have much smaller structures (one or two staff working on such requests) but the Study only collected indirect evidence. All of the ESPs consulted have developed some IT structure (e.g. company platform) to increase standardisation, improve efficiency and reduce time and costs for processing LEA requests. All ESPs consulted noted that the implementation of IT solutions led to a reduction in the number of staff and time needed to process the requests, and an increase in overall efficiency and effectiveness of the process. This improvement was stressed more in those countries that have recently implemented a SPOC (France).

LEAs' requests are examined and processed by ESPs on a '**first come, first served**' basis, and none of the ESPs consulted has a specific procedure for 'urgent' requests (unlike many of the OTTs consulted, see section 8.4.1). This approach is consistent with the notion that ESPs are legally obliged to address LEAs requests and have made efforts to ensure compliance. Thus, all requests are equally important and treated accordingly.

The creation of ad hoc departments and IT solutions (including stronger storage and security requirements) has incurred additional costs for ESPs, with about 42% of the respondents to the targeted survey categorising these as 'major additional costs'. The costs did not differ between B2C and B2C service providers.

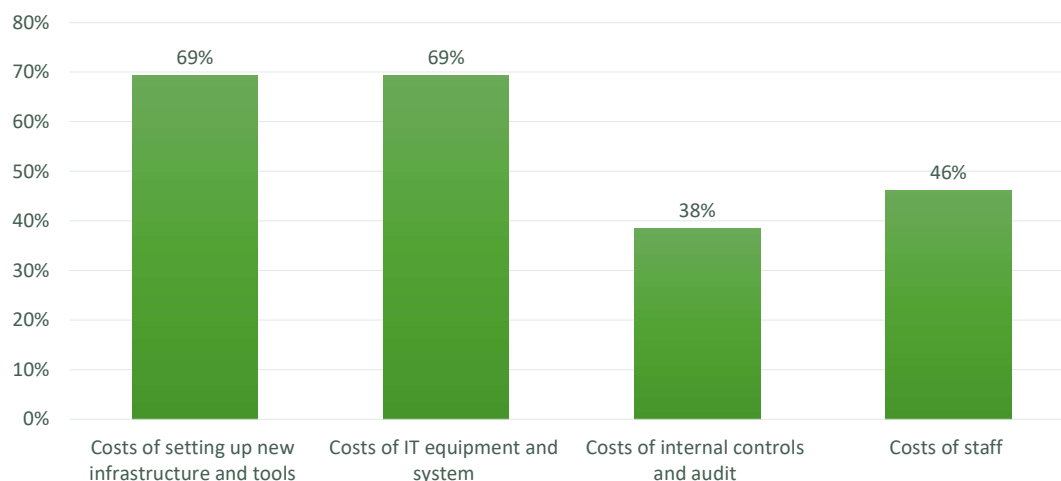
Figure 25: ESPs' views of data retention-related costs



Source: Targeted survey for ESPs, Questions 43 (N=13)

Set-up and infrastructure costs and IT costs represent the largest share of these additional costs (82% of the replies identified them as major costs), with staff another crucial cost (54%) and internal controls and audits a lesser concern (45%).

Figure 26: ESPs' views of data retention-related costs items



Source: Targeted survey of ESPs, Question 44 (N=13, multiple responses possible)

When asked to provide some indications of these costs, most of the ESPs did not reply, as they consider this sensitive information. The few replies can be summarised as follows:

- Initial costs of setting up new infrastructure and tools: between EUR 5.5 and 10 million over five years;
- Maintenance and support costs: between EUR 600,000 and EUR 2.5 million per year;
- Staff costs: between EUR 400,000 and EUR 800,000 per year;
- Other costs (new services that require adaptations of traffic data and increase in the volume of data to be retained) between EUR 400,000 and EUR 500,000 per year.

These figures reflect the costs for large providers. As the structure of costs and accounting systems differ between companies, it is very difficult to extrapolate reliable figures applicable to a large number of ESPs.

Reimbursement by the government of costs related to data retention is quite rare. Of the 10 Member States covered by the Study, only four (AT, DE, EE, FR) have some form of reimbursement for ESPs. In **France**, there are two types of reimbursement. For the infrastructure costs (related to the set-up and use of the PNJI), it is defined in an annual contractual arrangement between the ESP and the State. In addition, a fee-per-request is established, with a reimbursement provided to each provider on the basis of the requests they process on a yearly basis. However, according to the ESPs, the reimbursement only partially covers their costs. In **Estonia**, the costs for communicating the data are compensated, but not the costs of retaining that data.

While the costs reported can appear quite high, they need to be put in context. They represent a limited set of additional costs for large providers have not yet posed a barrier to ESPs deciding to provide additional services and/or enter a new market.

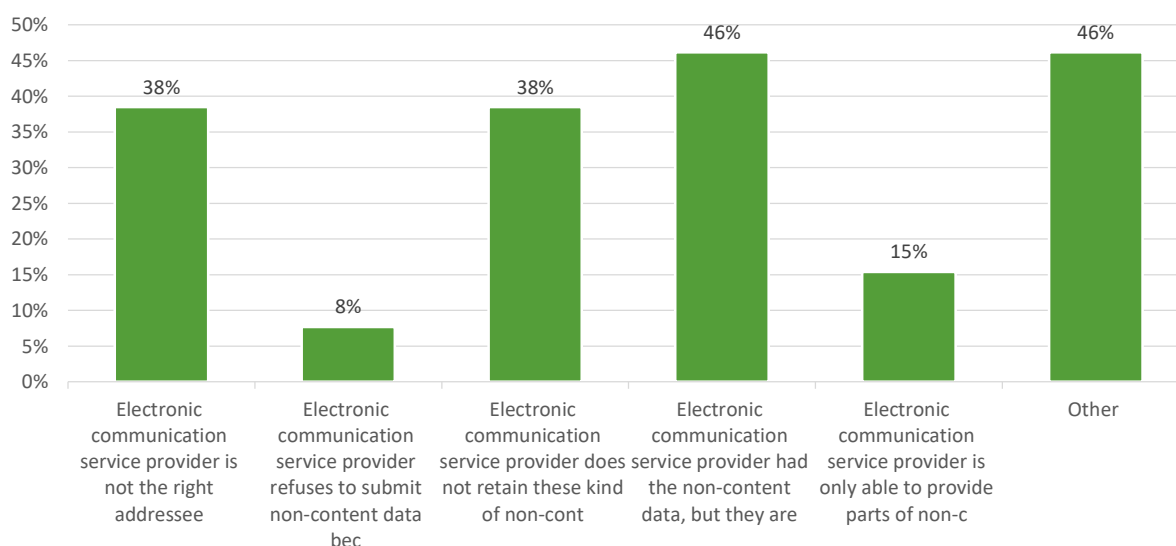
ESPs' management practices require them to process and reply to all requests received, in order to ensure compliance. This approach explains the very low refusal rate for LEA requests. When asked the share of LEA requests they refuse (i.e. the ESP did not disclose any non-content data or only a limited amount that did not suffice for LEAs to pursue the criminal case), ESPs overwhelmingly replied very rarely (92% of replies stated 'never' or 'rarely' (see Question 53 in Annex V). Essentially, ESPs examine and reply to every request they receive from LEAs, providing non-content data if they have it, or replying that they cannot provide it, if they do not have it. From the ESPs perspective, all requests dealt with are compliant.

ESPs are not necessarily in possession of the data requested. The most frequent reasons for failing to provide the data in full are expiration of the data retention time (46% of replies), not retaining that type of data (38%) and being the wrong address for the request. Technical problems with the IT system for data retention are very rare (see

Figure 27 below).

This assessment is different from that of LEAs (see section 6.1.3), which take an essentially opposite view of the 'success rate' for such requests. Overall, **the majority of stakeholders consulted (both LEAs and ESPs) stated that requests for non-content data were rarely unsuccessful.** 56% of LEA respondents and 92% of ESP respondents stated that requests are unsuccessful in less than 20% of cases (LEA survey question 36 in Annex IV and ESP survey question 53 in Annex V). The difference is likely due to the different perspectives of the stakeholders. While ESPs consider every reply 'successful', even one empty of data, LEAs are focused on the amount of data requested and subsequently accessed. The results show some frustration on the part of LEAs, which struggle not only with short retention periods in many Member States (the main reason behind unsuccessful requests given by 68% of both LEA and ESP respondents is that the non-content data is no longer retained), but also with the technical difficulties linked to some types of data (mainly dynamic IP addresses).

Figure 27: Reasons for ESPs being unable to provide the data requested



Source: Targeted survey of ESPs, Question 54 (N= 13)

Notably, most of the cases in which the ESPs no longer have the retained data are reported by **Slovenia**, which does not have data retention legislation, so that LEAs need to rely on data retained for business/commercial purposes (for short periods). Other cases are

reported in **Estonia** and **France**, but these appear related to very specific cases rather than indicative of a more general problem.

Requests addressed to the wrong providers represent a non-negligible share of the total (38% of the replies). In fact, the increasing IT automation and integration of systems, including the implementation of SPOCs, aims to improve the efficiency of the systems, including easier identification of the right address for each request.

The **time needed by ESPs to process the requests received is usually comparatively short**, with 38% of ESPs replying 'less than a day' and 31% 'less than a month' (see Question 55 in Annex V). Short processing times are facilitated by automated processes, and, in some cases, such as in France, are an integral part of contractual arrangements between the ESPs and the NRAs (Ministry of the Interior). LEAs suggested much longer waiting times to obtain the non-content data requests, with only 12% replying 'less than a day', and 29% 'less than a month', 18% 'less than a month' and 6% 'more than three months' (see Question 38 in Annex IV). This substantial discrepancy can be explained by the differences in automation of processes among Member States, and by the fact that a non-negligible proportion of LEAs respondents were prosecutors, judges and other LEA organisations less directly involved in the investigation process. These are likely to have access to non-content data received by ESPs only after they have been analysed by the police officers directly managing the investigation, thus have a different experience of the length of the process.

7.2.2. Vetting process

An important compliance element for ESPs is to verify that the requests they receive from LEAs are legitimate and that they can lawfully reply.

Most of the ESPs carry out controls of the requests, including **verification/vetting of the sources, as well as a verification of the request itself**.

When the request for access to non-content data is presented via the ESP IT platform, the **vetting of the source** (i.e. checking that the user presenting the request is authorised to do so) is not necessary. Only pre-authorised users (who are already registered and vetted) can access their platform, therefore the request is automatically considered legitimate.

When requests are submitted via other channels (e.g. certified emails), ESPs usually verify that the certified email address is among those belonging to the LEAs authorised to present the request.

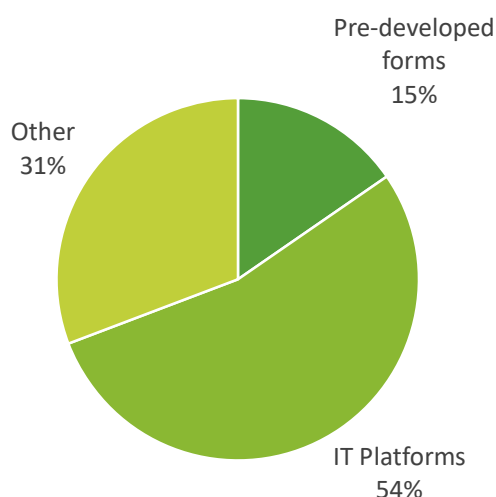
A similar approach is used to **verify the formal prerequisites for request for access itself**. When the request is presented via the IT platform, many ESPs do not verify that the request includes the ex-ante authorisation required and the appropriate legal basis quoted (the system itself includes such verification, especially when requests come from the SPOC used by LEAs). When the request is presented via other channels (such as certified email), in addition to the vetting of the source, ESPs verify that the request includes all necessary formal elements (e.g. ex-ante authorisation, legal basis, reference to the case file).

In general, most of the controls (especially on the request for access itself) are carried out manually by legal staff, as automation is more limited for this function.

It is common practice for most ESPs to contact the authority presenting the request for access in case of a lack of clarity or doubt about a request, so that it can be clarified and processed quickly, instead of refusing it.

7.2.3. Use of platforms and other tools

Most of the ESPs have implemented some form of automation to deal with requests for access to non-content data, including a range of tools such as fully fledged IT platforms (54%), pre-developed forms (15%), and other arrangements (31%), such as standardised formats and pre-registration systems.

Figure 28: Practical arrangements between ESPs and LEAs

Source: Targeted survey of LEAs, Question 45 (N=13, multiple answers possible)

In general, the platforms developed by ESPs process all types of requests to access data, including both non-content and content data (i.e. interceptions). However, in most cases, the two types of requests are treated slightly differently, with those on content data requiring more human intervention.

The degree of automation of ESPs' systems depends on the availability of databases and automated processes on the law enforcement side. The more that applications are integrated, the smoother the process. Overall, requests to access non-content data is mostly automated for subscriber data, while location and traffic data require more human intervention.

In **France**, where LEA requests are conveyed by the national SPOC (PNJI), each authorised requester can post their standardised request on the PNJI. The PNJI forwards the request to the ESP platform, which processes it either automatically (about 80% of cases) or requires some human intervention (mostly for location data). The answer follows the reverse process. To date, 98% of requests are handled using this process.

In other cases, the requests come to ESPs via several channels.

When transmitting non-content data to LEAs following an access request, the most common requirement is for the transmission to occur via the ESP IT platform or via encrypted certified email, with the encryption key being sent separately. While not very frequent, requests can arrive also via fax or traditional mail. Austria and Portugal have specific technology in place for the transmission of data. In **Austria**, there is a central transmission point, which ensures encryption of the non-content data files and the secure identification and authentication of the sender and recipient. **Portugal** has a computer application for the transfer of non-content data to LEAs. The software has an encrypted connection and authenticates both the ESP sender and the LEA receiver, using a username and password. The files containing the non-content data are encrypted using asymmetric keys made available through digital certificates and are signed electronically at their dispatch and reception to ensure the integrity of the data.

While costly to implement, all of the ESPs consulted considered the development of IT platforms a crucial investment that will allow significant savings in the medium to long-term.

The automation of these processes requires the development and agreement of standards and data formats between ESPs and LEAs. In some cases (e.g. Germany), the national legislative framework on data retention and/or data protection provided some technical guidance. In other cases (many of the remaining EU Member States covered by the Study),

the standards developed over time from the cooperation between ESPs and LEAs when developing forms, platforms and other technical arrangements.

Many of the existing arrangements only include police bodies, while prosecutors' offices and investigative judges often need to use less automated and sophisticated solutions.

Most of the ESPs consulted - even those that have invested a considerable amount of resources in developing their IT solutions - would welcome the creation of SPOCs, as they would improve the standardisation of procedures and technical elements in processing access requests. The ESPs' IT platforms are an attempt to move in that direction.

7.2.4. Other measures

All of the ESPs consulted have internal IT audits in place to verify the correct functioning of the IT systems used to retrieve and send non-content data to LEAs. These are integrated into the usual company IT audit practices.

Some ESPs have implemented internal verification processes. For instance, an ESP carried out controls on the completeness of the data provided to reply to the requests, especially in the early days of its presence in the Member State. This activity was instrumental in developing and fine-tuning internal templates for addressing requests, in the absence of pre-defined standards.

Finally, some ESPs periodically carry out tests (on fictional databases, structured the same as those for data retention purposes) to verify the accuracy of the algorithms used to extract the data automatically.

7.3. EX-POST MONITORING AND CONTROL PROCEDURES

After an LEA has obtained non-content data, there are no formal ex-post supervision procedures in six of the seven Member States (DE, EE, ES, FR, IT, PT). The legality of the measures leading to the access and use of non-content during prosecutions can, however, **always be challenged/appealed via complaints to the DPA and/or courts** and LEAs may be held liable based on general national rules on liability for law enforcement.

Available information shows that DPAs intervene only if a data subject specifically claims a breach of their data protection rights, rather than doing so in a systematic manner. Ex-post supervision by DPAs thus appears comparable to court supervision, rather than systematic oversight. These findings are in line with Chapter VI of the Law Enforcement Directive⁸⁷ (see section 4.2).

In **Slovenia**, there is also a mandatory control by the investigative judge, whereby police authorities must deliver all metadata gathered on granted measures to the public prosecutor, who must in turn deliver the metadata to the investigative judge. The judge then examines whether measures were implemented in the manner approved⁸⁸.

Both Poland and Ireland foresee ex-post supervision through the means of **general reviews** of the practices of LEAs in accessing non-content data. In **Ireland**, an appointed High Court judge has a supervisory role, verifying whether access to non-content data is compliant with the national legislation. The judge has the power to investigate any disclosure request and may access and inspect any official document or records pertaining to that request. They act upon the designated judge's own initiative. There is a provision in the national data retention legislation by which an individual who believes their data has been accessed can ask a referee to investigate such access. This 'complaints referee' is an appointed judge from the Circuit Court (one step down from the High Court). Their remit is confined to investigating and reporting on the individual case when requested. The

⁸⁷ Directive (EU) 2016/680.

⁸⁸ Article 153(1)(2) of the Slovenian Criminal Procedure Act.

legislation does not detail how active the judge should be, nor does it provide detailed guidelines. From interviews with Irish LEAs, it is possible to infer that the appointed judges have been active in their role and that the High Court judge's reviews have been 'strict' in the many queries made.

In **Poland**, LEAs must keep records of the number of requests sent to ESPs, their type, and purposes for which the data were used. These records are submitted to the competent District Court on a semi-annual basis, which supervises data access practices.

Four Member States (DE, IE, PT, SI) have **general transparency obligations** to maintain and disclose statistics on access to non-content data. In **Germany** and **Ireland**, this obligation is imposed on LEAs. German LEAs must transfer these statistics to the Federal Office for Justice (*Bundesamt für Justiz*) while Irish LEAs must submit them to the Minister of Justice annually. In **Portugal**, the ESPs must maintain statistics on access requests and transfer them to the DPAs. These reports generally include information on their internal procedures for granting access, numbers of requests received and legal justifications invoked by LEAs. There are currently no such transparency obligations in force in the other five Member States.

7.4. CROSS-BORDER PROCEDURES

For LEAs, requests to other Member States are facilitated by several EU instruments (section 7.4.1). ESPs are not directly involved in cross-border requests for non-content data, but this does not exempt them from facing challenges (section 7.4.2). The European Commission has proposed enhancing cross-border access to electronic evidence, including non-content data, through a more integrated/harmonised approach (section 7.4.3).

7.4.1. Cross-border instruments available to European LEAs

The main tool for cross-border exchange of information is **the EIO**, based on Directive 2014/41/EU⁸⁹ and used by all Member States covered by the Study except for Ireland, which has opted out. The EIO provides for mutual recognition of judicial decisions and simplifies and accelerates cross-border criminal investigations⁹⁰. Recital 30 of the Directive states that '*possibilities to cooperate under this Directive on the interception of telecommunications should not be limited to the content of the telecommunications, but could also cover collection of traffic and location data associated with such telecommunications, allowing competent authorities to issue an EIO for the purpose of obtaining less intrusive data on telecommunications.*' Requests for accessing non-content data in another Member State follow the same legal procedure as those at national level, except through an EIO.

The procedures for the EIO take precedence over the **Council of Europe's Convention on Mutual Assistance in Criminal Matters** of 1959 and its protocols, as well as over the EU's **Convention of 29 May 2000 on Mutual Assistance in Criminal Matters** (the 2000 Convention), which remains the main instrument for judicial requests to other Members of the Council of Europe⁹¹. The two instruments of judicial cooperation - the EIO and the 2000 Convention - are strong channels for the exchange of non-content data for

⁸⁹ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, Official Journal L 130, 1.5.2014, pp. 1-36, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>.

⁹⁰ Eurojust (2018). European Investigation Order, available at: <http://www.eurojust.europa.eu/doclibrary/corporate/Infographics/European%20Investigation%20Order/2018-European-Investigation-Order.pdf>.

⁹¹ Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Official Journal C 197, 12.7.2000, pp. 1-2, available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000F0712%2802%29>.

most of the LEA respondents to the survey, with 24 out of 30 judicial authorities making use of it, including nine out of 10 Prosecutor's Offices.

Council Framework Decision 2006/960/JHA on the exchange of information and intelligence between EU countries' law enforcement authorities⁹² (the so-called Swedish Framework Decision) is an additional means of exchanging telecommunications' non-content data between LEAs when this information is already at the disposal of the requested LEA. If the case relates to terrorism or cross-border crime, **Council Decision 2008/615/JHA** provides for reinforced cooperation and simplified exchange of any personal and non-personal data⁹³. This exchange is possible for data held by the LEAs themselves and data held by public authorities or private parties, which LEAs can obtain without coercive measures, as defined in national law. The channel identified for this exchange is **Europol's Secure Information Exchange Network Application (SIENA)**. However, if the data have already been obtained for an investigation or prosecution initiated nationally through coercive measures, the requested LEAs may transfer these data to their counterparts in another Member State⁹⁴. SIENA is widely used by police forces across Member States and by 15 of the 17 police respondents to the targeted survey.

Another route to obtain cross-border data is the **Council of Europe's Cybercrime contact point**, established by Article 35 of the Budapest Convention on Cybercrime⁹⁵ (the Budapest Convention). This point of contact is used by eight of the 11 LEA respondents that deal principally with cybercrime issues. This instrument is used in the fields of confidentiality, integrity and availability of computer data and systems, computer-related forgery and fraud, but also for the investigation and prosecution of child sexual exploitation and child pornography, and copyright infringement.

Finally, other **specialised frameworks** for the exchange of information are the Naples II Convention⁹⁶ in the field of cooperation between EU customs administrations, and Memoranda of Understanding of the European Securities and Markets Authorities (ESMA) and of the International Organization of Securities Commissions (IOSCO). These international cooperation tools are used by specialised national authorities, which are granted access to non-content data in the national legislative framework of data conservation, the Authority for Financial Markets (*Autorité des Marchés Financiers*) in France and the Revenue Commissioners (*Na Coimisinéirí Ioncaim*) in Ireland.

The significance of cross-border requests compared to national requests cannot be accurately assessed due to the lack of numerical data, but *prima facie* seems to vary greatly depending on the authority concerned. For example, in the case of an LEA dealing with serious financial crimes at national level, the percentage of cross-border requests rose to 30%, while figures from regional authorities are significantly lower.

The stakeholder consultation stressed three issues with respect to cross-border requests for data: (i) the **lack of harmonised rules**, (ii) the **excessive length to obtain the non-content data**, and (iii) the **lack of knowledge of other Member States' access practices**. The lengthiness of cross-border requests for non-content data sometimes threatens the possibility for LEAs to obtain data from other Member States, due to their

⁹² Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, Official Journal L 386, 29.12.2006, pp. 89-100, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006F0960>.

⁹³ Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Official Journal L 210, 6.8.2008, pp. 1-11, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0615>.

⁹⁴ Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, Article 1(5) and (6).

⁹⁵ Council of Europe, Convention on Cybercrime, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>

⁹⁶ European Union (1998). Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations, Official Journal C 024, 23/01/1998 P. 0002 – 0022, available at: [https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:41998A0123\(01\)](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:41998A0123(01)).

short retention periods, or indeed threatens the possibility to subsequently request data at national level based on the results of non-content data obtained abroad.

7.4.2. Cross-border procedures and connected challenges for ESPs

Requests addressed by LEAs to ESPs based in another Member State are not legally possible. Therefore, requests necessarily materialise through the intermediary of the national LEAs where the ESP is incorporated. ESPs in return do not send the information to the other Member State's requesting LEA but use the same intermediary authority. This **prevents ESPs from differentiating cross-border requests** from national requests, as clearly apparent from the answers of stakeholders in France, Italy and Poland.

ESPs are confronted with cross-border challenges in the case of **roaming**, from users of electronic communication services in Europe or outside. Roaming is a service that allows mobile users to continue using their home operator phone number and ECSs while visiting another country. In this case, the legal basis for accessing subscriber data is in the Member State where the SIM card is registered and not where it is used, requiring cross-border mechanisms. The disparity of rules is particularly difficult for ESPs operating in several Member States, which must be careful to distinguish the different legal frameworks for each sets of data and to refer LEAs to use cross-border cooperation mechanisms where appropriate.

In a basic roaming scenario (e.g. SIM card of a data subject registered in country A, using roaming services in country B), the home network (i.e. the ESP in country A) would receive billing files from the roaming network (i.e. ESP in country B), but it is very unlikely that they would receive any detailed traffic data. Therefore, if LEAs in country A want to access traffic data from when the data subject was in country B, they would need to present an EIO request (or resort to any other mechanism for cross-border access to data) to LEAs in country B. LEAs in country B would in turn present a (national) request for access to the ESP whose network the individual was using while in country B. The amount of data shared between ESPs depends on the specific roaming agreement between operators, so it is possible that some operators share more than others in their roaming files.

This issue becomes more critical with the development of the **IoT**, in particular connected cars, which typically move across several jurisdictions, and which may use a **SIM card registered in a different country than the country where the device or car is actually used**. In this situation, the ESPs of a Member State may see the activity generated through this SIM card, but the information related to the user is not available to either ESPs or LEAs of that Member State and the traffic data remain anonymous. European-level cooperation may address this issue. However, the stakeholders report many SIM cards originating from outside the EU and requiring judicial cooperation to obtain information. This issue is reinforced by the absence of mandatory SIM card registration laws in many States, including 14 EU Member States and the UK⁹⁷.

7.4.3. Possible future developments in cross-border requests

The demand for efficient cross-border procedures to access electronic evidence in other Member States is not disputed and the need for foreign evidence is increasing with a borderless internet and increasing numbers of users and activities.

In April 2018, the European Commission proposed a Regulation on European production and preservation orders for electronic evidence in criminal matters⁹⁸ and an accompanying

⁹⁷ As of March 2020, EU Member States not covered by a mandatory SIM card registration law were Croatia, Czechia, Denmark, Estonia, Finland, Ireland, Latvia, Lithuania, Malta, the Netherlands, Portugal, Romania, Slovenia and Sweden. See: GSM Association (GSMA) (2020). Access to Mobile Services and Proof of Identity 2020: The Undisputed Linkages, available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf.

⁹⁸ European Commission (2018). 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, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN>.

Directive⁹⁹, which would, in certain circumstances, allow authorised judicial and investigation authorities of a Member State to require the production or preservation (equivalent to a data preservation or so-called quick freeze) of subscriber, access, transactional and content data directly from the service providers of another Member State operating in the EU.

This proposal is currently undergoing the co-legislative procedure in the European Parliament and the Council. The draft legislation is not within the scope of this Study but if adopted could respond to certain identified issues and demands from LEAs regarding growing cross-border criminality.

7.5. QUICK FREEZE AND OTHER ALTERNATIVES TO DATA RETENTION

This section provides an overview of the **alternative solutions available** to LEAs to obtain non-content data **in the absence of general¹⁰⁰ data retention obligations for law enforcement purposes**. An alternative available to LEAs in Member States with no mandatory data retention schemes (AT, DE, SI) is to obtain non-content data retained by ESPs for business purposes (see previous sections). This section focuses primarily on the other main alternative available, namely data preservation (or so-called quick freeze). This is presented in section 7.5.1, along with its related challenges in section 7.5.2, while section 0 describes other possible alternatives.

7.5.1. Data preservation (quick freeze)

The main alternative solution available to LEAs to obtain non-content data for criminal investigations and prosecutions is a request for the **preservation of data, also known as 'quick freeze'**.

Quick freeze is a **targeted measure to preserve specific data linked to either a specific suspect or to specific facts surrounding a crime**. Similarly, as in the case of data retention, which provides LEAs with the means to look at historical non-content data retained for law enforcement purposes, quick freeze is applied from the moment a crime is detected or suspected and concerns **existing or past data that are currently stored by the ESP for other purposes¹⁰¹**. Like access to non-content data stored by ESPs for law enforcement or business purposes, requests for the preservation of data are generally ordered by the police or Prosecutor's Office and require judicial authorisation.

The origin of the quick freeze mechanism can be traced back to the 2001 **Budapest Convention**, which is the first international treaty in the field of cybercrime, dealing in particular with copyright infringement, computer-related fraud, child pornography, hate crimes and violations of network security. The Convention requires State Parties to implement a data preservation mechanism for a renewable period of up to 90 days **for the investigation and prosecution of certain cybercrimes**. It foresees the possibility for one State Party to request that another State order an entity under its jurisdiction to preserve data. Among the Member States covered by this Study, all except Ireland¹⁰² have ratified the Convention and implemented quick freeze in their national legal systems.

⁹⁹ European Commission (2018). 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, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN>.

¹⁰⁰ General data retention schemes are distinct from targeted data retention schemes, which could be linked to a specific suspect or to a specific group of suspects, to a specific facts surrounding a crime, etc.

¹⁰¹ As quick freeze can be ordered by successive requests by LEAs, at different time points, it may, in practice, allow for the preservation and access to data that is later than the moment when the incriminating facts were discovered and the first order was issued (e.g. in the case of crimes with multiple successive incriminating facts, such as organised crime).

¹⁰² Ireland has signed but not yet ratified the Convention.

Desk research and stakeholder consultation show that six Member States covered under this Study (AT, ES, IT, PL, PT, SI) have expanded the data preservation mechanism beyond the range of cybercrime offences defined by the Budapest Convention. As such, the quick freeze mechanism in these countries can be used for investigation of crimes not covered by the Convention.

In **Austria**, since 2018, quick freeze can be activated by order of the public prosecutor, without judicial approval. Quick freeze orders are generally valid for **three months** and renewable for up to one year. The non-content data that can be subject to a quick freeze order are traffic data, identification data and location data¹⁰³.

In **Italy**, the quick freeze framework allows for the preservation of non-content data, as well as content data of electronic communications, for a period of up to **90 days**, which can be extended for justified reasons for a maximum period of six months¹⁰⁴. The quick freeze procedure in Italy can be triggered for all types of crimes, with no thresholds, although the wording of the legal provision should limit its use to the investigation and prosecution of 'specific crimes'¹⁰⁵. The quick freeze procedure can be exercised by the Ministry of Home Affairs, or, by delegation from the latter, by certain heads of LEAs (in general, heads of LEAs' provincial offices) or officers responsible for the central offices specialised in IT technology within police services, with authorisation of the public prosecutor.

In **Spain**, the Public Prosecutor's Office or the judicial police may require any natural or legal person to 'preserve and protect' specific data on a computer system that is at their disposal until a judicial authorisation is granted for access to the retained data in accordance with the corresponding rules¹⁰⁶. This order may be kept for a maximum period of 90 days, renewable once – up to **180 days**. The requested party has an obligation to keep this request confidential.

The **Polish** Code of Criminal Procedure¹⁰⁷ contains a general quick freeze mechanism, which can be requested by the police for a maximum period of **90 days** with the authorisation of the court or the public prosecutor. This period cannot be prolonged but a written order authorising the preservation can follow later. The serving of such an order should happen no later than by 'the final termination of the proceedings'. Although quick freeze can be used for any type of criminal offence in Poland, LEAs have mentioned that it is primarily used in the investigation of crimes concerning sensitive data (e.g. investigations of paedophilia).

In **Portugal**, the quick freeze procedure can be used for any type of crime committed by means of a computer system¹⁰⁸. As a data preservation measure, quick freeze can be used to access specific computer data, including traffic data. It can be ordered either by a competent judicial authority or by the police, with the authorisation of a competent judicial authority. Data may be preserved for up to **three months**, with a possibility of renewal up to a maximum of one year. Quick freeze in Portugal is seen as a tool to expand the maximum data retention period of one year for an additional year, as the order to preserve the data could also relate to past data retained for law enforcement purposes. LEAs use this practice in some cases to make sure that data are not deleted before the procedure to access data is finalised. As such, the use of quick freeze has raised some doubts with the ESPs, who sometimes refuse to preserve the data above the mandatory data retention period of one year.

The **Slovenian** quick freeze can be ordered by a court and if a likelihood exists that non-content data will be deleted or modified before the court order could be served, a request

¹⁰³ Article 134(2b) and Article 135(2b) of the Code of Criminal Procedure (*Strafprozeßordnung*).

¹⁰⁴ Article 132 (4-ter) of the Privacy Code (*Codice della Privacy*).

¹⁰⁵ G.M. Baccari (2019). Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Cybercrime, UTET, pp. 1606-1607.

¹⁰⁶ Article 588*octies* of the Law on Criminal Procedure.

¹⁰⁷ Article 218a(1) of the Code of Criminal Procedure.

¹⁰⁸ Article 12 of the Cybercrime Law.

can be made orally by a public prosecutor or police officer. Such a freezing request will subsequently need to be confirmed to the ESP by a written court order. The duration of quick freeze orders is limited to **30 days**, renewable once.

Quick freeze should be particularly relevant in Austria, Germany and Slovenia, where there is no functioning mandatory data retention for ESPs. While Austria and Slovenia have expanded the use of quick freeze beyond the cybercrimes listed in the Budapest Convention, Germany has not. Some insights from interviews with LEAs show that **quick freeze is rarely used in Austria and Slovenia and is not used in Germany**. Statistics for Austria show that in 2018 and 2019, quick freeze was used in only 14 cases nationwide¹⁰⁹. Several representatives of Austrian LEAs commented that quick freeze is not an alternative to data retention as it is merely a tool that provides the possibility to ensure that certain data are not deleted. The same can be said for Slovenia, where quick freeze is used only in exceptional cases and is not seen as a real alternative to the system of access to non-content data stored by the ESPs for their own commercial purposes.

7.5.2. Issues related to data preservation

The quick freeze mechanism differs from data retention systems in several respects: (i) the time period for which data can be preserved, (ii) the extent of non-content data covered, (iii) the flexibility offered, and (iv) the procedure. Most of the LEAs consulted **do not consider data preservation a suitable alternative to mandatory data retention**.

Depending on the legal framework for data preservation, past non-content data can be frozen for as long as ESPs already keep them. As such, **quick freeze provides less legal certainty**: in the absence of harmonised retention periods for data retained for business purposes and in the absence of mandatory retention, LEAs cannot be sure what historical data retained by ESPs can actually be preserved. In general, because ESPs do not need location data or IP addresses of an internet connection for more than a few days, they cannot preserve such data if they have already been erased. LEAs therefore face similar difficulties as when they rely on accessing data stored by ESPs for business purposes. LEAs can use data preservation only when the facts which constitute a crime are relatively recent, or when the crime is ongoing at the time that it is detected by the investigation. While data retention guarantees availability of historical data linked to the case under investigation, data preservation can only be applied from the moment a suspicion arises and a preservation order is issued. It does not provide the ability to establish evidence trails prior to the preservation order¹¹⁰.

Box 6: Shortcomings of quick freeze mechanism

A law enforcement authority in one Member State gave the example of an attack against the security of information systems, which remained undetected for several months, but resulted in a visible breach only later - for instance, in the form of a ransom request, fraud or corruption of part of the information system. The interviewee stated that if there was no mandatory data retention, the use of a quick freeze mechanism, in this instance relying on the ESPs' own retention period policies for commercial and technical data, would typically not be sufficient for the investigators to trace back the facts to the time where the breach was committed and identify the perpetrator.

Moreover, the **extent of data that could be preserved and later accessed is limited**. Stakeholder consultation revealed that fewer types of data are available for investigations in the case of quick freeze than under general data retention schemes. This is because national rules on quick freeze often restrict the use of this tool to certain types of non-

¹⁰⁹ Austrian statistics on the usage of the quick freeze mechanism should be viewed in isolation from the data on the number of access requests presented in section 6.1.1. Whilst the number of quick freeze requests shows how often LEAs have asked for immediate preservation of data by the ESP, the numbers in section 6.1.1 represent the number of access requests for non-content data, i.e. the number of warrants sent out to the ESPs to access data that they store for business purposes.

¹¹⁰ See: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_14_269.

content data (e.g. traffic data), while retention measures generally aim to retain other categories of non-content data (i.e. subscriber, traffic and location data). Another distinction between data preservation and data retention is that the former is applied only for the preservation of data with respect to a particular person (or other specific factor), whereas data retention schemes are more general. As such, data preservation methods are similar to targeted data retention schemes. The quick freeze provides less flexibility than general data retention schemes. **Requests to freeze the data need to be targeted and specific**, meaning that LEAs should already have an idea of the key suspects of the crime and the types of data that should be preserved (e.g. data related to a specific suspect, specific phone number). Data retention schemes, on the other hand, enable LEAs to fine-tune requests according to the dynamics of the case at hand and request the data of new suspects, witnesses or alibis and other connections to the suspects uncovered as the investigation/prosecution progresses. Quick freeze does not work for the bulk preservation of data.

A final issue mentioned by some LEAs in respect of quick freeze requests is the **burdensome character of the tool**. As requests are targeted to a specific user, it is more difficult to specify them, unlike data retention schemes where requests can be wider (e.g. even in cases of targeted requests such requests could be linked to a specific device or time period and not solely to a specific user). This in turn requires LEAs to adopt a preventive approach and send an increased number of requests so as to avoid the destruction of potentially useful evidence. In addition, with data preservation, data are 'frozen' in the ESPs databases, so they cannot be deleted, modified, copied, accessed or provided to other organisations. Access to those data by LEAs is often subject to a court order, usually on the ground that the data relate to specific individuals suspected of being connected to a particular criminal investigation or prosecution. This means that LEAs have to request two authorisations, one for preserving the data and the other to access the data preserved.

7.5.3. Other alternatives to mandatory data retention

Other than quick freeze, stakeholders revealed few possible fallbacks at the disposal of LEAs (targeted data retention, surveillance mechanisms such as real time interception, access to digital evidence stored on electronic devices, etc.). However, LEA stakeholders emphasised that **none of these mechanisms could be seen as a real alternative to mandatory and general data retention**.

Retention of non-content data by ESPs can be general for data of all users or **targeted** for data of some users. This latter investigation tool was not identified in any of the Member States covered under this Study. None of the stakeholders considered a targeted data retention scheme as an alternative to general retention of data, as, inevitably, fewer data would be left at their disposal. In fact, some EU-level stakeholders criticised targeted data retention schemes as potentially discriminatory.

Surveillance mechanisms are not a viable alternative to general data retention as they can only be used in cases where the investigation and/or prosecution is already focused on an identifiable suspect. The identification of an individual is thus a prerequisite for the collection of non-content data. LEAs claim that general data retention is needed when the investigation has not yet centred around a circle of suspects and non-content data could help to detect the criminal.

Another common fallback at the disposal of LEAs is **access to digital evidence stored on electronic devices** such as smartphones, computers, tablets, etc. Such devices can contain records of non-content data stored on their hard drives. This alternative can be used, for instance, in investigations where a device is in the hands of law enforcement, implying that a suspect is already identified and located. Interviews suggested that this alternative is often used in criminal cases where LEAs are dealing with organised crime, organised and armed robbery, trafficking in stolen vehicles or theft. A positive feature of this tool is that the seizure of IT material can give access to data without the time limits that apply in cases of access to non-content data.

In the event of crimes committed by means of electronic communications and cybercrime, some of the evidence is necessarily digital and the recourse to non-digital evidence is, by its nature, inappropriate. Particularly in these cases, access to non-content data has been described by LEA stakeholders as the necessary first element to start an investigation, which may only later rely on non-digital evidence to corroborate the facts.

7.6. KEY FINDINGS

- Eight of the 10 Member States (AT, DE, EE, ES, FR, IT, PT, SI) have some form of ex-ante authorisation for LEAs to access non-content data. In general, the ex-ante authorisation is a judicial authorisation or an order by the public prosecutor (FR, IT). Exceptions to the general need for ex-ante authorisations are based on:
 - Type of non-content data (ex-ante requests are not necessary for subscriber data in AT, DE, EE and ES);
 - Type of offence investigated (EE): for misdemeanours, LEAs always require judicial authorisation. For criminal offences, the authorisation from the Prosecutor's Office is required in pre-court procedures and judicial authorisation is required during court proceedings;
 - Type of LEA making the request (AT, PT). In Austria, criminal police authorities can access subscriber data with no ex-ante authorisation but need authorisation from the public prosecutor to access traffic and location data, while security police authorities can access all types of non-content data without ex-ante authorisation. In Portugal, within the structure of the public prosecution there is no need to obtain prior approval from a superior to request the data.
- ESPs have practices to process requests to access non-content data, which include the verification of requests, extraction of non-content data and their transfer to LEAs using secured protocols, and development of technical solutions such as IT platforms and pre-developed forms. In general, the requests from LEAs are managed internally by the ESP (often by a dedicated department) and have necessitated the development of IT systems to store, extract and transmit the non-content data.
- Most of the ESPs interviewed carry out controls on the requests they receive from LEAs, which include a verification/vetting of the sources, as well as a verification of the requests themselves, which have a varying degree of automation.
- Reimbursement schemes for ESPs (totally or partially covering the costs related to data retention obligations) are not widespread, and, where they do exist, only partly cover the providers' costs.
- The use of SPOCs by LEAs is not very widespread. Among the Member States covered by the Study, France has a recently implemented SPOC (PNJI), which conveys the large majority of requests to access non-content data from LEAs. ESPs would welcome an increasing standardisation of procedures and use of SPOCs.
- Although several channels exist for the cross-border exchanges of non-content data in the EU (most commonly, the EIO and Europol channels), procedures in cross-border cases are particularly challenging. The most pressing issues are the lack of harmonised rules, the length of time to obtain the requested data, and the lack of knowledge of other Member States' practices in this respect. It remains to be seen if the proposed Regulation on European production and preservation orders for electronic evidence in criminal matters and the accompanying Directive will respond to some of these issues.
- The main alternative solution available to LEAs to obtain non-content data for criminal investigations and prosecutions is a request for the preservation of data,

also known as 'quick freeze'. However, as a targeted method linked either to a specific suspect or to the specific constituent facts of a crime, it cannot replace general and mandatory data retention schemes. In addition, quick freeze is not possible for all types of crimes and the range of data that could be preserved and later accessed is limited to the type and duration of data stored by the ESPs for their own business purposes.

8. RETENTION OF AND ACCESS TO NON-CONTENT DATA FROM OTT SERVICE PROVIDERS

After presenting the general legal framework (section 8.1.), this section focuses on OTTs' practices of retention of and access to non-content data (sections 8.2 and 8.3, respectively). It also describes the rules, procedures and practices implemented by LEAs and OTTs to access non-content data (section 8.4). Section 8.5 presents the key findings.

As no general data retention obligations exist for OTTs, this section takes an analytical approach, comparing the situation for OTTs with the current legal and practical arrangements for ESPs in respect of the retention of and access to non-content data.

8.1. REGULATORY FRAMEWORK

This section describes the current regulatory framework for retention of non-content data by OTTs, focusing on the general legal framework (section 8.1.1) and the role and function of national supervisory authorities (section 8.1.2).

The analysis in this section is based on information from the desk research and stakeholder input, in particular interviews with OTTs and national supervisory authorities.

8.1.1. Overview of general legal framework for retention of and access to non-content data

While the definition of OTTs generally refers to providers offering a broad scope of services provided over the public internet, the Study looks solely at the providers of instant messaging, email web-based services and voice-calling solutions. It excludes OTTs providing e-commerce, video and music streaming, cloud computing and storage, financial services, etc. The main concepts used in this section are explained and presented in **Annex II**.

Despite electronic communications services and OTT services often having the same functionality and being increasingly bundled together, the regulatory treatment of both types of services has long been divided, as the definition of ECSs at EU level¹¹¹ did not include internet-based services, such as those offered by OTTs. Consequently, **the general data retention obligation for law enforcement purposes imposed on ESPs based on the invalidated DRD and the e-Privacy Directive did not cover OTTs.**

Similarly, Member States' national legal frameworks for the telecommunications sector did not consider OTT services as part of ECSs. For this reason, **national data retention schemes in EU Member States do not apply to OTTs.**

As the difference in treatment of ECSs and OTT services has the potential to distort competition and create an inconsistent level of end-user protection, the new EECC broadened the definition of ECSs to encompass certain OTT services, such as instant messaging services, email web-based services and voice services. This, in turn, means that **from 21 December 2020, the e-Privacy Directive will become applicable to certain OTT services.**

OTTs are currently assessing which of their products and services fall under the broader definition of the ECSs provided in the EECC. This assessment is closely following the recent developments in EU case-law and legislative developments at both EU and national level. The OTTs note that this is not an easy exercise, considering the number of cases pending before the CJEU and delays in the adoption of the proposed e-Privacy Regulation. In the second stage, assuming that some of their services will fall under the new definition of ECSs, OTTs will need to check the applicability of potential data retention obligations in national legislation enacted based on Article 15 of the e-Privacy Directive. The results of

¹¹¹ Framework Directive 2002/21/EC.

this exercise will show if a specific OTTs will need to store non-content data for law enforcement purposes.

In the absence of a regulatory framework, **LEAs can only access those non-content data that OTTs retain for their own business and commercial purposes**. Some LEAs pointed out that this means that not all non-content data are available (e.g. non-content data related to dynamic IP address) and that they would benefit from a data retention scheme applicable to OTTs.

8.1.2. Role and function of national supervisory authorities

The scope of the competence of national supervisory authorities over OTTs is not clear from national telecommunications regulations. Table 8 below shows that NRAs or DPAs in most Member States consider themselves to have no competence over OTTs (AT, SI) or their role and competences are unclear and depend on whether or not OTT services are considered ECSs under national legislation (DE, EE, IT, PL). OTTs are not obliged to retain non-content data for law enforcement purposes in any of the Member States. This could change in the future, however.

As with ESPs, competences and responsibilities over OTTs could be claimed by both NRAs or DPAs, depending on the particularities of the national system. In **Italy**, the NRA's monitoring role over the Registry of Enrolled Operators (ROC) also extends to OTTs. The Italian NRA is proactive in contacting new operators in the market, in particular OTT platforms, to include them in the national database of operators. The **Portuguese DPA** exercises its supervisory functions over those OTTs with an office in the country.

Table 8: Overview of national authorities' competences in retention of non-content data by OTTs

Country	Competences of NRAs	Competences of DPAs
AT	x ■ No role	■ Stakeholder input not received
DE	x ■ Pure IoT services are generally excluded from the telecommunications regulation and are not subject to the rules on the obligation to store non-content data	✓ ■ If OTT services (e.g. messaging services operating in a closed system) fall within the concept of ECSs ■ To monitor the lawfulness of data transfers
EE	x ■ For OTT services that would qualify as ECSs (no OTT services so far falls under the national definition on ECSs), the rules on retention and access to non-content data would apply ■ In practice, OTTs are not requested to comply with national data retention rules	■ Stakeholder input not received
ES	■ Stakeholder input not received	■ Stakeholder input not received
FR	■ Stakeholder input not received	■ Stakeholder input not received
IE	■ Stakeholder input not received	■ Stakeholder input not received
IT	✓ ■ OTTs (including hybrid VoIP operators that commute a voice call from VoIP to 'normal' phone lines or	x ■ As OTTs are not considered ESPs based on the current legislative framework, the DPA has no real authority over OTTs

Country	Competences of NRAs	Competences of DPAs
	vice versa) need to be registered in ROC	
PL	<p style="text-align: center;">*</p> <ul style="list-style-type: none"> No competence as OTTs do not have the same obligations as ESPs (e.g. retention and storage of data related to the use of service) 	<ul style="list-style-type: none"> Stakeholder input not received
PT	<ul style="list-style-type: none"> Stakeholder input not received 	<p style="text-align: center;">✓</p> <ul style="list-style-type: none"> OTTs are subject to national law (i.e. have an establishment), all their national activities are subject to supervision of the DPA OTTs do not have any role in data retention
SI	<p style="text-align: center;">*</p> <ul style="list-style-type: none"> No role 	<ul style="list-style-type: none"> Stakeholder input not received

Source: Milieu elaboration, based on desk research and stakeholders' input

8.2. RETENTION OF NON-CONTENT DATA BY OTTS

The analysis in the following sections focuses on three points: types of non-content data retained by OTTs, data retention periods, and storage and security requirements.

Information was mainly gathered through desk research and interviews with the two largest OTTs. The low number of interviewees means the data are not very representative, however.

8.2.1. Purposes for which non-content data are retained and types of non-content data

OTTs are not obliged to retain non-content data for law enforcement purposes. Non-content data in their databases are thus (i) kept at the request of their users, (ii) retained for their own business and commercial purposes, or (iii) retained due to some kind of legal obligation. Business and commercial purposes include the contractual relationship between OTTs and their users (usually defined in service contracts or in general terms and conditions), billing, marketing and promotion, security, or other company reasons. As such, the legal framework could be compared to that of Austria, Germany and Slovenia, where there is no legal obligation for ESPs to retain particular non-content data for law enforcement purposes.

The types of non-content data that OTTs retain depend on the type of OTT services and/or products, ranging from IP log-in records to non-content data related to communication services, similar to ESPs. A good understanding of the types of data retained by OTTs is a prerequisite for a successful data request. To this end, the OTTs issue and/or publish special guidelines¹¹² for LEAs, outlining the types of information that an OTT service provider could provide.

In response to a request for access, OTTs are able to provide LEAs with the following non-content data:

- **Subscriber data:** registration and subscriber information (information captured at the time of account registration, such as username/account name, email address, name, state, country, postal code, telephone), billing information and billing

¹¹² Available at: <https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf>, <https://www.facebook.com/safety/groups/law/guidelines/>.

transactions (may include billing address and payment method/instrument(s)), IP logs (IP addresses captured at the time the user logged in to a specific service), customer service records regarding a device or service, services utilised, serial number, number service history (list of numbers subscribed to by a user), purchase history, device information (media access control (MAC) address) etc.;

- **Traffic data:** type of services used, type of communication, transaction logs, historical call detail records for calls received and placed, call invitation logs, short message service (SMS) historical detail records, historical record of email exchange activity, connection and sign-in logs with IP addresses, if available, possible IP connection history etc.;
- **Location data:** if relevant for the types of services.

8.2.2. Data retention periods

In the absence of any regulatory framework, OTTs retain non-content data for various lengths of time, depending on the purpose of processing and the type of data. Those rules on data retention lengths are usually described in the OTTs' privacy statements. The same type of data could thus be subject to different retention periods, depending on the purpose of processing.

Stakeholder consultation shows that some types of non-content data, such as IP address, may be stored for only short period of time (approx. 30 days).

8.2.3. Storage and security requirements

As non-content processed by OTTs are classified as personal data, OTTs need to observe and apply the GDPR provisions on security measures¹¹³, irrespective of whether or not they are obliged to retain non-content data.

As with ESPs, OTTs also need to ensure that no damage, loss or alteration occurs to the data and that only authorised personnel are involved in the processing. For this reason, OTTs need to implement technical, organisational and security measures for ensuring the security of the processing of non-content data. Stakeholder consultation did not reveal any particular requirements that would apply to OTTs, preventing confirmation that the storage and security requirements applicable to ESPs (section 5.5) also apply to OTTs. The Italian legal framework, however, imposes separate storage requirements for data retained for business and law enforcement purposes on both ESPs and OTTs established in Italy.

8.3. ACCESS TO AND USE OF OTTS' NON-CONTENT DATA

This section presents the practices regarding access to and use of OTTs' non-content data. It is structured around two topics: the numbers of access requests to OTTs by governments and LEAs (section 8.3.1) and the types of non-content data requested (section 8.3.2).

The analysis in this section is primarily based on the publicly available information from four OTTs: Apple, Facebook, Google and Microsoft, as well as information obtained through interviews with some OTTs and LEAs. The information gathered was compared against the results of the online surveys.

8.3.1. Numbers of access requests to OTTs and numbers of unsuccessful requests

A common practice among OTTs is to publish **transparency reports** with at least aggregated statistics on the numbers of legal requests for their customer data from

¹¹³ Article 32 GDPR.

governments and LEAs around the world and in a particular country¹¹⁴. This is possible because OTTs, similar to some ESPs that provide cross-border services, set up a single channel for requests, which is a means of accounting for all data sent out.

Table 9 shows the aggregated number of requests sent to four OTTs (Apple, Facebook, Google and Microsoft) over the whole of 2018 and in the period between 1 January 2019 to 30 June 2019¹¹⁵.

Table 9: Total number of requests sent to OTTs, 2018 and January-June 2019

MS	January-December 2018	January-June 2019
All Member States	129,098	74,059
Germany	64,593	36,194
France	32,063	17,583
Spain	10,833	6,559
Italy	9,252	5,129
Poland	5,890	4,996
Portugal	3,909	2,242
Austria	1,656	831
Ireland	564	263
Estonia	193	176
Slovenia	145	86

Source: Milieu elaboration from transparency reports of OTTs

In both years, the Member States which sent by far the highest number of requests were Germany and France, followed by Spain, Italy and Poland. Stakeholder consultation revealed that **the high level of requests from Germany** was due to particularities in the national approach to the investigation and prosecution of crimes, which obliges LEAs to follow-up on minor crimes, such as stolen devices. One of the German LEAs revealed that as ESPs retain non-content data for only seven days, they tend to request non-content data older than seven days from OTTs. Although the numbers of access requests were also high in **France**, such numbers were substantially lower than access requests to ESPs. This was confirmed through stakeholder consultation, with one interviewee from a French LEA noting that, as a general rule, LEAs refrain from requesting data from OTTs, as the procedure is difficult (e.g. OTTs sometimes demand a formal legal request letter) and often unsuccessful.

If the numbers of requests are compared against the total population in the Member States that could be theoretically affected by such access requests, it is clear that the access requests only refer to the non-content data of a very small percentage of the population, ranging from 0.004% in Slovenia to 0.078% in Germany. However, not all the population may be affected by such access requests, as not everyone uses OTT services. Nevertheless, in reality, far more OTTs users are impacted by law enforcement requests, as a single request may seek information about multiple accounts belonging to one user, or the same accounts may also be subject to repeated orders in different timeframes and as a result are 'double counted'. The number of accounts affected and/or other identifiers specified is thus substantially higher and could amount to a twofold or even threefold increase in the numbers of requests.

Due to the constraints outlined in section 6.1.1, an accurate comparison of numbers of requests to LEAs and OTTs in general and by Member State is impossible, due to the

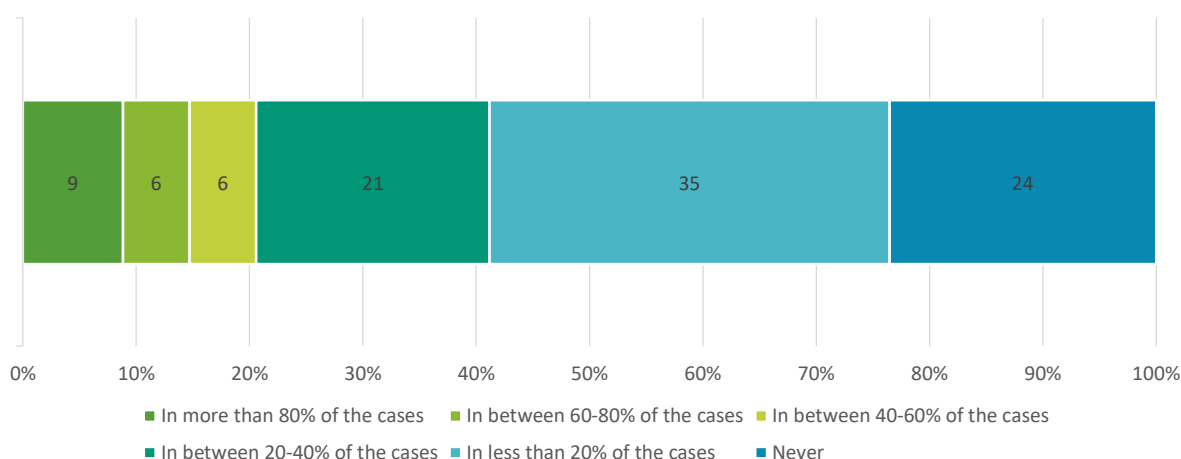
¹¹⁴ Available at: <https://www.apple.com/legal/transparency/choose-country-region.html>, <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>, <https://transparency.facebook.com/government-data-requests>, <https://transparencyreport.google.com/user-data/overview?hl=en>.

¹¹⁵ OTTs also operate in the B2B segment and requests from LEAs can - in some jurisdictions - be directed towards companies' data. The number of requests received for accounts associated with companies is presented in the overall statistics but can be ignored, as the numbers are very small.

absence of a homogenous reporting system. Nevertheless, the available figures show that **in all Member States with the exception of Germany, OTTs receive far less access requests from LEAs than ESPs**. The difference in figures is particularly evident for Estonia, France, Ireland, Italy and Portugal. Fewer requests are also sent to OTTs in Austria, Spain and Slovenia. In Slovenia, an LEA representative mentioned that obtaining data from OTTs is complicated because there are several providers, which are established in other countries.

This conclusion seems to be confirmed when looking at the estimated frequency of access requests to ESPs and OTTs in the last two years. Over 50% of LEA respondents stated that they have requested non-content data from OTTs in the last two years in less than 20% of cases (see Figure 29). Requests for ESPs' non-content data were more frequent, with over 50% of respondents stating that they have requested data in at least 60% of cases (see Figure 14).

Figure 29: Frequency of access requests to non-content data from OTTs in the course of a criminal investigation/prosecution, 2018 and 2019



Note: The figure shows police and public prosecutor responses. Other types of respondents were excluded as they either do not request non-content data (not investigative or prosecution bodies) or do so only rarely.

Source: Targeted survey of LEAs, Question 15 (N=29)

Germany stands out, as OTTs actually recorded a higher number of requests than those in the official governmental statistics for ESPs. Although it was not possible to clarify this discrepancy through the stakeholder consultation, it could be partly explained by the fact that official government statistics are an underestimation (e.g. only requests for traffic data are included) and that in case of ESPs the numbers are based on the number of warrants (which could include requests sent to multiple ESPs), whereas in case of numbers from OTTs, the same request sent to all four OTTs would be counted four times.

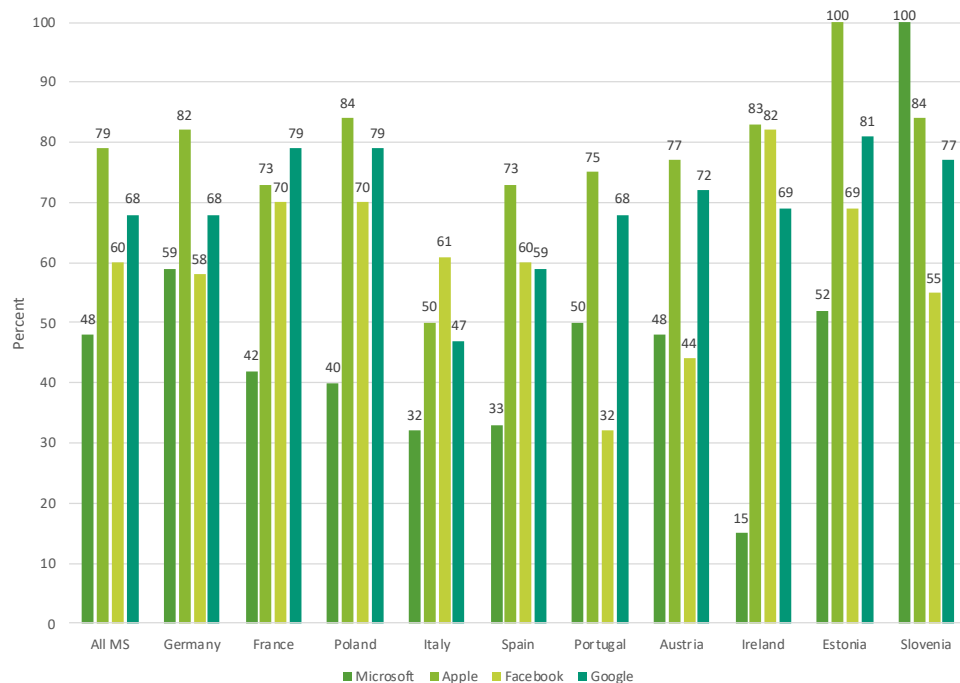
The number of granted requests could be lower than the number of actual requests, as OTTs **may reject LEA requests on the following grounds:**

- **Not meeting the legal/procedural requirements** - the request is not made by a legally authorised and competent authority, lack of a valid court order, wrong addressee;
- **Data requested not being found** - such data were not retained, or data were retained but the retention period has elapsed.

Reasons for an unsuccessful request are similar to those reported by the ESPs. Similar to ESPs, some OTTs consider all processed requests successful, regardless of whether or not the data were provided to LEAs in the end.

Figure 30 presents the success rate by country and OTT service provider.

Figure 30: Success rate of requests sent to individual OTTs, January-June 2019



Source: Milieu elaboration from OTT's transparency reports

The success rate is always above 50% and varies from 51% in Portugal to 74% in Slovenia, with the average of 66%. No correlation was detected between the number of access requests and the success rate. For instance, Germany, which has the highest access request rate, also has one of the highest success rates, while France and Portugal, which also record a high access request rate, have a much lower success rate (Portugal being the lowest).

The reasons for high successful request rates in France and Germany could be explained by the fact that larger Member States benefit from larger resources, which could be further invested in obtaining knowledge about the functioning of OTTs.

8.3.2. Types of non-content data and types of crime

Statistics held by the OTTs do not present breakdowns by type of non-content data, purpose for which LEAs request access (investigation and/or prosecution), type of crime (serious crimes, crimes or misdemeanours) or type of LEA requesting non-content data (LEAs vs. national security/intelligence services). This is chiefly due to the lack of uniformity across countries, lack of detailed explanations in the requests by the LEAs and the potential legal pursuit that could occur in certain countries due to disclosure of such detailed information.

The limited stakeholder input meant that information could not be obtained on the most common types of non-content data requests and types of crime for which data are requested. Several LEAs expressed their dissatisfaction with the type of non-content data available, with one noting that OTTs are not able to present non-content data connected to a dynamic IP address, such as the port number and the timeframe, as OTTs have no obligation to retain these data.

Anecdotal evidence suggests that approximately one-quarter of requests are related to cybercrimes, with the remainder concerning the resolution of other types of crime.

8.4. PROCEDURE TO ACCESS OTTS' NON-CONTENT DATA

This section focuses on procedures and practical steps implemented by OTTs to process requests to access non-content data, including the main challenges (section 8.4.1). Section 8.4.2 describes alternative procedures for requesting access to OTTs' non-content data.

The analysis in this section is based on information from desk research, the LEA survey, interviews with several OTTs and follow-up interviews with national stakeholders.

8.4.1. Procedure for requesting access to OTTs' non-content data and associated challenges

OTTs as large global players receive requests to access non-content data from governments and LEAs from all around the world. In the absence of any data retention framework, many of the OTTs **issue and/or publish special guidelines**¹¹⁶ for LEAs in order to facilitate a more effective access request procedure. The OTTs interviewed for this Study expressed their dissatisfaction with (sometimes) poorly formulated and incomplete requests from LEAs, which led them to promote the use of their internal procedural guidelines. Several OTTs facilitate training for law enforcement officers on the types of data available and how to obtain those data in line with their internal procedures. This helps to align their expectations and facilitate a more successful process of requesting non-content data. Publication of guidelines and their proactive approach to educating LEAs is the main difference between ESPs and OTTs.

The content and issues covered in the guidelines for LEAs are broadly the same across all OTTs, all of whom approach the problem in a similar way, i.e. through an **internal and centralised process for receiving, tracking, processing and responding to legal requests from governments and LEAs**. These guidelines outline the procedure for accessing retained non-content data, focusing on elements such as form of a request, information to be provided in case of a request (e.g. valid identifiers that could facilitate the search of relevant records), channels and procedure to submit a request, as well as legal conditions for the access request to be processed and approved (e.g. obligation to present a valid court order).

Only correctly submitted requests from competent LEAs are further processed by OTTs. An LEA's request to access data is approved only if such a **request is legally valid**, e.g. made in circumstances where it has a precise legal basis in the domestic law of the requesting country and pertains to the bona fide prevention, detection or investigation of offences. In principle, this means that a request to access non-content data should be **based on a valid court order**. Some OTTs set a rather high bar for obtaining non-content data and provide such data only in cases of serious crimes, excluding misdemeanours.

As is the case for ESPs, one of the major challenges for OTTs is to verify whether a request is from a credible source, such as a national/regional government or an LEA. To facilitate this process, the submission of access request is streamlined to a **specific online request system**¹¹⁷ or a **specific electronic address** responsible for receiving requests. In some cases, OTTs promote the use of templates for filing an access request¹¹⁸.

Some OTTs mention the problem of technical complexity in accessing data, as the non-content data retained are protected with complex and robust security systems. High

¹¹⁶ Available at: <https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf>, <https://www.facebook.com/safety/groups/law/guidelines/>.

¹¹⁷ See: <https://www.facebook.com/records/login/>.

¹¹⁸ See: <https://www.apple.com/legal/privacy/gle-inforequest.pdf>.

security measures mean that the process of identifying and retracting data is labour-intensive for OTTs.

Due to the increasing number of access requests and complexity of the procedure, a **high volume of manpower is needed to process access requests for non-content data**, with associated cost implications. Another cost-intensive element is the need to address new needs and new types of requests from LEAs, following technological trends (higher volume of demands and broader scope). The OTTs would **welcome reimbursement schemes**, not just to reduce costs but to incentivise LEAs to narrow their requests to what is really needed.

Stakeholder consultation showed that many OTTs have put in place **an internal vetting system** to check **whether or not requests to access non-content data are valid**, i.e. from a legitimate source and with **a legitimate legal basis**. As this verification process is extremely labour-intensive and has very low automation, OTTs usually have large compliance and data engineering support teams. The need for outside counsel was mentioned for cases that include audits of compliance with EU law and similar. The vetting process, in particular the burden of ensuring that requests have a valid legal basis, is one of the challenges in the procedure for responding to access requests.

In the eyes of OTTs, SPOCs reduce uncertainty about the source of requests and increase the efficiency of the procedure. As requests coming from SPOCs have been vetted, they are automatically considered legitimate. This means that **use of SPOCs provides for a smoother process with less confusion and misunderstanding**.

LEAs interviewed mentioned the biggest challenges as the following: problem in identifying the service provider (i.e. the legal entity behind the service/platform), the fact that OTTs are usually established in third countries, encryption of identification data which makes it impossible to identify the user, non-existent non-content data at the side of the providers, and long procedures for regular access requests.

8.4.2. Alternative procedure for requesting access to OTTs' non-content data

In addition to 'regular' access request procedures, the procedural guidelines of several OTTs specify rules for preservation requests for up to 90 days (so-called quick freeze) and for emergency requests (e.g. matters requiring disclosure of information without delay due to imminent and serious threat(s) to a child's safety, the life/safety of an individual(s), the security of a State and the security of critical infrastructure/installation(s)). In the case of the latter, access to non-content data could be provided in matter of hours. Such requests still undergo some sort of vetting procedure but are expedited, for obvious reasons.

8.5. KEY FINDINGS

- There is no EU or national legal framework imposing a general data retention obligation for law enforcement purposes on OTTs. This situation might change as of 21 December 2020, when the e-Privacy Directive and potentially its transposing legislation will become applicable to OTTs. There is a high degree of uncertainty for OTTs, who for now closely follow the ongoing proceedings at the CJEU.
- NRAs or DPAs in most Member States have no competence over OTTs or their role and competences are unclear and depend on whether OTT services are considered as ECSs under national legislation.
- In response to a request for access, OTTs are able to provide LEAs with a number of non-content data, which they keep for their own business or commercial purposes. Depending on the type of services they provide, such non-content data include (i) subscriber data (e.g. registration and subscriber information, billing information and billing transactions, IP logs, customer service records about a device or service, services utilised, serial number, number service history, purchase

history, device information); traffic data (e.g. type of services used, type of communication, transaction logs, historical call detail records for calls received and placed, call invitation logs, SMS historical detail records, historical record of email exchange activity, connection and sign-in logs with IP addresses, if available, possible IP connection history); and location data.

- Although OTTs are not obliged to report the numbers of access requests, they do so on their own initiative in their transparency reports, typically published on a six-monthly basis. LEAs in Germany and France send the highest number of requests to OTTs in both absolute figures and in relation to their total population. Nevertheless, certain Member States such as Portugal or Estonia send a relatively high number of requests in relation to their total population. The number of access requests is substantially lower than the number of requests to ESPs, with Germany as the exception.
- OTTs reject a number of law enforcement requests where: (i) they do not meet the legal requirements (e.g. the request is not made by a legally authorised and competent authority, or lacks a valid court order); and (ii) the data requested have not been found (e.g. such data were never retained, or were retained but the retention period has elapsed). Reasons for rejection and the overall success rate are similar to those reported by the ESPs.
- OTTs usually put in place internal and centralised processes for receiving, tracking, processing and responding to legal requests from governments and LEAs. Such processes are described in their guidelines and actively promoted at training offered to LEA officers. An internal vetting system is in place to check whether the requests to access non-content data are valid (from a legitimate source and with a legitimate legal basis). This vetting system is the most complex and labour-intensive part of the procedure to access non-content data. OTTs welcome the use of SPOCs, whose requests are already vetted and thus automatically considered legitimate.

9. LESSONS LEARNED AND FUTURE CHALLENGES

This section presents the key features of the national data retention schemes by looking at the views of ESPs and OTTs and the needs of LEAs in the 10 Member States covered by the Study. Section 9.1 presents the overall views and opinions of ESPs and LEAs on the national data retention schemes and cross-border procedures. Upcoming technological developments and related challenges are described in section 9.2, with the key findings summarised in section 9.3.

The analysis in this section is largely based on stakeholders' inputs, complemented and verified with available public information.

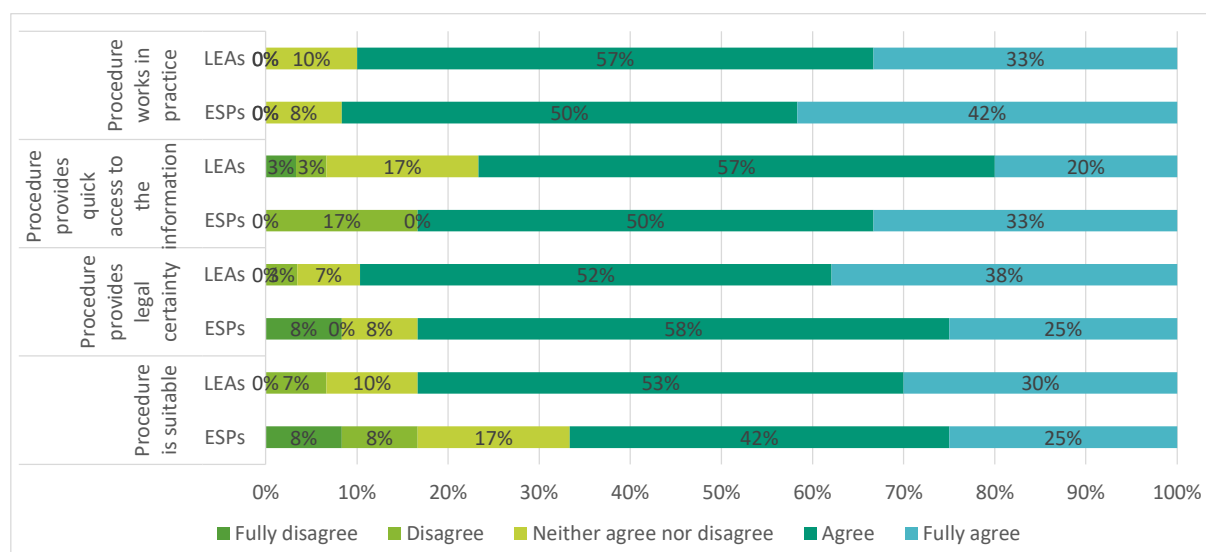
9.1. STAKEHOLDERS' VIEWS AND OPINIONS

While the Study was never intended to evaluate data retention schemes in the 10 Member States covered, stakeholders were asked to provide their opinions on the overall functioning of the system, for both national and cross-border requests.

Both LEAs and ESPs were asked whether the national and cross-border schemes work in practice, provide quick access to information, provide legal certainty and are suitable.

Overall, stakeholders expressed a positive opinion about the functioning of the national schemes, whether or not the country has a mandatory data retention scheme: aggregated results show that 91% of the stakeholders agreed or fully agreed that the national systems work in practice, 79% that they provide quick access to information, 88% that they provide legal certainty and 79% that they are suitable (see Figure 31).

Figure 31: Stakeholders' assessments of the national schemes for data retention



Source: Targeted surveys of LEAs and ESPs, Questions 51 and 72 (N=44, i.e. stakeholders from all 10 Member States covered by the Study)

ESPs have a slightly less positive assessment of the national schemes' general suitability (16% disagreed or fully disagreed, compared to 8% of LEAs) and ability to provide legal certainty (8% of ESPs fully disagreed, compared to none among LEAs). LEAs are more doubtful about the national systems' ability to provide quick access to information (6% of LEAs fully disagreed or disagreed, compared to none among ESPs). Overall, these differences are not significant and there was no major criticism of the national systems.

When looking at the **responses by Member State, opinions tended to be more positive generally for those countries (FR, PL) where the legislative framework has not changed recently and where automation of processes among LEAs is more widespread (including the use of SPOCs)**. Even in countries without a general data retention obligation (AT, DE, SI), stakeholders feel positive about their national legal framework, especially among LEAs. In Austria, for instance, all respondents claimed to agree if not fully agree that their national system works in practice, provides quick access, legal certainty and is suitable (in Germany and Slovenia, the numbers were slightly lower, at 75% and 80%, respectively). Stakeholder consultations confirmed that even in systems without a data retention obligation for law enforcement purposes, stakeholders tend to adapt their practices to the current situation. In Germany, where ESPs keep some non-content data for only seven days, LEAs adapted their practices so as to allow them to send access requests on time, as well as using other mechanisms, such as quick freeze and sending access request to OTTs.

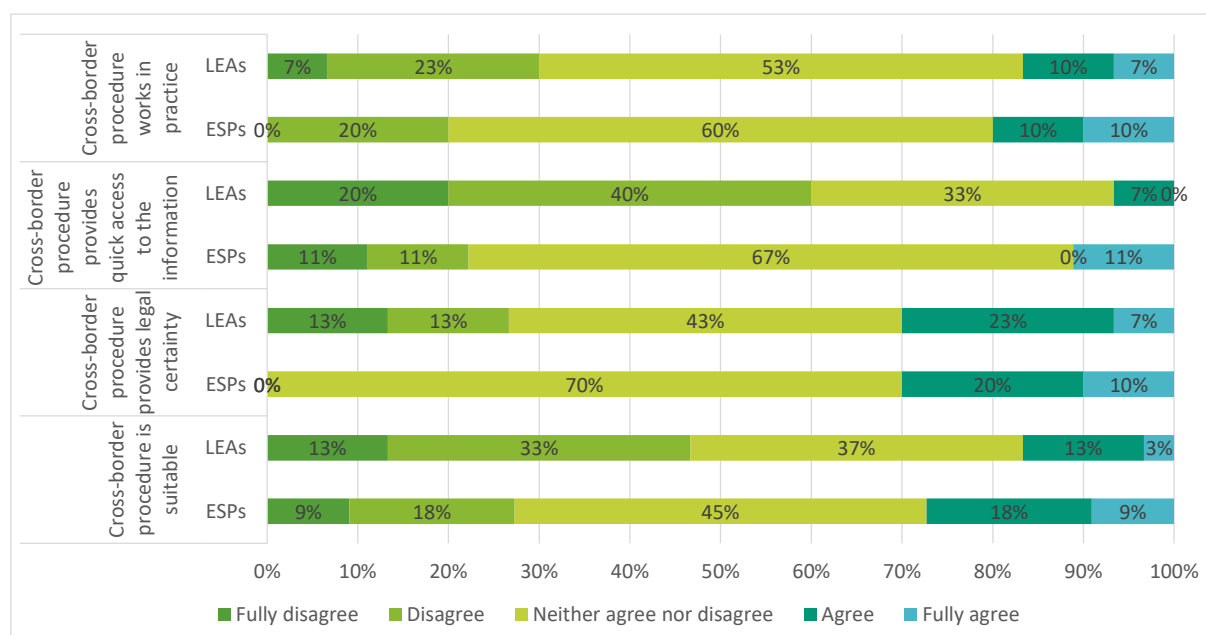
By contrast, stakeholders from Ireland, Italy and Portugal – all of which have general data retention schemes - expressed a certain level of disagreement, criticising the lack of legal certainty (IE, IT), quick access to information (IT, PT) and suitability (IE, IT). These results may be related to the ongoing challenges to national legislation in Ireland and Portugal, which have resulted in legal uncertainty. While other national legislation has been challenged in court (e.g. FR), stakeholders from those other countries expressed lower concerns about the resulting legal uncertainty. In Italy, negative opinions related to the extension of the data retention period for serious crimes, which increased the volume of data to be stored and processed (and costs) for ESPs, and by the comparatively large number of prosecutors in LEA sample (50%), who are somewhat detached from the practical aspects of using data retention systems in investigations.

Cross-border procedures for access to non-content data are far more challenging.

Requests addressed by LEAs to ESPs based in another Member State are not legally possible and are forwarded through the intermediary of the national LEAs where the ESP is incorporated. ESPs do not send the information to the other Member State's requesting LEA but, rather, through that same intermediary authority. This prevents ESPs from differentiating cross-border requests from national requests, while substantially increasing the time for LEAs in the originating country to receive the non-content data requested.

The complexity and length of cross-border procedures for data retention is reflected in the **stakeholders' opinions, which are much more negative than those in respect of national systems**.

Only a handful of stakeholders agreed or fully agreed that such procedures are suitable (20% of the replies of LEAs and ESPs combined), work in practice (18%), provide quick access to the information needed (8%) or legal certainty (35%).

Figure 32: Stakeholders' assessments of cross-border procedures and systems for data retention

Source: Targeted surveys of LEAs and ESPs, Questions 52 and 73 (N=42, i.e. stakeholders from all 10 Member States covered by the Study)

LEAs were slightly more critical than ESPs about the cross-border procedures, which can be attributed to the fact that they experience both sides of the system (presenting requests in another Member States and being the intermediary for LEAs based in another country). LEAs criticised the length of cross-border procedures, noting that they do not provide quick enough access to the information needed and are thus not suitable overall. In addition, as the data retention obligations and periods vary by type of non-content data between Member States, there is a risk that the request cannot be answered because the non-content data requested are not stored or were deleted in the meantime.

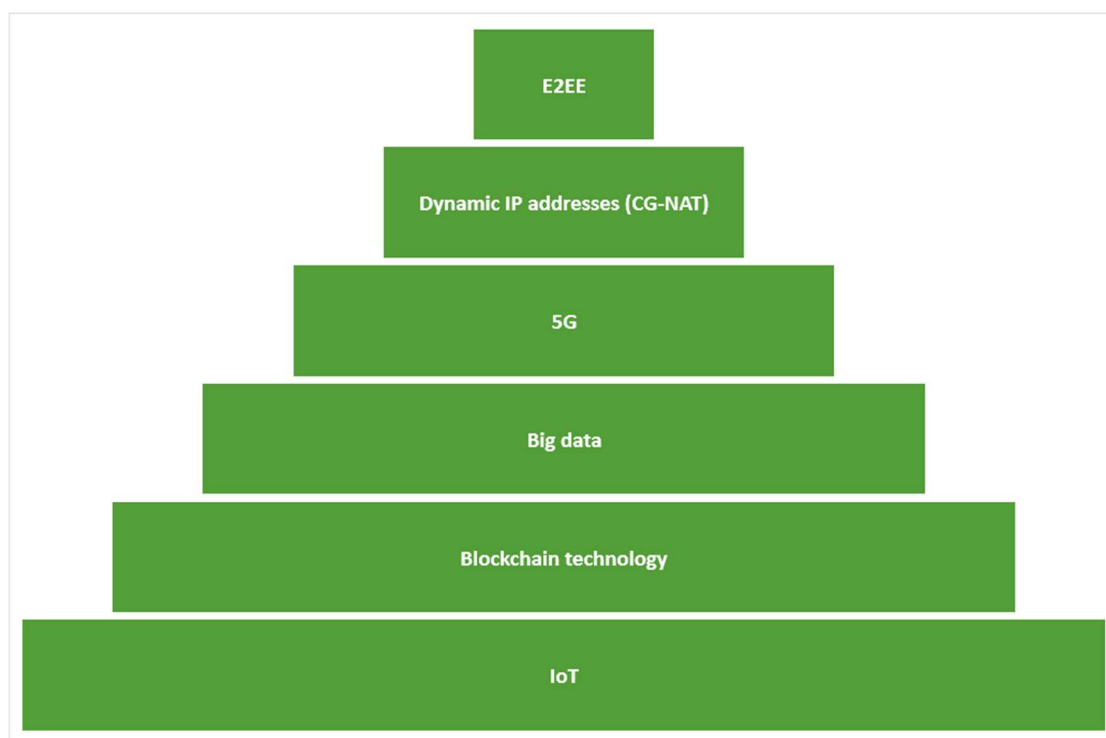
The presence of SPOCs or highly automated processes does not seem to influence LEAs' views of cross-border procedures for data retention, and they do not benefit from IT applications (other than the extraction of data by ESPs).

9.2. TECHNOLOGICAL DEVELOPMENTS AND CONNECTED CHALLENGES

Technological developments such as E2EE, dynamic IP addresses (CG NAT), the deployment of 5G and emergence of the IoT create challenges for the current regulatory and institutional framework on data retention.

In order to gain a better view of the projected impacts of technological developments on data retention, the Study investigated stakeholders' perceptions of the main technological challenges.

When asked about the **most relevant issues for data retention for law enforcement purposes in the present and near future, stakeholders identified E2EE and dynamic IP addresses as the key technological challenges, followed by the introduction of 5G and other related technology applications, such as Big Data, IoT and blockchain** (see Figure 33).

Figure 33: Ranking of technological challenges, LEAs and ESPs combined

Source: Targeted surveys of LEAs and ESPs, Questions 48 and 68, respectively (N=44, multiple answers possible)

LEAs focused more on issues already encountered in their daily investigation activities, as they ranked E2EE and dynamic IP addresses as the two most relevant problems. ESPs, by contrast, were more forward looking, ranking 5G as the most relevant challenge, followed by IP dynamic addresses.

The concerns of LEAs and ESPs do not vary markedly between countries, with the ranking of the issues showing no major changes in different EU Member States. Challenges posed by current and future technological developments are thus not dependent on national data retention schemes and are the same in countries with no data retention obligation and in those with general data retentions schemes.

9.2.1. Current challenges

This section discusses the challenges connected with the increased usage of OTT services and connected problems with E2EE and dynamic IP addresses.

The amount of non-content data relevant to LEAs has increased steadily in recent years: 65% of LEAs affirmed that **the number of requests to access non-content data increased in the last two years at least 'to some extent'** (LEA survey question 63, N=34, in Annex IV). The OTTs consulted confirmed this increasing trend (see section 8.3.1). This growing shift of communications from traditional telecommunication services to OTT services **poses particular challenges for LEAs**. While the ESP survey respondents stated that they have no role in requests for non-content data from communications that occur via an OTT platform, LEAs answers are diverse, showing a degree of unfamiliarity with the processing operations of OTTs (ESP survey question 63 in Annex V; LEA survey question 45 in Annex IV).

Analysis of the current practices highlighted an unequal level of cooperation between LEAs and OTTs across the 10 Member States covered by this Study, with some countries (DE, FR) experiencing good levels of cooperation with OTTs, while others (SI) have more trouble presenting requests and obtaining non-content data. Despite OTTs' efforts to improve

cooperation with LEAs (many organise training sessions with LEAs from all Member States to inform them of the type and period of metadata retained and the functioning of their procedures), the share of unsuccessful requests remains 44% on average (see section 8.3.1). The most frequent reasons for refusal are missing legal requirements (e.g. lack of a valid court order or failure to address the competent authority) and OTTs not having the information requested (they never had it or the retention period has elapsed).

The problem is more relevant for certain data, such as those connected to dynamic IP addresses (port number and timeframe), which are important for LEAs but are not retained by OTTs or are retained only for a short time for commercial or business purposes. LEAs highlighted the non-existent registration of users of OTT services, which could impede future investigations.

The applicability of the e-Privacy Directive to OTT services such as instant messaging services, email web-based services and voice services will likely solve some of these challenges, even if uncertainties persist with respect to the actual impact of these changes. The OTTs consulted are determining the extent of the applicability of the e-Privacy Directive to their services and closely following developments at the CJEU. LEAs are experiencing a set of negative impacts on their daily activities (including the need to involve OTTs as well as ESPs in their investigations, having less non-content data available and longer proceedings – see Question 45 in Annex IV). They hope that the upcoming regulatory changes will bring more clarity and increase the availability of non-content data.

Certain OTTs subject all messages, phone calls, videos and any other form of information exchanged on their platforms to E2EE. This means that the communication is encrypted directly by the sender's device and can only be decrypted by the receiver's device. The ESPs/OTTs involved in the transmission of the communication do not possess the cryptographic keys necessary to decrypt the communication.

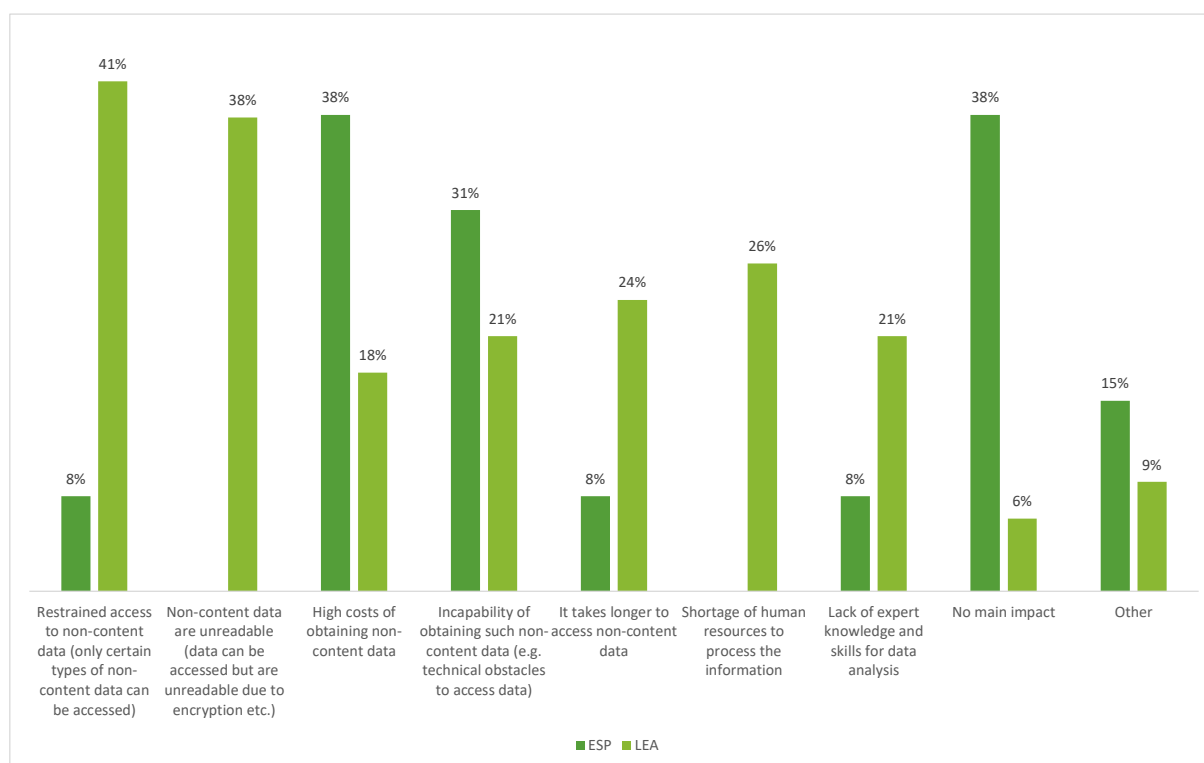
Such E2EE of content data affects access to non-content data. LEAs' and ESPs' responses both show that **E2EE increases the costs of answering the requests to access non-content data** and raises the importance of access to non-content data (see Question 47 in Annex IV and Question 68 in Annex V). Recruiting and integrating experts with sufficient IT knowledge and skills is another common issue raised by the LEAs.

The issue of **retention of dynamic IP addresses** was raised frequently by stakeholders in all Member States. The main challenge connected with the transition to dynamic IP addresses is the fact that internet-linked devices can no longer be identified based solely on their IP address (see section 5.2).

9.2.2. Upcoming challenges

This section discusses the challenges stemming from technological developments such as deployment of 5G, introduction of blockchain, IoT and others. It builds on inputs and suggestions provided by stakeholders via targeted surveys and interviews, complemented by information from the desk research.

Interestingly, while LEAs and ESPs agreed on the relevance of 5G in their practices, their views on the actual impacts are quite different. LEAs identified their top three impacts as restrained access (41%), unavailability of non-content data (38%) and shortage of personnel with the skills to interpret those data (26%). ESPs identified their key impacts as having no impact (42%), high costs (42%) and technical issues in obtaining the required non-content data (33%).

Figure 34: Likely impact of new technological trends (such as 5G or IoT) on access to non-content data

Source: Targeted surveys of LEAs and ESPs, questions 49 and 70, respectively (N=44, multiple answers possible)

While the principle of technology neutrality¹¹⁹ prevents EU legislation from directly helping or hindering particular technologies (especially emerging ones), legislative changes still need to keep pace with technological development. The EECC paves the way to the deployment of the next generation of networks – 5G. Like many other technological developments, 5G network infrastructure poses risks to the security of communications and thus requires a consolidated and coordinated approach among the Member States¹²⁰.

5G will introduce a new service-based architecture, including the complete virtualisation of the Core network¹²¹, network slicing¹²² and much broader use of cloud computing¹²³. 5G is expected to increase the overall security of the network, with the application of the 'security by design' principle, preventing intrusions from external players¹²⁴. Given its complex architecture, vulnerabilities may lead to potentially

¹¹⁹ Technology neutrality is defined as the freedom of individuals and organisations to choose the most appropriate and suitable technology for their needs. Products, services or regulatory frameworks taking into account the principle of technology neutrality neither impose nor discriminate in favour of the use of a particular type of technology. Regulation (EU) No 283/2014 — guidelines for trans-European networks in the area of telecommunications infrastructure, available at: <https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX%3A32014R0283>

¹²⁰ Council of the European Union, Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G, 3 December 2019 (OR. en), 14517/19, available at: <https://www.consilium.europa.eu/media/41595/st14517-en19.pdf>.

¹²¹ The Core network is the central part of the 5G infrastructure, which enables delivery of services over all kinds of networks - wireless, fixed, converged.

¹²² The segmentation of a single physical network into multiple virtual networks in accordance with particular use cases, which allows operators to deploy only the functions necessary to support specific customers and particular market segments.

¹²³ ENISA (2019). ENISA threat landscape for 5G network, available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>

¹²⁴ *Ibid.*

catastrophic security breaches, with consequences not only for individuals but for the security of entire nations.

While many of the technical solutions and standards for 5G networks are still under discussion, several analyses have been carried out on its characteristics and potential threat to security, including implications for law enforcement¹²⁵. Many stakeholders are still unclear about the possible implications of 5G, but nevertheless mentioned several issues as potential challenges (see list below). The available literature provides further basis for such concerns.

An immediate consequence of the introduction of 5G - acknowledged by all stakeholders consulted – also linked to OTTs and NRAs, is **the large increase of potentially relevant information, with related implications for the costs and infrastructure needed to store and process them.**

Encryption is expected to be a key feature of 5G, embedded in its basic architecture. The related problems risk becoming much broader and widespread, with almost all future electronic communications perhaps encrypted (not just OTT services, such as Skype and WhatsApp), reducing the amount of non-content data available to LEAs.

Given the widespread adoption of encryption, **5G is likely to make it harder for ESPs to continue to provide some of the information required under data retention obligations.** For instance, the current network technology uses radio interfaces and protocols that allow ESPs to provide LEAs with many pieces of information in a decrypted form, including non-content data for identification (e.g. **IMSI number**) and localisation of the device. 5G will likely use different interfaces and protocols for this information (Subscription Permanent Identifier (SUPI), or Subscription Concealed Identifier (SUCI)), which are encrypted¹²⁶. Non-content data normally available via data retention would thus be lost to law enforcement and judicial authorities (primarily the identification information, while data such as location, date, time, call duration are likely to remain available in decrypted form). 5G will have strict authentication processes (to identify a user before access is granted), such as false base detection, that will make it harder for law enforcement to investigate without being detected (the IMSI catchers necessary for interception of mobile devices and location of suspects/victims would be detected)¹²⁷.

The **fragmented and virtual architecture of 5G presents a further challenge for LEAs.** Until now, when carrying out a lawful interception, LEAs deal with a limited number of network providers. With 5G network slicing technology, however, network and service providers may not - unless they are obliged to do so - have a complete copy of the information available, which would make access to non-content data impossible. 5G architecture means that monitoring communications in the future might require the cooperation of numerous network providers, both at home and abroad, each under different jurisdictions. This would raise challenges for cross-border cooperation and procedures.

Another illustration of 5G fragmented architecture is **multi-access edge computing (MEC)**¹²⁸. To improve timely response, MEC will allow mobile phone networks to store and process contents in decentralised clouds in the vicinity of network users, which can directly communicate with each other. Information will not necessarily be directed via central

¹²⁵ ENISA (2019); NIS Cooperation Group (2020). Cybersecurity of 5G networks – EU Toolbox and risk mitigating measures, available at: <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

¹²⁶ <http://www.techplayon.com/5g-identifiers-supi-and-suci/>.

¹²⁷ The same issues have been reported by the Council of the European Union. See: Council of the European Union (2019). Law enforcement and judicial aspects related to 5G, Note (8983/19), available at: <https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf>

¹²⁸ MEC is a network architecture concept that enables cloud computing capabilities and an IT service environment at the edge of the cellular network, and, more generally, at the edge of any network. The basic idea behind MEC is that by running applications and performing related processing tasks closer to the cellular customer, network congestion is reduced and applications perform better. See: <https://www.etsi.org/technologies/multi-access-edge-computing>.

nodes, where data are currently retained. It is therefore possible that as network functions and components that were previously physical become virtual, existing measures to protect the confidentiality of data retention procedures will no longer work (e.g. protection against access or altering target lists by having specifically vetted staff to carry out the procedures on the national territory, physical protection measures such as access restrictions).

IoT and blockchain did not emerge as key challenges for stakeholders. As yet, the direct implications of IoT for law enforcement purposes are uncertain and mixed with those related to 5G. A logical challenge of the introduction of IoT is larger amounts of non-content data available. LEAs see this both as an advantage and a disadvantage. The development of IoT, especially in cars, has been welcomed by LEAs, as it gives a tremendous amount of information, in particular on location data. Although such large amounts of non-content data benefit criminal investigations, the wealth of information connected to SIM cards from regular mobile phones and those in the vehicles also create confusion (see challenges related to IMSI number above).

Challenges related to IoT services often stem from the cross-border nature of such services (e.g. cars roam all over the world and IoT services are usually offered through one centralised platform). While ESPs struggle to assign data retention rules to their IoT services offered across different jurisdictions, LEAs struggle to obtain such information, as cross-border cooperation mechanisms are needed.

Finally, several LEAs emphasised that the narrow scope of definition of the ECSs means that IoT services are not yet covered by the current legislation, providing uncertainty as to the success of their requests. Overall, there is a need for comprehensive legislation that can provide an unambiguous understanding and treatment of these issues.

Stakeholders consulted (especially LEAs) identified some technical challenges for **blockchain**, mostly related to the transmission of data packages. However, its adoption has been quite limited to date and LEAs do not perceive it as a challenge in the near future.

While the challenges described above refer to access to non-content data, it is likely that many of these will also have implications for content data and interceptions.

9.3. CONCLUSION

This section presents the overall conclusions of the Study on: (i) **the legal framework** (section 9.3.1), (ii) **the practices for retention of and access to data** (sections 9.3.2 to 9.3.7) in the 10 Member States covered under this Study, and (iii) **the impact of technological developments on data retention schemes** (section 9.3.8). By comparing the practices of ESPs and OTTs with the needs of LEAs, this section seeks to understand the areas of convergence between their various views and needs and the outstanding challenges in relation to national data retention schemes.

The absence of common definitions, reporting practices and publicly available statistics make it very **difficult to fully understand the dimensions of the issue or to compare the (very limited) evidence between Member States**. Statistics from operators (both ESPs and OTTs) are not comparable, complicating the identification of trends across Member States' practices and/or communication providers. The lack of comprehensive information, together with the limited response rate from stakeholders, limits the results of this Study and does not allow for a thorough assessment of the benefits and constraints of data retention.

9.3.1. Regulatory and institutional framework and its challenges

The regulatory and institutional framework for data retention in the 10 Member States included in the Study **is fragmented**. In seven of the 10 Member States examined, national laws stipulate a legal obligation for ESPs to retain non-content data (EE, ES, FR, IE, IT, PL, PT). In three Member States, where national data retention laws were repealed

(AT, SI) or are not currently enforced (DE), LEAs can only access non-content data that are kept by ESPs for their own commercial or business purposes.

The absence of national legal frameworks on data retention poses a risk of reduced access to important evidence for investigation and prosecution of crimes by LEAs. Existing differences in national laws also seem to raise issues for cross-border investigations, where LEAs are faced with different types of data and retention periods between countries.

In most Member States, apart from Austria, Poland and Spain, desk research revealed **some form of legal or political changes** regarding data retention frameworks, with four Member States¹²⁹ having cases pending before the CJEU (DE, EE, FR, IE). In countries that impose mandatory data retention obligation on ESPs, **defence lawyers have challenged the admissibility of non-content data as evidence in criminal proceedings**. As a result, LEAs in some countries are more cautious when making access requests in case convictions are overturned. This is particularly true for Ireland, where the national legislation on data retention remains valid but is not used to its full extent by LEAs.

There is no EU or national legal framework imposing a general data retention obligation on OTTs for law enforcement purposes. OTTs are an example of technology evolving more rapidly than legislation. They are exempt from data retention obligations, despite the increasing share of communications passing through their services. This situation will likely change from 21 December 2020, when the e-Privacy Directive and potentially its transposing legislation will also apply to OTTs. There is a high degree of uncertainty for the OTTs, who are closely following the ongoing proceedings at the CJEU.

In the majority of the Member States studied, the national legislative framework provides for access to non-content data by police authorities (including the military police, in some cases) and judicial authorities (public prosecutors and judges). In a few Member States (AT, EE, ES, PL), national intelligence agencies can also access data for law enforcement purposes. Many Member States have expanded the right to access retained non-content data to other types of national authorities, most commonly tax, customs or competition authorities, where criminal offences fall under the remit of that authority.

The actions of LEAs and ESPs are subject to the **supervision by national authorities**. In most Member States (AT, DE, EE, ES, IE, IT, PL, SI), competences and responsibilities are shared between NRAs and DPAs, with DPAs being primarily responsible for ensuring that personal data are processed in accordance with the relevant rules and safeguards, and NRAs primarily responsible for the oversight of the telecommunications sector, including ESPs' obligations under national data retention laws, where such laws exist. Although this overlap of competences could potentially raise issues, **stakeholders did not note any major problems**. However, the scope of the competences of the national supervisory authorities over OTTs is not always clear from the national telecommunications regulations.

9.3.2. Types of non-content data

The Study found that the **needs of LEAs in all Member States broadly overlap with the retention practices of ESPs, as ESPs tend to retain most types of non-content data, with a few notable exceptions, such as port numbers for dynamic IP addresses and - in some cases - location data**.

In countries with a mandatory data retention scheme, the types of data that ESPs are required to retain under the national laws are similar, namely subscriber, traffic and location data, with the notable exception of port numbers for dynamic IP addresses. There is no requirement to retain port numbers in Estonia and there are differences in the interpretation of the Irish law between ESPs and LEAs. A key difference is the amount of detail provided by data retention laws on the types of data to be retained. In Member States without a legal obligation to retain non-content data, LEAs rely on the data stored by ESPs for business purposes (e.g. business, commercial, invoicing, marketing, network

¹²⁹ Requests for preliminary rulings before the CJEU have also been filed by the courts in Belgium, which is not covered under this Study, and the UK, which is no longer an EU Member State.

security). In practice, the type of non-content data retained by each individual ESP for business purposes varies depending on its own terms of use. However, even in countries with no mandatory data retention schemes, the same types of non-content data are stored for at least one internal purpose.

While retained data points are broadly the same in all Member States, their classification as subscriber, traffic, and location data changes between countries. This can result in diverging rules across Member States regarding retention periods and access to the same type of data, complicating cross-border cases, in particular.

The most frequent data points requested by LEAs are subscriber data and traffic data, such as telephone number, physical address, date and time of the communication and location of the equipment or line at start of communication. However, LEAs request all types of non-content data identified in the Study. Certain types of data are more frequently requested for particular types of crimes and multiple data points are requested within the course of a single investigation. For example, IP addresses are requested much more frequently for the investigation of online fraud, cybercrimes, child sexual exploitation and other cyber-enabled crimes.

In general, **LEAs across all Member States frequently request non-content data**. Over 50% of LEA survey respondents had requested data in at least 60% of investigations over the last two years. **Requests for non-content data are rarely unsuccessful**, with the majority of both LEA and ESP respondents stating that requests are unsuccessful in less than 20% of cases. Portugal is an exception, where differences in the interpretation of the law between ESPs and LEAs have led to high unsuccessful request rates.

9.3.3. Retention periods of data

Generally, the mandatory **data retention period** for law enforcement purposes is 12 months, except in Ireland (12 months for internet data, 24 months for telephone data) and Italy. In Italy, data are retained for 72 months, to be accessed in cases of terrorism or other serious crimes. In practice, as ESPs operating in Italy cannot know in advance the types of crime for which data might be requested in the future, they retain all non-content data for 72 months by default. The data retained within the 72-month period is only transferred to competent LEAs for the investigation of serious crimes. For other types of crimes, the request for access must be made within the time limits set by the national legislation on data retention (i.e. 12 months for internet data and 24 months for telephone data).

Retention periods for non-content data retained for business purposes are unclear and vary from one ESP to another within the maximum data retention periods prescribed by the national legislation. Most of the ESPs consulted did not provide precise information on how long they use non-content data for internal purposes, citing business confidentiality reasons. Overall, the length of the retention period varies depending on the specific internal purpose for which the data are needed (e.g. commercial, invoicing, marketing, network security) and the regulatory requirements. For the purposes of LEAs, longer and clear data retention periods can be identified for invoicing purposes due to the legal thresholds for invoice contestation (on average three months). In addition, retention periods for business purposes can vary depending on the type of data. For example, subscriber data are usually retained throughout the timeframe of the contract between clients and ESPs (which could be several years), as these data are necessary for the subscription and provision of services to the client. The same is true for OTTs. The lack of clarity and variations in the length of the retention periods for business purposes is particularly problematic for LEAs in countries without mandatory data retention schemes, as they cannot know with certainty what non-content data will be available or for how long.

Where mandatory retention periods have been reduced (e.g. due to annulment of national data retention schemes or changes to data retention laws), **LEAs were able to adapt their practices** and are generally able to understand the data they need, obtain authorisation (if needed) and make requests in line with the national legal framework. In

the case of Germany, LEAs have managed to adapt their procedures so as to obtain judicial approval and access non-content data within one week. IT platforms, SPOCs and other automated procedures strongly support such efficient procedures.

Nevertheless, some Member States where national data retention laws were struck down following the annulment of the DRD (DE, SI) have registered a decrease in requests for non-content data. **LEAs in these countries cannot access certain types of non-content data, as they have no business value or are no longer available.** The 'problematic' data points are identification (e.g. IP addresses and port numbers for dynamic IP addresses) and location data that are generally not retained for invoicing. German LEAs also indicated difficulties in accessing location data, which are rapidly deleted as they have no business value for ESPs.

Many crimes committed via electronic means in Member States without mandatory data retention schemes risk not being prosecuted due to shorter retention periods. This is particularly true for crimes that depend on non-content data but take longer to investigate or that may only become apparent through the course of the investigation, such as crimes with an online dimension (e.g. child sexual exploitation, child pornography, cyberattacks), organised crime and similar. Non-content data could also be determining evidence in cases of crimes such as insider misconduct and environmental crimes. Too-short retention periods seem to be the main reason behind unsuccessful access requests.

Stakeholder consultation shows that non-content data do not solely serve as evidence but also as a first step in finding more substantial information through the identification of further elements such as a device, a person, or the location of a crime. Non-content data can clarify facts and thus reinforce a case and potentially lead to other pieces of evidence. With the help of non-content data, LEAs can identify more victims and potential perpetrators beyond the case at hand, which is only possible by obtaining data going sufficiently back in time. In Member States where LEAs have to rely on data retained by ESPs for business and commercial purposes, **many crimes risk not being detected.**

9.3.4. Storage of data

Secure storage of non-content data falls under the responsibility of both ESPs and OTTs. Security requirements imposed on ESPs for the storage of data are broadly the same across Member States, as they relate to GDPR requirements and remain technologically neutral. Some Member States, however, impose further security requirements such as location requirements and the separation of servers for business and data retention purposes (DE, IT, PT). In such cases, security requirements for retention of non-content data for law enforcement purposes are more stringent than for business purposes, resulting in increased protection of individuals' personal data. The majority of ESPs and OTTs consulted highlighted the high costs involved, for which they receive no form of reimbursement.

ESPs in Member States with general data retention schemes – and in those without – expressed discontent about the high costs incurred for the retention of data for law enforcement purposes (e.g. costs of infrastructure, maintenance, IT equipment, manpower for ensuring secure storage of non-content data and timely responses to LEA requests). ESPs and OTTs highlighted the need for cost recovery mechanisms, arguing that they perform a public interest mission that requires high investment with no business return. Reimbursement schemes are rare and, even when implemented, only partially cover the costs for ESPs.

9.3.5. Restrictions on the right to access non-content data

Most Member States restrict access to non-content data to certain specific serious crimes. In five Member States, access to non-content data is strictly limited to specific types of crimes, either listed in the legislation (DE, SI, PT) or the most serious crimes based on the custodial sentence (IE, ES). In four other Member States (EE, FR, IT, PL),

access is possible for any type of crime, including misdemeanours. However, stakeholder consultation highlighted that, in practice, non-content data are only requested when absolutely necessary, taking into account the severity of the crime and the availability of alternative evidence. **Restricting the right to access non-content data to serious crimes does not seem to pose problems in the Member States** as, in practice, data are chiefly required for those crimes where it represents either a key piece of evidence (e.g. cybercrime or child pornography) or a leading element to discover key evidence.

The majority of access requests are targeted rather than large-scale, limiting access to non-content data to a specific person or device. As a rule, large-scale requests occur in urgent situations, such as a terrorist attack or a missing person, and are formulated in a limited way in terms of time or area, for practical reasons (e.g. considerable amount of data that results from such requests and the difficulty in finding relevant evidence in broad datasets).

9.3.6. Procedure to access data

As a rule, the procedure that LEAs must follow to access non-content data **is regulated and incorporates several safeguards to limit excessive and general access to non-content data**. In some countries, access to subscriber data is less strict than access to other types of non-content data (AT, DE, EE, ES, PT).

The **actions of LEAs in this respect are supervised**. Eight of the 10 Member States (AT, DE, EE, ES, FR, IT, PT, SI) have some form of ex-ante authorisation for LEAs to access non-content data, either through a judicial authorisation or an order by the public prosecutor. Member States that do not request ex-ante authorisations instead foresee ex-post supervision.

Where ESPs and LEAs have developed automated procedures and processes such as IT platforms and SPOCs, these facilitate secure access to and transmission of data. SPOCs are particularly highly regarded by LEAs and ESPs/OTTs and contributes greatly to the effective functioning of national systems. SPOCs eliminate the need for an elaborate vetting process to verify the source of the request and decrease the costs of answering access requests. Several stakeholders would **welcome further standardisation of procedures and the use of SPOCs**, which as yet are used in only two of the 10 Member States (FR, DE). Estonia has implemented a system for secure request and processing of data between LEAs and ESPs based on the X-Road infrastructure.

Access procedures are particularly challenging in cross-border investigations. Differences in national data retention regimes, types of data and retention periods, as well as lack of knowledge of practices in other Member States are noted as the main obstacles to investigation and prosecution of cross-border crimes for all stakeholders involved. LEAs highlighted the difficulties linked to the lack of harmonised rules, the excessive length of time to obtain non-content data and lack of knowledge of other Member States' regulations and practices. ESPs and OTTs for their part pointed to different security requirements across the EU for centralised storage of information (e.g. data localisation requirements) and different retention regimes as their key challenges.

9.3.7. Alternatives to mandatory data retention

Few alternatives to mandatory data retention were identified. An alternative available to LEAs in Member States with no general mandatory data retention schemes is to obtain non-content data stored by the ESPs for business purposes, as is the case in Austria, Germany and Slovenia. Otherwise, **quick freeze is often the only alternative for LEAs** where retained data are not available. However, LEAs argue that these data cannot fully replace general and mandatory data retention, as national legislation limits its use to certain types of crime and its success depends on whether or not non-content data are even retained by ESPs.

9.3.8. Technological challenges

Existing technological challenges remain an issue. It is especially challenging for LEAs to obtain **IP addresses, particularly dynamic IP addresses assigned to multiple users at the same time through CG NAT**, despite their growing importance in the field of cybercrime, for example. Overall, LEA and ESP survey respondents ranked the use of dynamic IP addresses and CG NAT as the second biggest technological challenge in accessing/providing non-content data for law enforcement purposes. Port numbers for dynamic IP addresses are not retained by many ESPs in Germany, Ireland or Estonia. Even where port numbers are retained, LEAs also need very precise time stamps (to the second) for ESPs to identify the user behind a connection.

Upcoming technological developments (such as 5G and IoT) will likely complicate existing issues in data retention.

5G is expected to increase the share of E2EE communication, which in turn is likely to reduce the volume of non-content data available to LEAs via data retention schemes, as ESPs would no longer process – or retain – such data. 5G will also bring about new challenges, as its service-based architecture will make it harder for ESPs to provide certain types of data that are currently retained, such as IMSI numbers. Cross-border provision of communication services is expected to further increase with the implementation of 5G-enabled IoT applications. This will likely **broaden the need for cross-border investigations and cooperation between European LEAs**, for which current procedures are not suitable. Upcoming technological challenges might thus exacerbate the need for an EU-wide approach to data retention.

REFERENCES

References at EU level

Legal documents

- Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391–407, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT>.
- Commission proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, COM(2005) 438 final, 21.9.2005, [http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2005/0438/COM_COM\(2005\)0438_EN.pdf](http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2005/0438/COM_COM(2005)0438_EN.pdf).
- Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Official Journal C 197, 12.7.2000, pp. 1-2, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000F0712%2802%29>
- Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Official Journal L 210, 6.8.2008, pp. 1-11, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0615>.
- Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, pp. 89-100, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006F0960>.
- Council of Europe Convention on Cybercrime, Treaty N. 185, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>.
- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), Official Journal L 108, 24.4.2002, p. 33, <https://eur-lex.europa.eu/eli/dir/2002/21/2009-12-19>.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31.07.2002, pp. 0037-0047, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>.
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13.4.2006, pp. 54-63, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024>.
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal L 337, 18.12.2009, pp. 11-36, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136>.
- Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, pp. 1-36, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>.
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of

criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89-131, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680>.

- Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, pp. 36-214, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.321.01.0036.01.ENG&toc=OJ:L:2018:321:FULL.
- European Union Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations, Official Journal C 024, 23.01.1998, pp. 0002-0022, [https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:41998A0123\(01\)](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:41998A0123(01)).
- 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, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN>.
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017)010 final – 2017/03 (COD), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>.
- 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, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN>.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1-88, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

Literature

- Bruni, A. (2020). The NeverEnding story: lack of common security protocols in the electronic communication sector. Retrieved from: <https://www.law.kuleuven.be/citip/blog/the-neverending-story-lack-of-common-security-protocols-in-the-electronic-communication-sector/>.
- Ducuing, C. (2019). Legal principles behind technical complexities: the proposal from the Commission for a C-ITS Delegated Regulation. Retrieved from: <https://www.law.kuleuven.be/citip/blog/legal-principles-behind-technical-complexities-the-proposal-from-the-commission-for-a-c-its-delegated-regulation/>.
- ENISA (2019). ENISA threat landscape for 5G network, November 2019. Retrieved from: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>
- European Union Agency for Fundamental Rights and Council of Europe (FRA) (2018). Handbook on European data protection law, 2018 edition. Luxembourg: Publications Office of the European Union.
- Formici, G. (2019). ECJ, the floor is yours! The never ending story between data retention and right to privacy. Retrieved from: <https://www.law.kuleuven.be/citip/blog/ecj-the-floor-is-yours-the-never-ending-story-between-data-retention-and-right-to-privacy/>.
- Levin, S. L. and Schmidt, S. (2014). IPv4 to IPv6: Challenges, solutions, and lessons. *Telecommunications Policy*, 38(11), 1059-1068. Retrieved from: <https://doi.org/10.1016/j.telpol.2014.06.008>
- Vogiatzoglou, P. (2019.). Data retention tales: The Council of the EU strikes back. Retrieved from: <https://www.law.kuleuven.be/citip/blog/data-retention-tales-the-council-of-the-eu-strikes-back/>.
- Vogiatzoglou, P. (2017). Mass surveillance and the European Courts. Retrieved from: <https://www.law.kuleuven.be/citip/blog/mass-surveillance-and-the-european-courts/>.

- Vogiatzoglou, P. (2020). One more time with feeling: the latest AG Opinions on data retention and national security. Retrieved from: <https://www.law.kuleuven.be/citip/blog/one-more-time-with-feeling-the-latest-ag-opinions-on-data-retention-and-national-security/>.
- Vaughan-Nichols, S.J. (2020). *Static vs. dynamic IP addresses*. Avast Academy.

Case law

CJEU

- Advocate General's Opinion in Case C-623/17 *Privacy International*, 15.01.2020.
- Advocate General's Opinion in Joined Cases C-511/18 *La Quadrature du Net and Others* and C-512/18 *French Data Network and Others*, 15.01.2020.
- Advocate General's Opinion in Case C-520/18 *Ordre des barreaux francophones et germanophone and Other*, 15.01.2020.
- Advocate General's Opinion in Case C-746/18 *H.K. v Prokuratuur*, 21.01.2020.
- Case C-202/09, *Commission v Ireland*, 16.11.2009.
- Case C-207/16 *Ministerio Fiscal*, 02.10.2018.
- Case C-512/18 *French Data Network, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs v Premier ministre, Garde des Sceaux, Ministre de la Justice* (pending).
- Case C-520/18 *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministres* (pending).
- Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (pending).
- C-746/18 *H.K. v Prokuratuur* (pending).
- Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others*, 08.04.2014.
- Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21.12.2016.
- Joined cases C-793/19 and C-794/19 *SpaceNet a.o.* (pending).
- C-140/20 *Commissioner of An Garda Síochána and Others* (pending).

ECtHR

- *Benedik v. Slovenia*, Application No, 62357/2014, 24 April 2018.
- *Big Brother Watch and Others v. The United Kingdom*, Application Nos. 58170/13, 62322/14 and 24960/15, 13 September 2018.

Other documents

- Apple Transparency Report (n.d.). Retrieved from: <https://www.apple.com/legal/transparency/choose-country-region.html>.
- Apple's guidelines for law enforcement requests, Outside the United States.
- BEREC (2016). Report on OTT services, BoR (16) 35. Retrieved from: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5751-berec-report-on-ott-services_0.pdf.
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (2016). Online platforms and the Digital Single Market: Opportunities and challenges for Europe, COM(2016) 288/2. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288>.
- Council of the European Union (2019). Conclusions of the Council of the European Union on retention of data for the purpose of fighting crime – Council Conclusions (6 June 2019), Brussels, 6 June 2019 (OR. en), 10083/19. Retrieved from: <https://data.consilium.europa.eu/doc/document/ST-10083-2019-INIT/en/pdf>.

- Council of the European Union (2017). Conclusions of the Council of the European Union (23 June 2017), Brussels, 23 June 2017 (OR. en), EUCO 8/17, CO EUR 8 CONCL 3. Retrieved from: <https://www.consilium.europa.eu/media/23985/22-23-euco-final-conclusions.pdf>.
- Council of the European Union (2019). Council Conclusions on the significance of 5G to the European economy and the need to mitigate security risks linked to 5G, 3 December 2019 (OR. en), 14517/19. Retrieved from: <https://www.consilium.europa.eu/media/41595/st14517-en19.pdf>.
- Council of Europe (2018). Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments. Cybercrime Convention Committee, T-CY (2018)26.
- Eurojust (2018). European Investigation Order. Retrieved from: <http://www.eurojust.europa.eu/doclibrary/corporate/Infographics/European%20Investigation%20Order/2018-European-Investigation-Order.pdf>.
- European Commission (2014). MEMO, Frequently Asked Questions: the Data Retention Directive, Brussels, 8 April 2014. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_14_269.
- European Parliament (2019). Data retention for the purposes of prevention, investigation and prosecution of crime. Retrieved from: <http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-data-retention-directive/06-2019>.
- Facebook information for Law Enforcement Authorities (n.d.). Retrieved from: <https://www.facebook.com/safety/groups/law/guidelines/>.
- Facebook Transparency reports (n.d.) Retrieved from: <https://transparency.facebook.com/government-data-requests>.
- Google Transparency Report (n.d.) Retrieved from: <https://transparencyreport.google.com/user-data/overview?hl=en>.
- GSM Association (GSMA) (2020). Access to mobile services and proof of identity 2020: The undisputed linkages. Retrieved from: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf.
- Microsoft Law Enforcement Requests Report (n.d.). Retrieved from: <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>.
- Milieu Consulting (2017). Study assessing the completeness and conformity of measures of Member States to transpose Council Framework Decision 2006/960/JHA ('The Swedish Initiative'). Specific Contract No. 2016.01 (HOME-2016-FW-LECO-0001), October 2017.
- NIS Cooperation Group (2020). Cybersecurity of 5G networks – EU Toolbox and risk mitigating measures. Retrieved from: <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.
- Privacy International (2017). National data retention laws since the CJEU's Tele-2/Watson Judgment. Retrieved from: https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf.
- Vodafone Group Plc (2017). Country by country disclosure of law enforcement assistance demands 2016-17. Retrieved from: https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/vodafone_drf_law_enf_ormcement_disclosure_country_demands_2016-7.pdf.
- <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-01/cp200004en.pdf>.
- <https://ec.europa.eu/digital-single-market/en/telecoms>.

References at Member State level

National legal documents

Austria

- Code of Criminal Procedure, Federal Law Gazette 631/1975, last amended by Federal Law Gazette I 24/2020, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326>.
- Data Protection Act, Federal Law Gazette I 136/2001, last amended by Federal Law Gazette I 14/2019, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597>.
- Data Security Regulation, Federal Law Gazette II 402/2011, last amended by Federal Law Gazette II 228/2016. EU Police Cooperation Act, Federal Law Gazette I 132/2009, last amended by Federal Law Gazette I 104/2019, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006630>.
- Extradition and Legal Assistance Act, Federal Law Gazette 529/1979, last amended by Federal Law Gazette I 20/2020, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002441>.
- Federal Criminal Police Office Act, Federal Law Gazette I 22/2002, last amended by Federal Law Gazette I 118/2016, <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001745>.
- Federal Law on International Police Cooperation (Police Cooperation Act - PolKG), Federal Law Gazette II No 402/2011, amended by Federal Law Gazette II No 228/2016.
- Federal Tax Code, Federal Law Gazette 194/1961, last amended by Federal Law Gazette I 23/2020, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003940>.
- Financial Criminal Act, Federal Law Gazette 129/1958, last amended by Federal Law Gazette I 23/2020, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003898>.
- General Civil Code, Judicial Law Collection 946/1811, last amendment by Federal Law Gazette I 16/2020, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001622>.
- Law on Judicial Cooperation in Criminal Matters with the Member States of the European Union, Federal Law Gazette I 36/2004, last amendment by Federal Law Gazette I 20/2020, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003339>.
- Law on the Federal Office for Corruption Prevention and Anti-Corruption, Federal Law Gazette I 72/2009, last amendment by Federal Law Gazette I 111/2019, <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006390>.
- Military Powers Act, Federal Law Gazette I 86/2000, last amendment by Federal Law Gazette I 102/2019, <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20000864>.
- Police Cooperation Act, Federal Law Gazette I 104/1997.
- (Police) State Protection Act, Federal Law Gazette I 5/2016, last amendment by Federal Law Gazette I 32/2018,

<https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009486>.

- Public Prosecutors Act, Federal Law Gazette 164/1986, last amendment by Federal Law Gazette I 32/2018, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000842>.
- Security Police Act, Federal Law Gazette 566/1991, last amendment by Federal Law Gazette I 113/2019, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792>.
- Telecommunications Act, Federal Law Gazette I 70/2003, last amendment by Federal Law Gazette I 23/2020, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849>.

Estonia

- Elektroonilise side seadus (*Electronic Communications Act*), <https://www.riigiteataja.ee/en/eli/513012020007/consolide>.
- Isikuandmete kaitse seadus (*Personal Data Protection Act*), <https://www.riigiteataja.ee/en/eli/523012019001/consolide>.
- Julgeolekuasutuste seadus (*Security Authorities Act*), <https://www.riigiteataja.ee/en/eli/ee/514112013020/consolide/current>.
- Kaitseväge korralduse seadus (*Estonian Defence Forces Organisation Act*), <https://www.riigiteataja.ee/en/eli/ee/530102013067/consolide/current>.
- Kaitseväge põhimäärus (*Statute of the Estonian Defence Forces*), <https://www.riigiteataja.ee/akt/117122019011?leiaKehtiv>
- Karistusseadustik (*Penal Code*), <https://www.riigiteataja.ee/en/eli/ee/519012017002/consolide/current>.
- Korrakaitse seadus (*Law Enforcement Act*), <https://www.riigiteataja.ee/en/eli/525032019010/consolide>.
- Kriminaalmenetluse seadustik (*Code of Criminal Procedure*), <https://www.riigiteataja.ee/en/eli/ee/530102013093/consolide/current>.
- Politsei ja piirivalve seadus (*Police and Border Guard Act*), <https://www.riigiteataja.ee/en/eli/ee/512112013003/consolide/current>.
- Sideettevõtjale sõnumite ülekandmise ja teabe andmise kulude hüvitamise kord (*Procedure for Compensating the Communications Undertaking for the Costs of Transmitting Messages and Providing Information*), <https://www.riigiteataja.ee/akt/920593>
- Tsiviilkohtumenetluse seadustik (*Code of Civil Procedure*), <https://www.riigiteataja.ee/en/eli/ee/513122013001/consolide/current>.
- Õiguskantsleri seadus (*Chancellor of Justice Act*), <https://www.riigiteataja.ee/en/eli/ee/530102013051/consolide/current>.
- Väärteomenetluse seadustik (*Code of Misdemeanour Procedure*), <https://www.riigiteataja.ee/en/eli/ee/515052014001/consolide/current>.

France

- Code de la défense (*Code of Defence*), <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307>.
- Code de la sécurité intérieure (*Code of Interior Security*), <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000025503132>
- Code de procédure pénale (*Code of Criminal Procedure*), <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154>.

- Code des postes et des communications électroniques (*Code on Postal and Electronic Communications*), <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987>.
- Décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques (*Decree no. 2006-358 on the retention of data from electronic communications*), <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000637071&categorieLien=id>.
- Décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (*Decree no. 2011-219 on the retention and communication of data allowing the identification of any person who contributed to the creation of online content*), <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&categorieLien=id>.
- Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (*Decree no. 2015-1185 designating the specialised intelligence services*), <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031239603&categorieLien=id>.
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (*Act for trust in the digital economy*), <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000801164>.
- Loi n° 2015-912 du 24 juillet 2015 relative au renseignement (*2015 Intelligence Act*), <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id>.

Germany

- Abgabeordnung (*Fiscal Code*), https://www.gesetze-im-internet.de/ao_1977/.
- Bundesdatenschutzgesetz (*Federal Data Protection Act*), https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html.
- Bundeskriminalamtgesetz (*Federal Criminal Police Office Act*), https://www.gesetze-im-internet.de/bkag_2018/.
- Gesetz über das Zollkriminalamt und die Zollfahndungsämter (*Act on the Customs Criminal Office and the Customs investigators*), <https://www.gesetze-im-internet.de/zfdg/BJNR320210002.html>.
- Gesetz über die Bundespolizei (*Federal Police Act*), https://www.gesetze-im-internet.de/bpgs_1994/.
- Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (*Act for the Introduction of a retention obligation and a maximum time for retention of traffic data*), https://www.bmjbv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/BGBl_Hoechstspeicherfrist.pdf;jsessionid=08AAFCFAF011441D16FE1385705299B2B.2_cid334?__blob=publicationFile&v=3.
- Strafprozessordnung (*Code of Criminal Procedure*), <https://www.gesetze-im-internet.de/stpo>.
- Telekommunikationsgesetz (*Telecommunications Act*), https://www.gesetze-im-internet.de/tdg_2004/.
- Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (*Regulation on the technical and organisational implementation of measures of surveillance of telecommunications*), https://www.gesetze-im-internet.de/tdg_v_2005/BJNR313600005.html.

Ireland

- Communications (Retention of Data) Act 2011, Number 3 of 2011, <http://www.irishstatutebook.ie/eli/2011/act/3/enacted/en/html>.

- Competition Act 2002, Number 14 of 2002, <http://www.irishstatutebook.ie/eli/2002/act/14/enacted/en/html>.
- Criminal Justice (Surveillance) Act 2009, Number 19 of 2009, <http://www.irishstatutebook.ie/eli/2009/act/19/enacted/en/html>.
- Interception of Postal Packets and Communications Messages (Regulation) Act 1993, Number 10 of 1993, <http://www.irishstatutebook.ie/eli/1993/act/10/enacted/en/html>.

Italy

- Conversion Law 155/2005, Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale (Conversion into law, with modifications, of Law Decree 27 July 2005 no. 144, containing urgent measures to fight international terrorism), <https://www.camera.it/parlam/leggi/05155l.htm>.
- Criminal Procedure Code, 1988, Codice di procedura penale (Criminal Procedure Code), Decree of the President of the Republic 447/1988, <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447>.
- Data Protection Code, 2003, Codice in materia di protezione dei dati personali (Data Protection Code), Legislative Decree 196/2003, <https://www.camera.it/parlam/leggi/deleghe/Testi/03196dl.htm>.
- Decree Law 7/2015, 2015, Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione (Urgent measures for the fight against terrorism, also of international nature, and prorogation of the international missions of armed and police forces, cooperation initiatives for the development and support of the reconstruction processes and participation in initiatives of international organisations to consolidate peace and stabilisation processes), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2015-02-19&atto.codiceRedazionale=15G00019>.
- Decree Law 149/2017, 2017, Disposizioni di modifica del Libro XI del Codice di procedura penale in materia di rapporti giurisdizionali con autorità straniera (Provisions modifying Book XI of the Criminal Procedure Code concerning judicial relationships with foreign authorities), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2017-10-16&atto.codiceRedazionale=17G00163>.
- Law Decree 354/2003, 2003, Disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia (Urgent provisions for the functioning of water tribunals and interventions on justice administration), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2003-12-29&atto.codiceRedazionale=003G0387>.
- Law Decree 144/2005, 2005, Misure urgenti per il contrasto del terrorismo internazionale (Urgent measures against international terrorism), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2005-07-27&atto.codiceRedazionale=005G0176>.
- Law 45/2004, 2004, Conversione in legge, con modificazioni, del decreto-legge 24 dicembre 2003, n. 354, recante disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia (Conversion into law, with modifications, of Law Decree 354/2003, containing urgent provisions for the functioning of water tribunals and interventions on justice administration), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2004-02-27&atto.codiceRedazionale=004G0068>.
- Law 48/2008, 2008, Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (Ratification and execution of the Council of Europe Convention on cybercrime, adopted in Budapest on 23 November 2001, and national implementation measures), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2008-04-04&atto.codiceRedazionale=008G0070>.

- Law 124/2007, 2007, Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto (Intelligence system for the security of the Republic and new provisions governing secrecy), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2007-08-13&atto.codiceRedazionale=007G0139>.
- Law 167/2017, 2017, Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017 (Provisions for fulfilling the obligations deriving from Italy's membership of the European Union – European law 2017), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2017-11-27&atto.codiceRedazionale=17G00180>.
- Legislative Decree 109/2008, 2008, Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (Decree implementing Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2008-06-18&atto.codiceRedazionale=008G0131>.
- Legislative Decree 271/1989, 1989, Norme di attuazione, di coordinamento e transitorie del codice di procedura penale (Implementing, coordination and transitional provisions of the Criminal Procedure Code), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=1989-08-05&atto.codiceRedazionale=089G0340>.
- Decree of the President of the Republic 335/1982, 1982, Ordinamento del personale della Polizia di Stato che espleta funzioni di polizia (Provisions on the personnel of the State Police exercising police functions), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=1982-06-10&atto.codiceRedazionale=082U0335>.
- Law 203/1991, 1991, Conversione in legge, con modificazioni, del decreto-legge 13 maggio 1991, n. 152, recante provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa (Conversion into law, with modifications, of Law Decree 13 May 1992, no. 152, containing urgent measures on the fight against organised crime and transparency and good administration), <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=1991-07-12&atto.codiceRedazionale=091G0250>.

Poland

- Act of 8 December 2017, *Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa* (Act of 8 December 2017 on the State Protection Service), OJ 2018, item 138, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000138>.
- Act of 9 June 2006, *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (Act of 9 June 2006 on the Central Anti-Corruption Bureau), OJ 2006 No. 104 item 708, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040708>.
- Act of 9 June 2006, *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service), OJ 2006 No. 104 item 709, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040709>.
- Act of 9 November 2017, *Ustawa z dnia 9 listopada 2017 r. o zmianie ustawy o niektórych uprawnieniach pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych oraz funkcjonariuszy i pracowników urzędów nadzorowanych przez tego ministra oraz niektórych innych ustaw* (Act of 9 November 2017 amending the act on certain rights of employees of the office servicing the minister competent for internal affairs as well as officers and employees of offices supervised by that minister and some other acts), OJ 2018 item 106, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000106>.

- Act of 12 October 1990, *Ustawa z dnia 12 października 1990 r. o Straży Granicznej* (Act of 12 October 1990 on the Border Guard), OJ 1990 No.78, item 462, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900780462>.
- Act of 16 July 2004, *Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne* (Act of 16 July 2004 Telecommunications Law), O.J. 2004 no 171 item 1800, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041711800>.
- Act of 16 September 2011, *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 9 lutego 2018 r. w sprawie ogłoszenia jednolitego tekstu ustawy o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej* (Act of 16 September 2011 on the exchange of information with law enforcement authorities of the Member States of the European Union, third countries, European Union agencies and international organisations), OJ 2018, item 484 and 2019, item 125, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000484>.
- Act of 16 November 2016, *Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej* (Act of 16 November 2016 on the National Tax Administration), OJ 2016 item 1947, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20160001947>.
- Act of 24 May 2002, *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency), OJ 2002 No. 74 item 676, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20020740676>.
- Announcement of the Marshal of the Sejm of the Republic of Poland of 22 February 2019, *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 22 lutego 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych* (Announcement of the Marshal of the Sejm of the Republic of Poland of 22 February 2019 regarding the publication of a uniform text of the Act on Military Police and military law enforcement agencies), OJ 2019 item 518, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000518>.
- Act of 6 June 1997, *Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego* (Act of 6 June 1997 - Code of Criminal Proceedings), OJ 1997 No. 89 item 555, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970890555>.
- Police Act of 6 April 1990, *Ustawa z dnia 6 kwietnia 1990 r. o Policji* (Police Act of 6 April 1990), OJ 1990 no 30 item. 179, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900300179>.
- Regulation of the Minister of Justice of 28 April 2004, *Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji - do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych*, (Regulation of the Minister of Justice of 28 April 2004 on the technical preparation of systems and networks used for the transmission of information - to collect lists of telephone connections and other information transfers and methods of securing IT data), OJ 2004 No. 100 item 1023, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041001023>.
- Regulation of the Minister of Infrastructure of 28 December 2009, 2009, *Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania* (Regulation of the Minister of Infrastructure of 28 December 2009 regarding a detailed list of data and types of public telecommunications network operators or providers of publicly available telecommunications services obliged to retain and store data), OJ 2009 No. 226, item 1828, <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20092261828>.

Portugal

- Law 32/2008 of 17 July, <https://dre.pt/web/guest/pesquisa/-/search/456812/details/normal?q=32%2F2008>.
- Law 41/2004 of 18 August, <https://dre.pt/web/guest/pesquisa/-/search/480710/details/normal?q=lei+41%2F2004/>.

- Law 53/2008, of 29 August (Law on Internal Security), <https://dre.pt/web/guest/pesquisa/-/search/453479/details/normal?q=lei+53%2F2008/>.
- Law 109/2009 of 15 September (Cybercrime law), <https://dre.pt/web/guest/legislacao-consolidada/-/lc/128879174/view?q=lei+109%2F2009/>.
- Criminal Procedure Code, http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis&ficha=1&pagina=1&/
- Order 469/2009 of 06 May 2009, http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1265&tabela=leis&so_miolo=/

Slovenia

- Code of Obligations, *Obligacijski zakonik*, Official Gazette of the Republic of Slovenia, Number 97/07 – official consolidated text, 64/16 – odl. US in 20/18 – OROZ631, <http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1263>.
- Constitutional Court Act, *Zakon o Ustavnem sodišču*, Official Gazette of the Republic of Slovenia, Number 64/07 – official consolidated text, 109/12 and 23/20, <http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO325>.
- Consumer Protection Act, *Zakon o varstvu potrošnikov*, Official Gazette of the Republic of Slovenia, Number 98/04 – official consolidated text, 114/06 - ZUE, 126/07, 86/09, 78/11, 38/14, 19/15, 55/17 - ZKotI and 31/18, <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO513>.
- Criminal Procedure Act, *Zakon o kazenskem postopku*, Official Gazette of the Republic of Slovenia, Number 32/12 – official consolidated text, 47/13, 87/14, 8/16 – odl. US, 64/16 – odl. US, 65/16 – odl. US, 66/17 – ORZKP153,154 in 22/19, <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362>.
- Electronic Commerce Market Act, *Zakon o elektronskem poslovanju na trgu*, Official Gazette of the Republic of Slovenia, Number 96/09 – official consolidated text and 19/15, <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4600>.
- Electronic Communications Act, *Zakon o elektronskih komunikacijah*, Official Gazette of the Republic of Slovenia, Number 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 and 40/17, <http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6405>.
- General Act of monitoring and controlling the use of data services from the Agency for Communication Networks and Services (AKOS) of the Republic of Slovenia, *Splošni akt o spremljanju in nadzoru porabe podatkovnih storitev*, Official Gazette of the Republic of Slovenia, Number 9/18, <http://www.pisrs.si/Pis.web/pregledPredpisa?id=DRUG4475>.
- Information Commissioner Act, *Zakon o informacijskem pooblaščenču*, Official Gazette of the Republic of Slovenia, Number 113/05 and 51/07 – ZUstS-A, <http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4498>.
- Penal Code, *Kazenski zakonik*, Official Gazette of the Republic of Slovenia, Number 50/12 – official consolidated text, 6/16 – popr., 54/15, 38/16 in 27/17, <http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050>.
- Police Tasks and Powers Act, *Zakon o nalogah in pooblastilih policije*, Official Gazette of the Republic of Slovenia, Number 15/13, 23/15 – popr., 10/17, 46/19 – odl. US and 47/19, <http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6314>.
- Constitution of the Republic of Slovenia, *Ustava Republike Slovenije*, Official Gazette of the Republic of Slovenia, Number 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a, <http://pisrs.si/Pis.web/pregledPredpisa?id=USTA1>.

Spain

- Law 34/2002, *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico* (Law 34/2002 of information society services and electronic commerce), BOE-A-2002-13758, <https://www.boe.es/eli/es/l/2002/07/11/34/con>.
- Law 25/2007, *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de Comunicaciones* (Law 25/2007 of 18

October on the retention of data of electronic communications and public communications networks), BOE-A-2007-18243, <https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243>.

- Law 31/2010, *Ley 31/2010, de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea* (Law 31/2010 of 27 July 2010, on simplifying the exchange of information and intelligence between the security services of the Member States of the European Union), BOE-A-2010-, <https://www.boe.es/buscar/act.php?id=BOE-A-2010-12134>.
- Law 9/2014, *Ley 9/2014, de 9 de mayo, General de Telecomunicaciones* (Law 9/2014 of 9 May on General Telecommunications), BOE-A-2014-4950 (), <https://www.boe.es/buscar/doc.php?id=BOE-A-2014-4950>.
- Order ITC/110/2009, *Orden ITC/110/2009, de 28 de enero, por la que se determinan los requisitos y las especificaciones técnicas que resultan necesarios para el desarrollo del capítulo II del título V del reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril* (Order ITC/110/2009, of 28 January, determining the requirements and technical specifications necessary for the development of Chapter II of Title V of the Regulations on the conditions for the provision of electronic communications services, universal service and user protection, approved by Royal Decree 424/2005, of 15 April), <https://www.boe.es/buscar/doc.php?id=BOE-A-2009-1771>.
- Order ITC/313/2010, *Orden ITC/313/2010, de 12 de febrero, por la que se adopta la especificación técnica ETSI TS 101 671 'Interceptación legal (LI), Interfaz de traspaso para la interceptación legal del tráfico de telecomunicaciones'* (Order ITC/313/2010 of 12 February implementing and adapting the technical specification ETSI TS 101 671 on lawful interception (LI) and on the handover interface for the LI of telecommunications traffic), <https://www.boe.es/buscar/doc.php?id=BOE-A-2010-2626>.
- Order ITC/682/2010, *Orden ITC/682/2010, de 9 de marzo, por la que se adopta la especificación técnica ETSI TS 133 108 (3GPP TS 33.108) "sistema de telecomunicaciones móviles universales (UMTS); LTE; seguridad 3G; interfaz de traspaso para la interceptación legal (LI)"* (Order ITC/682/2010 of 9 March implementing and adapting the technical specification ETSI TS 133 108 (3GPP TS 33.108) on the Universal Mobile Telecommunications System (UMTS), as well as 3G security and the handover interface for LI), https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-4629.
- Organic Law 4/1981, *Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio* (Organic Law 4/1981 of 1 June on the states of alarm, emergency and siege), BOE-A-1981-12774, <https://www.boe.es/buscar/act.php?id=BOE-A-1981-12774>.
- Organic Law 10/1995, *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal* (Organic Law 10/1995 of 23 November on the Criminal Code), BOE-A-1995-25444, <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>.
- Organic Law 2/2002, *Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia* (Organic Law 2/2002 regulating the ex-ante judicial control of the National Centre for Intelligence (CNI)), <https://www.boe.es/buscar/act.php?id=BOE-A-2002-8627&p=20020507&tn=1#aunico>.
- Organic Law 13/2015, *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica* (Organic Law 13/2015 of 5 October on the amendment of the Law on Criminal Procedure to strengthen the procedural safeguards and regulate the technological investigation measures), BOE-A-2015-10725, <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10725>.
- Organic Law 3/2018, *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (Organic Law 3/2018 of 5 December on the protection of personal data and guaranteeing digital rights), BOE-A-2018-16673, <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>.
- Royal Decree of 14 September 1882, *Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal* (Royal Decree of 14 September 1882 adopting the Law on Criminal Procedure), BOE-A-1882-6036, <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>.

- Royal Legislative Decree 1/1996, *Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia* (Royal Legislative Decree 1/1996 of April 12, 1996, approving the recast text of the Law on Intellectual Property, regularising, clarifying and harmonising the legal provisions in force on the subject), BOE-A-1996-8930, <https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930>.
- Royal Decree 424/2005, *Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios* (Royal Decree 424/2005 of 15 April adopting the Regulation on the conditions for the provision of electronic communications services, universal service and user protection), BOE-A-2005-6970, <https://www.boe.es/buscar/act.php?id=BOE-A-2005-6970>.
- Royal Decree 1720/2007, *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal* (Royal Decree 1720/2007 of 21 December adopting the Regulation developing Organic Law 15/1999 of 13 December on the protection of personal data), BOE-A-2008-979, <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979>.
- Royal Decree 770/2017, *Real Decreto 770/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior* (Royal Decree 770/2017 of 28 July developing the structure of the Ministry of Interior), Official Gazette BOE-A-2017-9013, <https://www.boe.es/buscar/act.php?id=BOE-A-2017-9013>.

Literature

Austria

- Berka, W. and Trappel, J. (2019). *Internet Freedom*. Manz, Vienna.
- Burgstaller, M., Stricker, S. and Zotter, A. (2019). Central data of the legal protection officer 2018. *SIAC-Journal*. Neuer Wissenschaftlicher Verlag, Vienna, pp.4-17.
- Danek, M. and Mann, I. (2017). *Article 229*, Vienna Commentary on the Code of Criminal Procedure. Manz, Vienna.
- Giese, K. (2018). *Security Police Law, Special Administrative Law*, Vol 12, Verlag Österreich, Vienna, pp. 45-90.
- Hinterhofer, H. and Oshidari, B.P. (2017). *System of Austrian Criminal Proceedings*. Manz, Vienna.
- Lendl, F. (2019). *Article 76a*, Vienna Commentary on the Code of Criminal Procedure. Manz, Vienna.
- Reindl-Krauskopf, S., Salimi, F. and Stricker, M. (2018). *IT Criminal Law*. Manz, Vienna.
- Riesz, T. and Schilchegger, M. (2016). *Telecommunications Act*. Verlag Österreich, Vienna.
- Vogl, M. (2014). *Article 18*, Vienna Commentary on the Code of Criminal Procedure. Manz, Vienna.

Estonia

- Illimar Pärnamägi (2020). Varjatud jälgimiseks mõeldud volitusnormide eesmärgi tuvastamine. Väljapääs normipadrikust (*Identifying the aim of provisions delegating authority for covert surveillance. escape from the thicket of laws and regulations*), *Juridica* II/2020, pp. 130–142. Retrieved from: https://www.juridica.ee/article.php?uri=2020_2_varjatud_jalgimiseks_m_eldud_volitusnormide_eesm_rgi_tuvastamine_v_ljap_s_normipadrikust
- Schasmin, P. and Ginter, C. (2017). Lahendite *Tele2 Sverige* ja *Digital Rights Ireland* mõju sideandmete mugavkasutusele Eestis (*Impact of Tele2 Sverige and Digital Rights Ireland on convenient use of communication data in Estonia*), *Juridica* I/2017, pp. 42–52. Retrieved from: https://www.juridica.ee/article.php?uri=2017_1_lahendite_i_tele2_sverige_i_ja_i_digital_rights_ireland_i_m_ju_sideandmete_mugavkasutusele_ee
- Uno Lõhmus (2015). Elektroonilise side andmete säilitamise lõpetamata saaga (*Unfinished saga of retaining electronic data*), *Juridica* X/2015, pp. 735–745. Retrieved from:

https://www.juridica.ee/article.php?uri=2015_10_elektronilise_side_andmete_s_ilitamise_l_petamata_saaga

- Uno Lõhmus (2016). Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte (*The saga on retention of electronic communications data was resolved, but not yet in Estonia*), Juridica X/2016, pp. 698–708. Retrieved from: https://www.juridica.ee/article.php?uri=2016_10_elektronilise_side_andmete_s_ilitamise_saaga_sai_lahenduse_eestis_siiski_veel_mitte.

Germany

- Kühling, J. (2017). Todesstoß für die Vorratsdatenspeicherung: der Beschluss des OVG NRW und seine Folgen (Deathblow for data retention: the decision of the Higher Administrative Court of North-Rhine Westphalia and its consequences). Verfassungsblog.de. Retrieved from: <https://verfassungsblog.de/todesstoss-fuer-die-vorratsdatenspeicherung-der-beschluss-des-ovg-nrw-und-seine-folgen/>.
- Schulze, M. (2019). Ein Weg aus der Zwickmühle für das Bundesverfassungsgericht (A way out of the dilemma for the Federal Constitutional Court). Verfassungsblog.de. Retrieved from: <https://verfassungsblog.de/ein-weg-aus-der-zwickmuehle-fuer-das-bundesverfassungsgericht/>.

Italy

- Baccari, G.M. (2019). 'Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati'. In A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Cybercrime, UTET, 2019, p. 1607.
- Gatto, C.E. (2019). 'Il principio di proporzionalità nell'ordine europeo di indagine penale'. *Diritto penale contemporaneo*, Issue 2.
- Luparia, L. (2019). 'Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio'. *Diritto di internet*, Issue 4. Retrieved from: https://dirittodiinternet.it/wp-content/uploads/2019/12/14_Luparia.pdf.
- Marcolini, S. (2019). 'L'istituto della Data Retention dopo la sentenza della Corte di giustizia del 2014', in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Cybercrime, UTET, 2019.
- Signorato S. (2018). 'Novità in tema di data retention. La riformulazione dell'art. 132 codice privacy da parte del d.lgs. 10 agosto 2018', n. 101. *Diritto Penale Contemporaneo*, Issue 11.

Poland

- Chałubińska-Jentkiewicz, K. and Taczowska-Olszewska, K. (2019), 'Provision of services by electronic means. Commentary, Art. 18 [Data necessary to provide services]'. In C.H.Beck, Warsaw 2019, 1st edition.

Portugal

- Pinho, C. (2018). 'Lei de retenção de dados de comunicações eletrónicas: aposentar ou reformar?', *Revista do Ministério Público*, 154, Abril-Junho, pp. 167-192.
- Silva Ramalho, D. And Duarte Coimbra, J. (2015). 'A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre a conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves', *O Direito*, Ano 147, IV, p. 997-1012.
- Ferreira, P. (2008). 'A retenção de dados pessoais nas comunicações eletrónicas'. *Estudos Comemorativos dos 10 anos da Faculdade de Direito da Universidade Nova de Lisboa*, Volume II, Almedina, pp. 429-443.

Slovenia

- Avbelj, M. and others, 2011, 'Komentar Ustave Republike Slovenije' (Commentary of the Slovenian Constitution), Faculty of government and European studies, Kranj, 2011.
- Križnar, P. (2017). 'Anonimnost uporabnikov predplačniških paketov' (Anonymity of prepaid phone users), Legal practice (Pravna praksa) 6/2017.

- Križnar, P. (2018). '*Je hramba prometnih podatkov uporabnikov predplačniških storitev zakonita?*' (Is the preservation of traffic information for users of prepaid services legal?), Legal practice (Pravna praksa) 28-29/2018.
- Križnar, P. (2018). '*Benedik proti Sloveniji*' (Benedik vs. Slovenia), Legal practice (Pravna praksa) 19/2018.
- Križnar, P. (2017). '*IP-naslov za potrebe kazenskega postopka*' (IP-address for the purpose of the criminal procedure), Legal practice (Pravna praksa) 14/2017.
- Lesjak, A. (2019). '*Komentar k 37. členu Ustave Republike Slovenije*' (Commentary on Article 37 of the Slovenian Constitution), in *Komentar Ustave Republike Slovenije* (Commentary of the Slovenian Constitution), Nova univerza – European faculty of law, 2019.
- Šepec, M. (2015). '*Kazniva dejanja kibernetkega kriminala - značilnosti in posebnosti sodobnega kazenskega prava*' (Cybercrimes – characteristics and features of modern criminal law) (doctoral dissertation), July 2015.
- Tomšič, A. (2016). '*Podatki o komunikacijskih sredstvih z odredbo sodišča*' (Data regarding communication means with a court order), Legal practice (Pravna praksa) 28/2016.
- Žirovnik, J. (2016). '*Podatki o naročnikih komunikacijskih sredstev brez odredbe sodišča*' (Subscriber information without court order), Legal practice (Pravna praksa) 29-30/2016).

Spain

- López-Lapuente, L. (2008). 'La conservación de los datos por los operadores de servicios de comunicaciones electrónicas. Análisis de la Ley 25/2007, de 18 de octubre, sobre conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones' (The preservation of data by the operators of electronic communications. Analysis of the Law 25/2007 of 18 October on retention of data relating to the electronic communications and public communication networks). Uría Menéndez Publications. Retrieved from:
<https://www.uria.com/documentos/publicaciones/1931/documento/articuloUM.pdf?id=3164>.

National case-law

Austria

- Decision of the Data Protection Commission 3 October 2007, K 121.279/0017-DSK/2007 – *Datenschutzkommission* 3.10.2007, K 121.279/0017-DSK/2007.
- Judgment of the Higher Administrative Court of 30 April 2009, 2007/05/0266 – *Verwaltungsgerichtshof* 30.4.2009, 2007/05/0266.
- Judgment of the Constitutional Court of 1 July 2009, G 31/08 – *Verfassungsgerichtshof* 1.7.2009, G 31/08.
- Judgment of the Constitutional Court of 1 July 2009, G 147, 148/08-14 – *Verfassungsgerichtshof* 1.7.2009, G 147, 148/08-14.
- Judgment of the Constitutional Court of 29 June 2012, B 1031/11 – *Verfassungsgerichtshof* 29.6.2012, B 1031/11.
- Judgment of the Constitutional Court of 27 June 2014, G 47/2017-49 and others – *Verfassungsgerichtshof* 27.6.2014, G 47/2017-49 ua.
- Judgment of the Constitutional Court of 29 June 2012, B 1031/11 – *Verfassungsgerichtshof* 29.6.2012, B 1031/11.
- Judgment of the Constitutional Court of 29 November 2017, G 223/2016-23 – *Verfassungsgerichtshof* 29.11.2017, G 223/2016-23.
- Judgment of the Constitutional Court of 11 December 2019, G 72-72/2019-48, G 181-182/2019-18 – *Verfassungsgerichtshof* 11.12.2019, G 72-72/2019-48, G 181-182/2019-18.
- Judgment of the Higher Administrative Court of 24 April 2013, 2011/17/0293 – *Verwaltungsgerichtshof* 24.4.2013, 2011/17/0293.

- Judgment of the Supreme Court of 5 March 2015, 12 Os 93/14i (12 Os 94/14m) – OGH 5.3.2015, 12 Os 93/14i (12 Os 94/14m).

Estonia

- Criminal Chamber of the Supreme Court (*Riigikohtu kriminaalkolleegium*), Court order in case 1-16-6179, 12.11.2018, available at: <https://www.riigiteataja.ee/kohtulahendid/fail.html?id=237436063>.
- Criminal Chamber of the Supreme Court (*Riigikohtu kriminaalkolleegium*), Court decision in case 3-1-1-51-14, 23.02.2015, available at: <https://www.riigiteataja.ee/kohtulahendid/fail.html?id=206132124>.

France

- Judgement of the French Council of State 26 July 2018 in *French Data Network and others*, N. 393099, ECLI:FR:CECHR:2018:393099.20180726, available at: https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETA_TEXT000037253929&fastReqId=1863567356&fastPos=1.

Germany

- Bundesverfassungsgericht – BverfG (*German Federal Constitutional Court*), 26.03.2017 - 1 BvR 3156/15, available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2017/03/rk20170326_1bvr315615.html.
- Bundesverfassungsgericht – BverfG (*German Federal Constitutional Court*), 1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08, available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html.
- Decision of German Federal Administrative Court of the 25 September 2019 in Cases BVerwG 6 C 12.18 and BVerwG 6 C 13.18, available at: <https://www.bverwg.de/pm/2019/66>.
- Decision of the German High Administrative Court of North-Rhine Westphalia of 22 June 2017 in Case 13 B 238/17, available at: https://www.justiz.nrw.de/nrwe/ovgs/ovg_nrw/j2017/13_B_238_17_Beschluss_20170622.html.

Ireland

- Dwyer v Commissioner of An Garda Síochána [2018] IEHC 685; [2019] IEHC 48.
- Dwyer v Commissioner of An Garda Síochána [2020] IESC 4.

Italy

- Judgment of the Court of Cassation (criminal division) in case no. 37212/2014.
- Judgment of the Court of Cassation (criminal division) in case no. 20558/2005.
- Judgment of the Padova Tribunal, order of 15 March 2017.
- Judgment of the Court of Cassation (criminal division) in case no. 33851/2017.
- Judgment of the Court of Cassation (criminal division) in case no. 36380/2019.

Portugal

- Decision of the Constitutional Court of Portugal in case 420/2017, available at: <http://www.tribunalconstitucional.pt/tc/acordaos/20170420.html>.
- Case pending before the Constitutional Court of Portugal.

Slovenia

- Decision of the Constitutional Court of the Republic of Slovenia of 2 October 2008 in case Up-106/05-27, available at: <http://odlocitve.us-rs.si/sl/odlocitev/US28326>.
- Decision of the Constitutional Court of the Republic of Slovenia of 13 February 2014 in case Up-540/11-23, available at: <http://odlocitve.us-rs.si/sl/odlocitev/US30348>.

- Decision of the Constitutional Court of the Republic of Slovenia of 3 July 2014 in case U-I-65/13-19, available at: <http://odlocitve.us-rs.si/si/odlocitev/US30439>.
- Decision of the Constitutional Court of the Republic of Slovenia of 9 October 2019 in cases Up-709/15-29 and Up-710/15-34 from 9 of October 2019, available at: <https://www.us-rs.si/media/up-709-15.up-710-15.pdf>.
- Judgment of the District Court in Celje of 29 October 2019 in case P 772/2017.
- Judgment of the Higher Court in Celje of 22 January 2019 in case II Kp 25975/2017, available at: <http://www.sodnapraksa.si/?q=II%20Kp%2025975/2017%20&database%5bSOVS%5d=SOVS&database%5bIESP%5d=IESP&submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2015081111428258>.
- Judgment of the Supreme Court of the Republic of Slovenia of 23 July 2015 in case XI Ips 9569/2015-396, available at: <http://www.sodnapraksa.si/?q=XI%20Ips%209569/2015-396%20&database%5bSOVS%5d=SOVS&database%5bIESP%5d=IESP&submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2015081111385097>.
- Judgment of the Supreme Court of the Republic of Slovenia of 9 June 2016 in case I Ips 90495/2010-500, available at: <http://www.sodnapraksa.si/?q=I%20Ips%2090495/2010-500&database%5bSOVS%5d=SOVS&database%5bIESP%5d=IESP&submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2015081111399568>.
- Judgment of the Supreme Court of the Republic of Slovenia of 7 February 2018 in case I Ips 23071/2014, available at: <http://www.sodnapraksa.si/?q=I%20Ips%2023071/2014%20&database%5bSOVS%5d=SOVS&database%5bIESP%5d=IESP&submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2015081111418603>.
- Judgment of the Supreme Court of the Republic of Slovenia of 31 January 2010 in case I Ips 35112/2015, available at: <http://www.sodnapraksa.si/?q=I%20Ips%2035112/2015%20&database%5bSOVS%5d=SOVS&database%5bIESP%5d=IESP&submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2015081111427184>.
- Pending case in front of the Constitutional Court of the Republic of Slovenia, case number U-I-144/19.

Spain

- Court Judgment in case 110/2019, available at: <http://www.poderjudicial.es/search/documento/TS/8641291/Prescripcion/20190201>.
- Supreme Court Judgment in case 4084/2014, available at: <http://www.poderjudicial.es/search/AN/openDocument/81a0f8291c0aafa5/20171127>.
- Supreme Court Judgment in case 2800/2017, available at: <http://www.poderjudicial.es/search/AN/openDocument/fdb55a277052cafa/20170818>.
- Supreme Court Judgment in case 3062/2016, available at: <http://www.poderjudicial.es/search/AN/openDocument/2bd52de9df8311dd/20160708>.

Other documents

Austria

- 1074 Beilage 24. Gesetzgebungsperiode – Regierungsvorlage – Vorblatt und Erläuterungen (1074 of the supplements to the 24th legislative period - government bill - cover sheet and explanations), pp.12-16. Retrieved from: https://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf.
- 65 Beilage 26. Gesetzgebungsperiode – Regierungsvorlage – Erläuterungen (65 of the supplements to the 26th legislative period – government bill – explanations), p. 147. Retrieved from: https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00065/fname_686351.pdf.
- 17 Beilage 26. Gesetzgebungsperiode – Regierungsvorlage – Erläuterungen (17 of the supplements to the 26th legislative period – government bill – explanations), pp. 6, 12.

- Retrieved from: https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00017/fname_682032.pdf.
- 128 Beilage 22. Gesetzgebungsperiode – Regierungsvorlage – Materialien (128 of the supplements to the 22nd legislative period – government bill – materials). Retrieved from: https://www.parlament.gv.at/PAKT/VHG/XXII/I/I_00128/fname_004832.pdf.
 - 763 Beilage 25. Gesetzgebungsperiode – Regierungsvorlage – Erläuterungen (763 of the supplements to the 25th legislative period – government bill – explanations), p.1. Retrieved from: https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_00763/fname_432301.pdf.
 - 1075 Beilage 24. Gesetzgebungsperiode – Regierungsvorlage – Vorblatt und Erläuterungen, ad § 53 Abs 3a, 3b, 3c Sicherheitspolizeigesetz und § 76a Strafprozessordnung (1075 of the supplements to the 24th legislative period – government bill – cover sheet and explanations, ad Art. 53 para 3a, 3b, 3c Security Police Act and Art. 76a Code of Criminal Procedure). Retrieved from: https://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01075/fname_206859.pdf.
 - 1293 Beilage 18. Gesetzgebungsperiode – Regierungsvorlage (1293 of the supplements to the 18th legislative period – government bill), p. 27. Retrieved from: https://www.parlament.gv.at/PAKT/VHG/XXIII/I/I_01293/imfname_262581.pdf.
 - 257 Beilage 26. Gesetzgebungsperiode – Regierungsvorlage - Erläuterungen (257 of the supplements to the 26th legislative period – government bill – explanations), p.16. Retrieved from: https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00257/fname_708780.pdf.
 - Bundesministerium Verfassung, Reformen, Deregulierung und Justiz, Sicherheitsberichte. Retrieved from: <https://www.justiz.gv.at/home/justiz/daten-und-fakten/berichte/sicherheitsberichte~2c94848525f84a630132fdbd2cc85c91.de.html>.

Estonia

- Advokaadibüroo Sorainen (Law firm Sorainen) (2017). Julgeolekuasutuste tegevuse regulatsiooni võrdlev analüüs (*Comparative analysis of the regulation on activities of security authorities*), published by the Ministry of the Interior. Retrieved from: https://www.siseministeerium.ee/sites/default/files/dokumentid/Uuringud/Sisejulgeolek/2017_julgeolekuasutuste_regulatsiooni_vordlev_analuus.2017-01-17.est.loplik.pdf.
- Andmekaitse Inspektsioon (*Data Protection Inspectorate*) (2015). Metaandmed ja privaatsus: juhised organisatsioonidele ja kodukasutajale seaduse rakendamisel (*Metadata and privacy: guide for organisations and home users for implementing the law*), 28 October 2015, p. 4. Retrieved from: <https://www.aki.ee/sites/default/files/dokumentid/metaandmed.pdf>.
- Erikomisjon sai ülevaate prokuratuuri järelevalvest jällitus- ja julgeolekuasutuste üle (*Select Committee was provided an overview of the Prosecutor Office's supervision over surveillance and security authorities*) (2017). Parliament's press release, 6 February 2017. Retrieved from: <https://m.riigikogu.ee/pressiteated/julgeolekuasutuste-jarelvalve-erikomisjon-et-et/erikomisjon-sai-ulevaate-prokuratuuri-jarelevalvest-jalitus-ja-julgeolekuasutuste-ule/>.
- Erikomisjon sai ülevaate prokuratuuri järelevalvest jällitus- ja julgeolekuasutuste üle (*Select Committee was provided an overview of the Prosecutor Office's supervision over surveillance and security authorities*) (2018). Parliament's press release, 5 February 2018. Retrieved from: <https://m.riigikogu.ee/pressiteated/julgeolekuasutuste-jarelvalve-erikomisjon-et-et/erikomisjon-sai-ulevaate-prokuratuuri-jarelevalvest-jalitus-ja-julgeolekuasutuste-ule-2/>.
- Government of the Republic of Estonia (2017). *National Security Concept 2017*. Retrieved from: https://www.riigikantselei.ee/sites/default/files/content-editors/Failid/national_security_concept_2017.pdf.
- Julgeolekuasutuste erikomisjon kontrollis KAPO jällitustegevust (*Security Authorities Surveillance Committee examined the surveillance activities of Estonian Internal Security Service*) (2016). Parliament's press release, 18 April 2016. Retrieved from: <https://www.riigikogu.ee/pressiteated/julgeolekuasutuste-jarelvalve-erikomisjon-et-et/julgeolekuasutuste-erikomisjon-kontrollis-ka-po-jalitustegevust/>.
- Justiitsministeerium (Ministry of Justice) (2012). Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri, (*Explanatory memorandum of the draft legislation for changing the Code of Criminal Procedure and related acts*). Retrieved from: <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/86dde8ff-c50e->

[48ba-a39e-a325fe15a3f0/Kriminaalmenetluse%20seadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20\(175%20SE%20II\).](#)

- Justiitsministeerium (Ministry of Justice) (2018). Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine), (*Legislative intent for the draft act for amending the Electronic Communications Act and related acts (retention and use of communications data)*), 31 October 2018. Retrieved from: <https://humanrights.ee/app/uploads/2018/12/VTK-sideandmed-31.10.18.pdf>.
- Käsper, K. (2017). On data retention and Estonia. Retrieved from: <https://humanrights.ee/en/2017/12/data-retention-estonia/>.
- Õiguskantsler (*Chancellor of Justice*) (2015). Õiguskantsleri seisukoht elektroonilise side seaduse § 111¹ alusel sideandmete töötlemise põhiseaduspärasuse kohta (*Opinion of the Chancellor of Justice on the constitutionality of processing communications data according to § 111¹ ECA*), 15 July 2015. Retrieved from: http://oiguskantsler.ee/sites/default/files/field_document2/õiguskantsleri_seisukoht_vastu_olu_mittetuvastamise_kohta_elektronilise_side_andmete_kogumine_sideettevotete_poolt.pdf.
- Õiguskantsler (*Chancellor of Justice*) (2016). Õiguskantsleri seisukoht elektroonilise side seaduse § 111¹ alusel sideandmete töötlemise põhiseaduspärasuse kohta (*Opinion of the Chancellor of Justice on the constitutionality of processing communications data according to § 111¹ ECA*), 22 April 2016. Retrieved from: https://www.oiguskantsler.ee/sites/default/files/field_document2/elektronilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseaduspärasus.pdf.
- Õiguskantsler (*Chancellor of Justice*) (2019). Õiguskantsleri seisukoht elektroonilise side seaduse § 111¹ lõigetes 2 ja 3 nimetatud andmete töötlemise kohta (*Opinion of the Chancellor of Justice on the processing of communications data listed in § 111¹ Subsections 2 and 3 ECA*), 4 September 2019. Retrieved from: https://www.oiguskantsler.ee/sites/default/files/field_document2/Elektronilise%20side%20seaduse%20%C2%A7%20111%20%C3%B5igetes%20%20ja%20%20nimetatud%20andmete%20%C3%B6%20%C3%B6tlemine.pdf.
- Schasmin, P. (2016). Privaatsusõiguse piiramise õiguslik raamistik Euroopa Inimõiguste Kohtu ning Euroopa Kohtu lahendite alusel (*The legal framework for the interference with privacy according the European Court of Human Rights and European Court of Justice*), Master's thesis. Retrieved from: http://dspace.ut.ee/bitstream/handle/10062/53040/schasmin_ma_2016.pdf.

France

- Ministère de la Justice (2017). La plateforme nationale des interceptions judiciaires en chiffres, Communiqué de presse. Retrieved from: <http://www.presse.justice.gouv.fr/communiques-de-presse-10095/archives-des-communiques-de-2017-12858/la-plateforme-nationale-des-interceptions-judiciaires-en-chiffres-30997.html>.

Germany

- Bundesamt für Justiz (Federal Office for Justice) (2018). Telekommunikationsüberwachung. Retrieved from: <https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html>.
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und Bundesnetzagentur (BNetzA) (2012). Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten. Retrieved from: <https://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenZumSpeichernVonVerkehrsdaten.html>.
- Bundesnetzagentur, Automatisiertes Auskunftsverfahren (§ 112 TKG). Retrieved from: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/AutomatisiertesAuskunftsverfahren/AutomatisiertesAuskunftsverfahren-node.html.

- Deutsch Telekom (n.d.). *Verdict: The European Court of Justice overturns data storage directive*. Retrieved from: <https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/archiv-datenschutznews/news/verdict-the-european-court-of-justice-overturns-data-storage-directive-360432>.
- Telefonica (n.d.). *Häufige Fragen*. Retrieved from: <https://www.telefonica.de/unternehmen/datenschutz/haeufige-fragen.html>.
- Vodafone (n.d.). *Datennutzung vor Vertragsschluss*. Retrieved from: <https://www.vodafone.de/unternehmen/verantwortung/datenschutz-fuer-telefon-internet.html>.

Ireland

- Communications (Retention of Data) Bill. Retrieved from: [http://www.justice.ie/en/JELR/General Scheme - Communications \(Retention of Data\) Bill.pdf/Files/General Scheme - Communications \(Retention of Data\) Bill.pdf](http://www.justice.ie/en/JELR/General Scheme - Communications (Retention of Data) Bill.pdf/Files/General Scheme - Communications (Retention of Data) Bill.pdf).
- Mr Justice Murray (2017). *Law on the Retention of and Access to Communications Data Report*, April 2017. Retrieved from: <http://www.justice.ie/en/JELR/Review of the Law on Retention of and Access to Communications Data.pdf/Files/Review of the Law on Retention of and Access to Communications Data.pdf>.
- O'Keeffe, C. (2018). Personal data shared 92,000 times to State agencies by phone and internet firms. *The Irish Examiner*. Retrieved from: <https://www.irishexaminer.com/breakingnews/ireland/personal-data-shared-92000-times-to-state-agencies-by-phone-and-internet-firms-891004.html>.

Italy

- Italian Data Protection Authority (2018). Parere sullo schema di decreto legislativo recante Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio - 22 febbraio 2018 (Opinion No. 99 of 22.02.2018 on the proposed legislative decree 2016/680). Retrieved from: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8005333>.
- Italian Data Protection Authority (2018). Parere sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 - 22 maggio 2018 (Opinion No. 312 of 22.05.2018 on the proposed legislative decree implementing Regulation (EU) 2016/679). Retrieved from: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9163359>.
- Italian Data Protection Authority (2008). Sicurezza dei dati di traffico telefonico e telematico (Act on telephone and telematic data security of 17 January 2008). Retrieved from: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1482111/>.
- Italian Data Protection Authority (2007). Measures, 19.09.2007. Retrieved from: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1442463>.
- Italian Data Protection Authority (2007). Misure e accorgimenti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati - 19 settembre 2007 (Measures for the protection of the interested parties with regard to the retention of phone and electronic traffic data for law enforcement purposes of 19 september 2007). Retrieved from: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1442463/>.
- Italian Opinion No. 99 of 22.02.2018 and no. 312 of 22.05.2018, the Italian Data Protection Authority.
- Opinion No. 312 of 22.05.2018, the Italian Data Protection Authority.

Poland

- National Security Bureau (2020). Website. Retrieved from: <https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn->

propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html.

Portugal

- National Data Protection Commission (2017). Opinion No. 24/2017.
- National Data Protection Commission (2017). Opinion 641/2017. Retrieved from: https://www.cnpd.pt/bin/revistaforum/forum2017_1/files/assets/common/downloads/forum_de_protecao_de_dados_4.pdf.
- National Data Protection Commission (2017). Opinion 1008/2017. Retrieved from: https://www.cnpd.pt/bin/decisoos/Delib/20_1008_2017.pdf.
- National Data Protection Commission (2015). Opinion No. 51/2015.
- Ombudsman (2019). Request of the Ombudsman to the Constitutional Court to review the constitutionality of L. 32/2008, 26 August 2019. Retrieved from: https://www.provedor-jus.pt/site/public/archive/doc/2019_08_26_Q_7746_2017_Tribunal_Constitucional.pdf.

Slovenia

- A1 Slovenija (n.d.). General Terms of use for A1 Slovenija d.d. Retrieved from: https://www.a1.si/documents/10179/2451178/20180420_A1_Splosni_pogoji_za_izvajanje_elektronskih_komunikacijskih_storitev_za_potrosnike_clean.pdf/82dc1e78-8c95-4c47-9705-49f6677a686c.
- A1 Slovenija (n.d.). Privacy Policy for A1 Slovenija d.d. Retrieved from: https://www.a1.si/documents/10179/3145147/A1_Politika_varstva_osebnih_podatkov_AP_R18.pdf/d6957269-f4b9-464f-a405-98fddee3e128.
- Ministrstvo za Notranje Zadeve, Policija, Služba generalnega direktorja policije (2019). Letno poročilo o delu policije. Retrieved from: https://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2019_popr.pdf.
- Motion for review of constitutionality and legality of Articles 149.b and 149.c of the CPA. Retrieved from: <https://telemach.si/Binary/12693/Pogoji-varovanja-osebnih-podatkov-3-2020.pdf>.
- Slovene Information Commissioner (2017). Opinions of 24 January 2017 on case 0712-1/2017/130. Retrieved from: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-podlocbah-in-mnenjih/odlocbe-in-mnenja-vop/?tx_jzvopdecisions_pi1%5BshowUid%5D=2859&tx_jzvopdecisions_pi1%5BhighlightWord%5D=0712-1%2F2017%2F130.
- Slovene Information Commissioner (2014). Opinions of 17 April 2014 on case 0712-1/2014/1651. Retrieved from: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-podlocbah-in-mnenjih/odlocbe-in-mnenja-vop/?tx_jzvopdecisions_pi1%5BshowUid%5D=2342&tx_jzvopdecisions_pi1%5BhighlightWord%5D=0712-1%2F2014%2F1651.
- Slovene Information Commissioner (2013). Opinions of 4 June 2013 on case 0712-1/2012/2854. Retrieved from: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-podlocbah-in-mnenjih/odlocbe-in-mnenja-vop/?tx_jzvopdecisions_pi1%5BshowUid%5D=2302&tx_jzvopdecisions_pi1%5BhighlightWord%5D=0712-1%2F2012%2F2854.
- Telekom Slovenija (n.d.). General Terms of use for Telekom Slovenija d.d. Retrieved from: https://www.telekom.si/podporaobrazci/splosni_pogoji_uporabe_elektronskih_komunikacijskih_storitev_druzbe_telekom_slovenije_d_d.pdf.
- Telemach (n.d.). General Terms of use for Telemach d.o.o. Retrieved from: <https://telemach.si/Binary/12692/24-TMH-Splosni-pogoji-poslovanja-A5-3-2020-NET.pdf>.
- Telemach (n.d.). Terms of protecting personal data for Telemach d.o.o. Retrieved from: <https://telemach.si/Binary/12693/Pogoji-varovanja-osebnih-podatkov-3-2020.pdf>.
- T-2 (n.d.). General Terms of use for T-2 d.o.o. Retrieved from: https://www.t-2.net/sites/www.t2.si/files/files/uploads/article/splosni_pogoji_poslovanja_0.pdf.

- T-2 (n.d.). Terms of processing personal data for T-2 d.o.o. Retrieved from: https://www.t-2.net/sites/www.t2.si/files/files/uploads/article/20190226_splosni_pogoji_obdelave_osebni_h_podatkov_v_druzbi_t-2_d_o_o_kv_0.pdf.
- https://www.sds.si/sites/default/files/Zahteva%20za%20oceno%20ustavnosti_hisnepreiskave_080519.pdf.

Spain

- Ministry of Foreign Affairs (n.d.). *Guía de Tratados Bilaterales con Estados* (Guide of Bilateral Agreements). Retrieved from: <http://www.exteriores.gob.es/Portal/es/SalaDePrensa/Multimedia/Publicaciones/Documentos/GUIA%20TRATADOS%20CON%20PAISES.PDF>.

ANNEX I: ANALYSIS FRAMEWORK

Table 10: Analysis framework for the Study

Question	Data Collection Tools	Stakeholders	Indicators
Legal Framework			
What is the national legal framework regarding the retention of non-content data for law enforcement purposes? Is there any specific legal obligation to retain data for law enforcement purposes? What are these obligations (who must retain what, for how long, timeframe for providing requested data, for what type(s) of crime)?	Desk research Legal analysis	Desk research and legal analysis will be performed by the core team and the national experts respectively. In case of doubts or grey areas, we will discuss and validate the issues with Member States.	Existence of obligations to retain the non-content data for law enforcement purposes If yes, type of data to be retained, operator on whom the obligation is placed and time period of retention
What is the national legal framework regarding access to non-content data by law enforcement authorities (who can request and ex-ante authorise access, for what purposes, for what type(s) of crime, is there any ex-post control, what data can be accessed, etc.)?	Desk research Legal analysis	Desk research and legal analysis will be performed by the core team and the national experts respectively. In case of doubts or grey areas, we will discuss and validate the issues with Member States.	Existence of legal provisions on access to non-content data by the law enforcement authorities If yes, existence of ex-ante authorisation and ex-post controls
Are there legal provisions granting LEAs access to non-content data retained by ESPs for business purposes? Are such legal provisions independent from the national law(s) on data retention or not? Is such access granted by provisions other than laws (e.g. police procedural rules)?	Desk research Legal analysis	Desk research and legal analysis will be performed by the core team and the national experts respectively. In case of doubts or grey areas, we will discuss and validate the issues with Member States.	Existence of provisions granting LEAs access to non-content data retained by electronic communication service providers for business purposes If yes, what type provisions (e.g. legal provisions or procedural rules)
Does the legal framework regarding the retention of non-content data for law enforcement purposes include Single Points of Contacts (SPOCs)? If yes, who are they (e.g. what type of authority, organisational structure)? If yes, what is their role?	Desk research Legal analysis	Desk research and legal analysis will be performed by the core team and the national experts respectively. In case of doubts or grey areas, we will discuss and validate the issues with Member States.	Existence in the national legal framework of Single Points of Contacts (SPOCs) If yes, organisational structure and role in the framework content data for law enforcement purposes

Question	Data Collection Tools	Stakeholders	Indicators
Are there any legal challenges arising from the relevant national legal framework, for instance from criminal and criminal procedural law, data protection law, electronic communication services regulations, competition law, consumer protection law etc? What is their extent? Are there any ongoing processes aiming at amending the legislation?	Targeted interviews	Representatives from law enforcement authorities Representatives from the telecommunication regulatory authorities	Existence of relevant case-law Existence of planned amendments to legal framework Existence of legal challenges pertaining to the admissibility of evidence in judicial proceedings that rely on non-content data evidence.
What is the legal framework regarding the retention of non-content data for law enforcement purposes in cross-border cases? What is the legal framework regarding the retention of non-content for law enforcement purposes with third countries?	Desk research Legal analysis	Desk research and legal analysis will be performed by the core team and the national experts respectively. In case of doubts or grey areas, we will discuss and validate the issues with Member States.	Existence of legal provisions on access to non-content data by the law enforcement authorities in cross-border cases Existence of legal provisions on access to non-content data in third countries by the law enforcement authorities
National Practices			
What non-content data are retained and for how long by electronic communication service providers? Are they retained for commercial/business purposes and/or for law enforcement purposes? What data is retained solely due to the obligation of retention for law enforcement purposes and would therefore not be retained for commercial/business purposes?	Surveys Targeted interviews	Representatives from electronic communication service providers (differentiated by size and number of providers in the national market) Representatives from the telecommunication regulatory authorities	Extent and type of non-content data retained by electronic communication service providers For commercial/business purposes For law enforcement purposes
What are the requirements/practices to ensure the security of retained non-content data (e.g. localisation of data, separation of databases, encryption or pseudonymisation etc.)?	Desk research Surveys Targeted interviews	Representatives from electronic communication service providers (differentiated by size and number of providers in the national market) Representatives from Law Enforcement Authorities	Extent and type of requirements for security of non-content data retained by electronic communication service providers, if differentiated between commercial/business purposes and law enforcement purposes

Question	Data Collection Tools	Stakeholders	Indicators
What is the role of Single Points of Contact (SPOCs) in the relationship between LEAs and electronic communication service providers? (if applicable)?	Desk research Surveys Targeted interviews	Representatives from electronic communication service providers (differentiated by size and number of providers in the national market) Representatives from Law Enforcement Authorities	Presence of SPOCs in the national framework for LEAs and/or ESPs; Role of SPOCs in the national framework for LEAs and/or ESPs (e.g. mandatory or voluntary, used frequently or not)
What are the additional costs associated with retention of data for law enforcement purposes? Are these costs reimbursed to the industry?	Surveys Targeted interviews	Representatives from electronic communication service providers (differentiated by size and number of providers in the national market)	Additional costs for retention of data for law enforcement purposes If relevant, proportion reimbursed to the industry
What is the impact of the retention and access to data for law enforcement purposes on the business models of electronic communication service providers? What are the impacts of business models for electronic communication service providers?	Surveys Targeted interviews	Representatives from electronic communication service providers	Change in business model of the industry linked to data retention and access requirements (e.g. leaving or opening specific market segments, cost of required specific infrastructure adaptation, impact on cross-border provision of services)
What is the number of requests for a given time period according to the category of data requested e.g. subscriber fixed and mobile telephony data (who registered a phone number), traffic data (who called whom and at what time), location data, other non-content data (such as computer non-content data, IP addresses, IP logs etc.)?	Desk Research Surveys	Representatives from law enforcement authorities Representatives from electronic communication service providers	Number of requests for 01/01/2018 to 31/08/2019 per category of data requested
What is the number of requests for a given time period according to the category of data requested e.g. subscriber fixed and mobile telephony data (who registered a phone number), traffic data (who called whom and at what time), location data, other non-content data (such as computer non-content data, IP addresses, IP logs etc.)?	Desk Research Surveys	Representatives from law enforcement authorities Representatives from electronic communication service providers	Number of requests for 01/01/2018 to 31/08/2019 per category of data requested in cross-border cases Procedures in place, issues and challenges related to requesting data and answering to requests in cross-border cases

Question	Data Collection Tools	Stakeholders	Indicators
in cross-border cases? What procedures are in place for accessing such data?			
What is the number of requests for a given time period according to the category of data requested when electronic communication service providers are based in third countries e.g. subscriber fixed and mobile telephony data (who registered a phone number), traffic data (who called whom and at what time), location data, other non-content data (such as computer non-content data, IP addresses, IP logs etc)? What procedures are in place for accessing such data?	Desk Research Surveys	Representatives from law enforcement authorities Representatives from electronic communication service providers	Number of requests for 01/01/2018 to 31/08/2019 per category of data requested when electronic communication service providers are based in third countries Procedures in place, issues and challenges related to requesting data and answering to requests when electronic communication service providers are based in third countries
<i>Benefit of using the data</i>			
Proportion of investigations and/or prosecutions in which non-content data were used as determinative and/or exclusionary evidence over the total number of investigations and/or prosecutions for which non-content data were requested from ESPs Proportion of investigations and/or prosecutions that were discontinued or dropped due to the problems in accessing non-content data over the total number of investigations and/or prosecutions for which non-content data were requested from ESPs Proportion of prosecutions in which evidence based on non-content data were declared inadmissible over the total number of prosecutions cases that have used non-content data	Desk Research Surveys Targeted interviews	Representatives from law enforcement authorities	Share of investigations and prosecutions where non-content data have been used compared to all investigations and prosecutions

Question	Data Collection Tools	Stakeholders	Indicators
Technological context			
What is the impact of the increase in the use of machine-to-machine communication, Web-based communication (e.g. VoIP, social media messaging services), dynamic IP addresses, use of CGN-NAT?	Desk Research Surveys Targeted interviews	Representatives from law enforcement authorities Representatives from ESPs Representatives from the telecommunication regulatory authorities	Practical/technical implications of recent technological developments (e.g. volume of data to be stored and exchanged); Cost implications of recent technological developments
What is the impact of cross-border electronic communication service provision on data retention for law enforcement purposes?	Desk Research Surveys Targeted interviews	Representatives from law enforcement authorities Representatives from ESPs Representatives from the telecommunication regulatory authorities	Practical/technical implications of cross-border provision of electronic communication services (e.g. applicability of data retention obligations to cross-border ISPs and cloud service providers or existence of geographical restrictions for storage of data subject to retention provisions) Cost implications of recent technological developments
What is the impact of end-to-end encryption on access to non-content data for law enforcement purposes?	Desk Research Surveys Targeted interviews	Representatives from law enforcement authorities Representatives from ESPs Representatives from the telecommunication regulatory authorities	Practical/technical implications of end-to-end encryption; Cost implications of end-to-end encryption
What is the expected impact of future standards or technologies (e.g. 5G, Internet of Things) on the retention and access to non-content data for law enforcement purposes?	Desk Research Surveys Targeted interviews	Representatives from law enforcement authorities Representatives from ESPs Representatives from the telecommunication regulatory authorities	Existence and type of future standards/ technologies Practical/technical implications of future standards/technologies Cost implications of future standards/ technologies

Source: Milieu elaboration

ANNEX II: KEY CONCEPTS AND DEFINITIONS

This Study uses some specific terms:

- Electronic communications non-content data;
- Electronic communications services (ESCs);
- Electronic communications service provider(s) (ESPs);
- Law enforcement authority(-ies) (LEAs);
- Law enforcement purposes;
- National security purposes;
- Over-the-Top communications services (OTT services);
- Over-the-Top services providers (OTTs);
- Serious crime.

Each of these concepts is defined and explained in the paragraphs below.

Electronic communications non-content data

Taking into account Member States' particularities, as well as technological progress, the concept of **electronic communications non-content data** (also known as **metadata**) is defined broadly and includes all types of non-content data that currently exist in practice and are not part of the content of electronic communications. This concept goes beyond the definitions provided in EU secondary law documents, such as the e-Privacy Directive, the proposed e-Privacy Regulation and the now-invalidated Data Retention Directive (DRD).

Non-content data include information on the **identity of the sender** of a communication (i.e. subscriber data or service-associated information), **traffic** (i.e. traffic data or communication-associated information), **location** of the communication equipment (i.e. location data) and **data on the destination of a communication** that include any information enabling the identification of the receiver(s) and attempted receiver(s) of a communication. To enable more clarity and precision in survey questions and when communicating with stakeholders, data on the destination of a communication were differentiated from other types of traffic data. However, as a sub-category of traffic data, they are included under traffic data in the main body of the Study.

The Study also uses the term **identification data**, which are data that could be classified either as subscriber data or traffic data, based on national laws and practices (e.g. device identification numbers, IP addresses, SIM numbers, ports for dynamic IP addresses).

The classification of non-content data used throughout this Study is presented in the table below. Identification data are marked in **bold**.

Table 11: Types of electronic communications non-content data

Subscriber data	Traffic data	Location data	Data on the destination of a communication ¹³⁰
Name	Duration of the communication	Location of the equipment or line at the start of the communication (e.g. cell towers, Wi-Fi hotspots)	Destination of the communication: identifiers of the account, device or relevant service to which the communication has been sent
Physical address associated	Date and time of the communication (including time zone)	Location of the equipment or line at the end of the communication (e.g. cell towers, Wi-Fi hotspots)	Destination of the communication: identifiers of the account, device or relevant service to which the communication has been forwarded, routed or transferred
Username	Data volume of the electronic communication		Destination of the communication: identifiers of the account, device or relevant service to which the communication has been attempted to be forwarded, routed or transferred
Email address	Missed calls (including number of rings of missed calls)		
Telephone number	Start of the communication		
SIM number	End of the communication		
Device identification numbers (e.g. IMEI number, MAC number)	Connection to the relevant service		
IP address	Disconnection from relevant service		
Port number for dynamic IP addresses	Type of communication (e.g. voice, SMS, email, chat, forum, social media)		
Billing and payment information (e.g. client number)	Type of the relevant service (e.g. asymmetric digital subscriber line (ADSL), Wi-Fi, VoIP, cable, 3G or 4G network)		

Source: Milieu elaboration, from desk research and stakeholders' input

¹³⁰ Note: the data on the destination of a communication are a sub-category of traffic data and are thus included as traffic data in the main body of the Study.

Electronic communications services (ECSs) and electronic communications service provider(s) (ESPs)

For the purposes of the Study, electronic communications services (ECSs) **services**, normally provided for remuneration, that are **provided by means of electronic signals over telecommunications or broadcasting networks**, for example. This notion follows the definition provided in the current EU legal framework for electronic communications networks and services¹³¹. It excludes services controlling editorial content and information society services that do not involve the transmission of signals.

Electronic communications service providers are providers of ECSs.

Law enforcement purposes and law enforcement authorities (LEAs)

The concept of the 'law enforcement purposes' in this Study shall be interpreted as broadly as possible, covering purposes of **prevention, investigation, detection and prosecution of criminal offences** or the execution of criminal penalties and/or similar purposes.

Law enforcement authorities (LEAs) are national criminal authorities that are active in the fields of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties. 'Law enforcement' is used to encompass both police and judicial authorities. The different stages in a criminal investigation, ranging from investigation to prosecution and from police to judicial bodies, have concepts as defined in relevant national laws.

National security

This Study does not deal with strictly **national security issues**. Pursuant to Article 4(2) of the Treaty on European Union, national security remains the sole responsibility of each Member State. The application of EU law in this context is, however, a complex issue that is currently pending before the CJEU. National security may be further juxtaposed with the notion of public security, as the former explicitly falls outside the competence of the EU¹³², while the latter may be regulated within the EU legal order. Although the distinctive boundaries between the two concepts are not always clear, it may be understood that national security when invoked as a derogation to EU law should be construed narrowly. More specifically, in interpreting the national security derogation included in the e-Privacy Directive and in the Data Protection Directive that preceded the GDPR, AG Manuel Campos Sanchez-Bordona suggested that only activities seeking to safeguard national security, performed by government authorities, with their own resources, may be considered to fall outside the scope of EU law¹³³. In such cases, the EU rules and safeguards are not applicable to the authorities in question. On the contrary, when Member States provide by law an obligation for private actors, for instance ESPs, to retain personal data and allow access to the retained data by law enforcement and national security agencies, those activities fall within the scope of EU rules. While it is not clear if the AG Opinion will be followed by the CJEU in its forthcoming ruling, a cautious approach is appropriate in the meantime.

In the absence of a clear definition of '**national security**' in EU legislation and case-law, this concept should be interpreted as including national government secret services' or intelligence agencies' efforts to protect state sovereignty, security and constitutional democracy from certain criminal offences such as espionage, terrorism, support for terrorism, separatism, etc.

¹³¹ In particular, the European Framework Directive (Directive 2002/21/EC).

¹³² Consolidated version of the Treaty on European Union, 2016, OJ C 202, (Treaty on European Union), Article 4(2).

¹³³ Advocate General's Opinions in Case C-623/17 *Privacy International*, Joined Cases C-511/18 *La Quadrature du Net and Others* and C-512/18 *French Data Network and Others*, and Case C-520/18 *Ordre des barreaux francophones et germanophone and Others*, available at: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-01/cp200004en.pdf>.

As government secret services or intelligence agencies also request and obtain non-content data from ESPs, information about those requests have also been gathered. To avoid collecting non-comparable answers, this issue was carefully considered in the mapping of stakeholders. Access requests to obtain non-content data made by national government secret services or intelligence agencies exclusively for national security purposes with their own resources have been excluded from further collection of data. Requests made by such agencies for law enforcement purposes (i.e. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and/or similar purposes, such as prevention of terrorist acts) have been included.

Over-the-Top communications services (OTT services) and Over-the-Top service providers (OTTs)

Although the definition of OTT services includes anything provided over the public internet, the scope of this Study is confined to those **OTTs** that provide messaging and voice calling solutions, excluding OTTs providing e-commerce, video and music streaming, cloud computing and storage, financial services, etc.

In its 2016 report on OTT services¹³⁴, the Body of European Regulators for Electronic Communications (BEREC) defined an OTT service as ‘a content, a service or an application that is provided to the end user over the public Internet’¹³⁵. In essence, this means that anything provided over the public internet is an OTT service, as content, a service or an application. The provision of services generally occurs without the involvement of internet access providers. The BEREC taxonomy for OTT services under the current framework distinguishes between three types of OTT services:

- OTT services that could be qualified as electronic communications services (ECSs) (i.e. OTTs providing services allowing users to make calls to Publicly Available Telephone Services – PATS);
- OTT services that are not ECSs but could potentially compete with ECSs (e.g. OTT voice, instant messaging);
- Other OTT services (e.g. e-commerce, video and music streaming cloud computing and storage, financial services)¹³⁶.

In line with the BEREC definition and in view of the future legal developments described in section 4.2, the definition of **OTT services** used for the purposes of this Study includes only the first two types of OTT services (so-called communication services). The OTT services taken into consideration are shown in the table below.

Table 12: Mapping of OTT services in scope

OTT services		
Instant messaging services (Facebook Messenger, WhatsApp, Google Talk, iMessage etc.)	Email web-based services (Gmail, Outlook etc.)	Voice services (Skype, Teams, FaceTime, WhatsApp, Google Talk etc.)

Source: Milieu elaboration, from desk research and stakeholders’ input

Serious crime

There is no autonomous concept of ‘**serious crime**’ at EU level. EU policy and legislative documents sometimes provide a list of crimes that amount to ‘serious crime’ for the purposes of that particular instrument. However, there are no common defining

¹³⁴ BEREC (2016). Report on OTT services, BoR (16) 35, https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5751-berec-report-on-ott-services_0.pdf.

¹³⁵ *Ibid.*, p. 16.

¹³⁶ *Ibid.*, pp. 15-17.

criteria¹³⁷. Where serious crime is defined, that definition may differ from one EU instrument to another.

In general, the approach taken by the EU legislator is to delimit serious crime by the nature, severity and punishment of the crime. For instance, felonies punishable by a custodial sentence or a detention order for a maximum period of at least a few years are likely to fall under the definition of serious crime¹³⁸.

The notion of serious crime is further defined by each Member State's national law. Serious crime for the purposes of this Study could include any of the types of crime in the (non-exhaustive) table below.

Table 13: Typology of relevant serious crimes

Types of serious crime		
Organised crime	Human trafficking	Child sexual exploitation and child pornography
Drug trafficking	Trafficking of weapons	Corruption
Fraud	Money laundering	Cybercrime
Murder, grievous bodily injury	Kidnapping	Organised and armed robbery
Trafficking of cultural goods	Counterfeiting and product piracy	Rape
Trafficking in stolen vehicles	Theft	Other

Source: Milieu elaboration, from desk research and stakeholders' input

¹³⁷ Paoli et al. (2017). Exploring definitions of serious crime in EU policy documents and academic publications: A content analysis and policy implications. *European Journal of Criminal Policy Research*, 23, 269–285.

¹³⁸ See, for example, the definition of serious crime under Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

ANNEX III: DETAILED ANALYSIS OF INFORMATION

Regulatory and institutional framework on retention of non-content data

This section of Annex III presents the detailed analysis materials referred to in section 4 of the report.

Table 14: Authorities authorised to access non-content data for law enforcement purposes based the national legislative frameworks

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
Overview	10 / 10	3 / 10	9 / 10	7 / 10	7 / 10	4 / 10	4 / 10	3 / 10	3 / 10	4 / 10	2 / 10
AT	✓ Any officer working on the case.	x	✓ Public prosecutor working on the case.	✓ Investigating judge working on the case.	✓	✓ Any officer working on the case.	x	x	x	✓	x
DE	✓ Certain officers (e.g. detectives) that have access to specific software.	x	✓ Public prosecutor instructs the investigative personnel (e.g. police officers).	✓ Judge working on the case.	✓ Customs investigation	x	✓	x	x	x	x
EE¹³⁹	✓ List of individuals	✓ The comman-	✓	✓ Judge working on	✓ List of individuals	✓ List of individuals	✓ List of individuals	✓ List of individuals	✓ List of individuals	✓	✓ List of individuals

¹³⁹ Pursuant to the Code of Criminal Procedure, there is a differentiation between the bodies that can request subscriber data (for which no ex-ante authorisation is necessary) and other data retained by ESPs (location and traffic data). Based on the main provision on non-content data requests, investigative bodies (within their competence, the Police and Border Guard Board, the Estonian Internal Security Service, the Tax and Customs Board, the Competition Authority, the Military Police, the Environmental Inspectorate and the

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
	/ positions approved internally. Access requests mostly submitted through a single responsible department.	der or an authorised official.		the case.	/ positions approved internally ¹⁴⁰ .	/ positions approved internally.	/ positions approved internally. Access requests mostly submitted through a single responsible department.	/ positions approved internally ¹⁴¹ .	/ positions approved internally.		/ positions approved internally.
ES	✓	x	✓ Public prosecutor working on the case.	✓ Judge working on the case.	✓ Only with involvement of police or judge.	✓	✓	x	x	✓ Only with involvement of police or judge.	x
FR	✓ Only judicial police officers.	x	✓ Public prosecutor working on the case.	✓ Judge working on the case.	✓ Civil servant at least of a 'controller' grade and	x	x	x	✓ Authorised agents authorized by the controller	x	✓ Investigator appointed by the Secretary

Prisons Department of the Ministry of Justice) can request all types of non-content data, whereas the bodies conducting proceedings (i.e. courts, the Prosecutor's Office) can only request subscriber data. However, it became evident through stakeholder consultation that the Prosecutor's Office may make non-content data requests by invoking an alternative provision. Nonetheless, while both the courts deciding criminal cases and the Prosecutor's Office have the possibility to request non-content data, neither submit such requests in practice, but rather request investigative bodies to do so, should the need arise.

¹⁴⁰ In Estonia, the tax and customs authorities form a single authority, the Tax and Customs Board, the structural units of which are responsible for performing different functions.

¹⁴¹ In Estonia, the police and border guard form a single authority, the Police and Border Guard Board, the structural units of which are responsible for performing different functions.

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
					designated by the service manager. Request should be authorised by the prosecutor of which the service depends.				of connection data requests. Requests should be made through the General Rapporteur		General. Request should be authorised by the controller of connection data requests.
IE	✓ Only officers of a certain rank.	x	x	x	✓ Only officers of a certain rank.	x	✓ Only officers of a certain rank.	NA	✓ No rank requirement.	x	x
IT	✓ Only with the authorisation and upon request of the Public Prosecutor.	x	✓ Public prosecutor delegates this task to police.	x	x	x	x	x	x	x	x
PL	✓ Any officer with authorisation of the superior	✓ Any officer with authorisation of the superior	✓ Public prosecutor working on the case.	✓ Judge working on the case.	✓ Any officer with authorisation from head of	✓ President of the Administration / head of a	x	✓ Any officer with authorisation of the command	x	✓ President of the bureau or a person authorised	x

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
	officer or any officer with the authorisation of the commander of a police department directly to ESPs.	officer or any officer with the authorisation of the commander of a police department directly to ESPs.			authority.	customs and tax office / any person authorised by them.		der of a police department.		by him/her.	
PT	✓ Any officer working on the case.	✓ Any officer working on the case.	✓ Public prosecutor working on the case.	x	x	x	x	✓ Any officer working on the case.	x	x	x
SI	✓ Any officer working on the case.	x	✓ Public prosecutor working on the case.	✓ Investigating judge working on the case.	x	x	x	x	x	x	x

Source: Milieu elaboration, from desk research and stakeholders' input

Table 15: Overview of competences of national authorities regarding retention of non-content data

Country	Competences of NRAs	Competences of DPAs	Overlap of competences	Potential issues
AT	<ul style="list-style-type: none"> Primarily responsible for the electronic communications sector Limited responsibilities, only if specified in the Telecommunications Act 	<ul style="list-style-type: none"> Primarily responsible for the protection of personal data Decides on complaints from data subjects about violations of their rights regarding processing of personal data, including in cases of access to non-content data Rules on retention periods and storage on non-content data 	✓	<ul style="list-style-type: none"> When checking compliance with the Telecommunications Act, NRA can also issue measures to enforce data protection provisions in the telecommunication sector DPA is also responsible to oversee protection of personal data in the electronic communications sector Stakeholders did not report any major issues
DE	<ul style="list-style-type: none"> Can issue orders and other measures to ensure compliance with Chapter 7 of the Telecommunications Act, including on topic such as data protection Can issue technical and security guidelines 	<ul style="list-style-type: none"> Limited to protection of personal data with comprehensive investigative powers 	✓	<ul style="list-style-type: none"> If NRA adopts security guidelines regarding retention, an approval of the DPA is needed The DPA addresses its complaints to the NRA and transmits further results of its inspection to the NRA at its own discretion Stakeholders did not report any major issues
EE	<ul style="list-style-type: none"> Primarily responsible for electronic communications sector Supervision powers over the ESPs obligations to retain data, delete data and provide statistics 	<ul style="list-style-type: none"> Primarily responsible for the protection of personal data Decides on complaints from data subjects, including in relation to the unlawful processing of their electronic communications non-content data Ensures ESPs compliance with the rules on processing of personal data, including rules in the Electronic Communications Act (e.g. ESPs need to report on personal breaches) 	✓	<ul style="list-style-type: none"> Stakeholder input revealed that the DPA does not exercise pro-active supervision over the non-content data requests but only handles complaints
ES	<ul style="list-style-type: none"> Primarily responsible for the telecommunications sector and audio-visual communication services Primarily competent in cases when ESPs do not retain the necessary data 	<ul style="list-style-type: none"> Primarily responsible for the protection of personal data, in particular in respect of security standards and if data are retained for a shorter period of time than prescribed by law 	✓	<ul style="list-style-type: none"> Competence to oversee ESPs obligations under national data retention rules are shared between the DPA and the NRA Competences of the DPA are restricted only to being a sanctioning authority, whereas the competences of the NRA go beyond the merely sanctioning field

Country	Competences of NRAs	Competences of DPAs	Overlap of competences	Potential issues
FR	<ul style="list-style-type: none"> Based on law, NRA is responsible for the retention obligation in the telecommunication sector The NRA however indicated that it does not have any competence, stating that the competent authority is the Inter-ministerial Defence Electronic Communications Commissioner, in charge of the implementation of the technical aspects of SPOCs and the relation with the ESPs 	<ul style="list-style-type: none"> Primarily responsible for the protection of personal data 	*	<ul style="list-style-type: none"> Based on limited stakeholder input no overlaps of competences has been detected
IE	<ul style="list-style-type: none"> Oversight and supervisory role regarding ESPs complying with all pertinent legal obligations, including data retention obligations Statutory investigatory powers such as the compelling of the provision of information to it by ESPs, where it is a criminal offence not to comply 	<ul style="list-style-type: none"> Primarily responsible for the protection of personal data, in particular in respect of security standards The designated High Court judge may communicate with the DPA regarding matters relevant to its function 	✓	<ul style="list-style-type: none"> Stakeholders did not report any major issues
IT	<ul style="list-style-type: none"> Primarily advisory and monitoring role, which is exercised actively Maintains the Registry of Enrolled Operators - ROC Supervision over ESPs obligations to support the LEAs, which include power of suspension or even loss of the licence and possible criminal sanctions 	<ul style="list-style-type: none"> Exclusive competences for the protection of personal data The role in supervising the ESPs' obligations is limited to security requirements and more of an advisory role Can issue opinions (e.g. criticizing the extension of the retention period to 72 months) 	✓	<ul style="list-style-type: none"> Data retention for LEAs is essentially a DPA competence DPA and NRA need to cooperate on some topics Stakeholders did not report any major issues
PL	<ul style="list-style-type: none"> Supervision of telecommunications undertakings as regards their compliance with legal 	<ul style="list-style-type: none"> Supervises compliance with the provisions on the protection of personal data, including the ones in the Telecommunications Law 	✓	<ul style="list-style-type: none"> Competences in the area of confidentiality and personal data overlap, but DPA remains the competent authority for the protection of personal data

Country	Competences of NRAs	Competences of DPAs	Overlap of competences	Potential issues
	requirements in the area of data retention ■ Supervision over ESPs' compliance with the telecommunications confidentiality regulations	■ No competence over judicial bodies		
PT	■ No competence over data retention topics	■ Wide supervisory powers both in terms of supervision over data protection rules (e.g. complaints from data subjects) and data retention rules ■ Supervisory powers over ESPs obligation to guarantee the protection and safety of non-content data, which include investigative powers and powers to receive certain records and statistics	✖	■ Responsibilities are centralised by the DPA, while the NRA does not have a role on data retention topics
SI	■ Supervision and sanction powers regarding the legal basis, the purpose and the time period of data retention ■ No legal powers over the obligation of the ESPs to assist LEAs in access to non-content data	■ Primarily responsible for the protection of personal data ■ Can demand from the ESPs to inform them about security measures taken and the number of access requests	✓	■ Stakeholders believe the roles are relatively clearly divided

Source: Milieu elaboration, from desk research and stakeholders' input

Retention of non-content data

This section of Annex III presents the detailed analysis materials referred to in section 5 of the report.

Table 16: Subscriber data retained per Member State

	AT	DE	EE	ES	FR	IE	IT	PL	PT	SI
IP address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Name	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Email address	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓
Physical address	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Telephone number	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Username	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓
Billing and payment information	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓

Table 17: Identification data retained per Member State

	AT	DE	EE	ES	FR	IE	IT	PL	PT	SI
IP address	Access data	T	S	T	S	S	T	T	S/T	T
Device identification numbers (e.g. IMEI)	Access data	T	S	T	S	S	T	T	S/T	T
Port number for dynamic IP address	✗	✗	✗	T	S	✗	T	T	S/T	T
SIM number	Access data	T	S	T	S	S	T	T	S/T	T

Note: T means the data is considered as traffic data, S means the data is considered as subscriber data. Austria has a distinct category of data named 'access data'. There are disagreements between ESPs and LEAs in Portugal over the interpretation of the national law.

Table 18: Traffic data retained per Member State

	AT	DE	EE	ES	FR	IE	IT	PL	PT	SI
Duration of the communication	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Date & time of the communication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data volume of the communication	✓	✓	✗	✓	✓	✗	✓	✗	✓	✓
Missed calls (incl. N° of rings)	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓
Start & end of the communication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Connection/disconnection from the service	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓
Type of communication (e.g. voice, SMS...)	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Type of network technology (e.g. Wi-Fi, 3/4G network)	✗	✗	✓	✓	✓	✓	✓	✗	✓	✓
Identifiers of the receiver(s) of a communication	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Identifiers of the forwarded, routed or transferred receiver(s)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Identifiers of the attempted receiver(s).	✓	✗	✓	✗	✗	✓	✓	✓	✗	✓

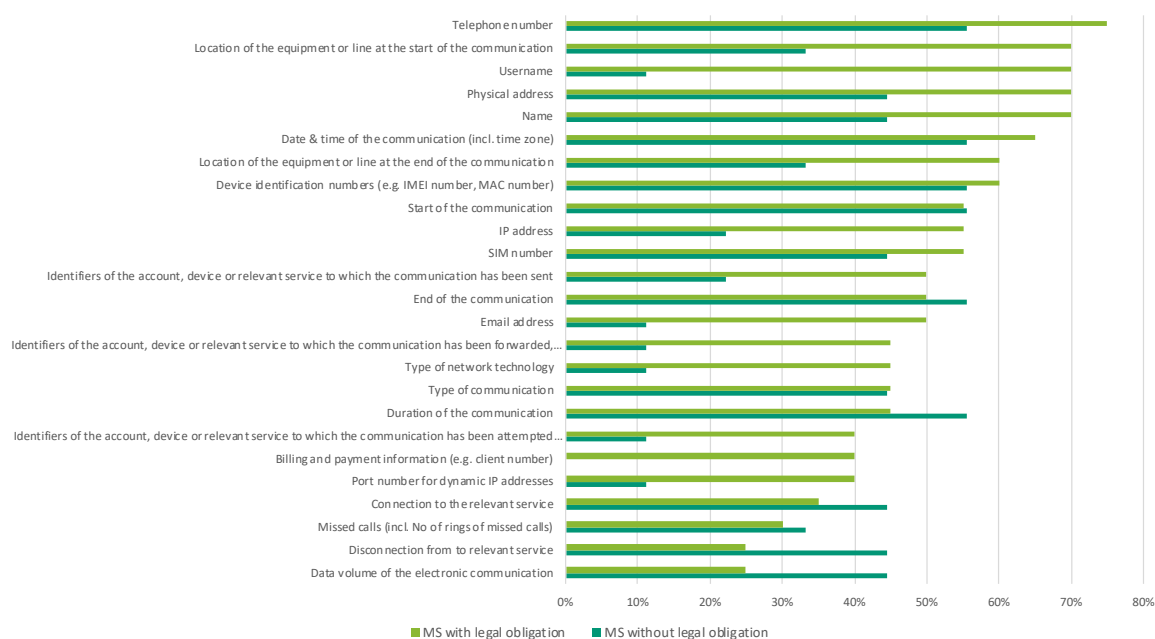
Table 19: Location data retained by Member State

	AT	DE	EE	ES	FR	IE	IT	PL	PT	SI
Location at the start of the communication (e.g. cell towers, Wi-Fi hotspots)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Location at the end of the communication (e.g. cell towers, Wi-Fi hotspots)	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓

Note: These tables are based on the national laws of the Member States covered by the Study and if at least one ESP survey respondent stated that they retain the type of data listed. It is possible, however, that not all ESPs operating within a Member State retain all of the data points. Source: Milieu elaboration, from desk research and stakeholders' input

Access to and Use of non-content data by law enforcement authorities

This section of Annex III presents the detailed analysis materials referred to in section 6 of the report.

Figure 35: In how many cases on average do you use this type of data? Respondents who answered in at least 60% of cases – by type of Member State

Note: This figure only shows police and public prosecutor responses. Other types of respondents were excluded as they either do not request non-content data at all (they are not investigative or prosecution bodies) or in only rare cases.

Source: Survey to LEAs, question 21, (N=28)

Procedure to access non-content data

This section of Annex III presents the detailed analysis materials referred to in section 7 of the report.

Table 20: Types of crimes for which LEAs can access non-content data based on the national legislative frameworks

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
AT	<u>Criminal police</u> : No crime threshold to access subscriber data. Access to other types of data only in case of imminent danger ¹⁴² . <u>Security police</u> : No crime threshold to access any type of data	-	No crime threshold to access subscriber data. Access to other types of data linked to specific crime thresholds		Can only access subscriber data for revenue crimes - no threshold. To access traffic data linked to IP addresses: minimum penalty for financial offenses must exceed €10,000	Access only for specific types of crimes (e.g. terrorism) with a threshold >1 year imprisonment	-	-	-	Access only for specific types of crimes (e.g. bribery) - no threshold.	-
DE	Distinction between access to data retained for business purposes and	-	Distinction between access to data retained for business purposes and mandatory data. <u>Business</u> : only crimes of considerable significance		Crimes of a full taxation nature or combined with other crimes and public charges	-	Crimes linked specifically to the traffic of weapons	-	-	-	-

¹⁴² Translation of Article 76a paragraph 2 of the Austrian Code of Criminal Procedure.

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
	mandatory data. <u>Business:</u> only crimes of considerable significance to be decided on a case-by-case basis. <u>Retained data:</u> list of specific crimes		to be decided on a case-by-case basis. <u>Retained data:</u> list of specific crimes		which touch upon tax bases, tax measurements or tax amounts.						
EE	No crime threshold but <i>ultima ratio</i> principle applies.		No crime threshold but <i>ultima ratio</i> principal		No revenue crime threshold but ultima ratio principal	No crime threshold but ultima ratio principal			No competition crime threshold but ultima ratio principal	No corruption crime threshold but ultima ratio principal	No financial crime threshold but ultima ratio principal
ES		-	Only for serious crimes		-	Only for serious crimes		-	-	-	-
FR	No crime/offence threshold	-	No crime/offence threshold		Specific revenue crimes	-	-	-	Only competition crimes – no threshold	-	Market abuses
IE	Only for serious crimes	-	-	-	Only for serious revenue crimes	-	Only for serious crimes	-	Only for serious competition crimes	-	-
IT	Access linked to the Public Prosecutor	-	Serious crimes for access within 72	-	-	-	-	-	-	-	-

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
			months, and any crimes for access within shorter periods of time depending on the type of data								
PL	No crime/offence threshold		No crime/offence threshold		Only revenue crimes – no threshold	No crime/offence threshold	-	No crime/offence threshold	-	Only corruption crimes – no threshold	-
PT	Only for serious crimes listed in the legislation		Only for serious crimes listed in the legislation	-	-	-	-	Only for serious crimes listed in the legislation	-	-	-
SI	Only for specific crimes listed in the legislation	-	Only for specific crimes listed in the legislation		-	-	-	-	-	-	-

Source: Milieu elaboration, from desk research and stakeholders' input

Table 21: Ex-ante authorisations required to access non-content data

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
AT	<u>Criminal police:</u> No authorisation to access subscriber data. For other types of data need order of the Public Prosecutor with judicial authorisation. <u>Security police:</u> No authorisation required	-	No authorisation required		None	Authorisation following review of legal protection officer (valid for maximum of 6 months)	-	-	-	No authorisation to access subscriber data. For other types of data need order of the Public Prosecutor with judicial authorisation.	-
DE	Judicial authorisation - except for access to subscriber data	-	Judicial authorisation - except for access to subscriber data	Authority responsible for granting authorisation	Judicial authorisation - except for access to subscriber data	-	Judicial authorisation except for access to subscriber data	-	-	-	-

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
EE	No authorisation needed to access subscriber data. For other types of data it depends on the type of offence. <u>Criminal offences:</u> Authorisation from the Prosecutor's Office in pre-court proceedings and Court authorisation during court proceedings <u>Misdemeanours:</u> Court authorisation.		Authorities responsible for granting authorisation. To a limited extent can request non-content data in criminal proceedings (no additional authorisation necessary) but in practice rarely do.		No authorisation needed to access subscriber data. For other types of data it depends on the type of offence. <u>Criminal offences:</u> Authorisation from the Prosecutor's Office in pre-court proceedings and Court authorisation during court proceedings. <u>Misdemeanours:</u> Court authorisation. ¹⁴³			Can make non-content data requests in criminal proceedings. No authorisation needed to access subscriber data. For other data, authorisation from the Prosecutor's Office in pre-court proceedings and Court authorisation during court proceedings	No authorisation needed to access subscriber data. For other types of data it depends on the type of offence. <u>Criminal offences:</u> Authorisation from the Prosecutor's Office in pre-court proceedings and Court authorisation during court proceedings <u>Misdemeanours:</u> Court authorisation	Can make non-content data requests in misdemeanour proceedings. No authorisation needed to access subscriber data. For other data, authorisation from the Court.	
ES	Judicial authorisa-	-	Judicial authorisa-	Authority responsible	-	Judicial authorisation	Judicial authorisation	-	-	-	-

¹⁴³ Concerning security authorities it should be noted that while ex-ante authorisation is required for non-content data requests in criminal and misdemeanour proceedings (save for requesting subscriber data), security authorities do not require external ex-ante authorisation prior to submitting the request pursuant to the Security Authorities Act for purposes of ensuring national security and constitutional order.

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
	tion except for subscriber data		tion, except for subscriber data	for granting authorisation							
FR	Authorisation from the Public Prosecutor	-	Authority responsible for granting authorisation	Can only act with a mandate from the Prosecutor	Authorisation from the Public Prosecutor	-	-	-	Authorisation from a Magistrate from Council of State or Court of Cassation	-	Authorisation from a Magistrate from Council of State or Court of Cassation
IE	If traditional procedure to obtain evidence is applied, a warrant from District Court is needed, on Garda application, to investigate a specific crime.	-	-	-	Authorisation from a superior above a certain rank.	-	None	-	None	-	-
IT	Only with mandate from Public Prosecutor –	-	Must issue a reasoned order	-	-	-	-	-	-	-	-

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
	also, right for investigated person or the defendant in criminal proceedings (their lawyers) to access metadata phone/ Internet line handed to the investigated person / defendant for a period of 24 months.										
PL	None		None		None	None	-	None	-	None	-
PT	Authorisation from investigative judge - except for subscriber data		None	Authority responsible for granting authorisation - except for subscriber data	-	-	-	Authorisation from investigative judge except for subscriber data	-	-	-

MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
SI	Authorisation from investigative judge	-	Authorisation from investigative judge	Authority responsible for granting authorisation	-	-	-	-	-	-	-

Source: Milieu elaboration, from desk research and stakeholders' input

Table 22: Ex-post supervision of access to non-content data by LEAs

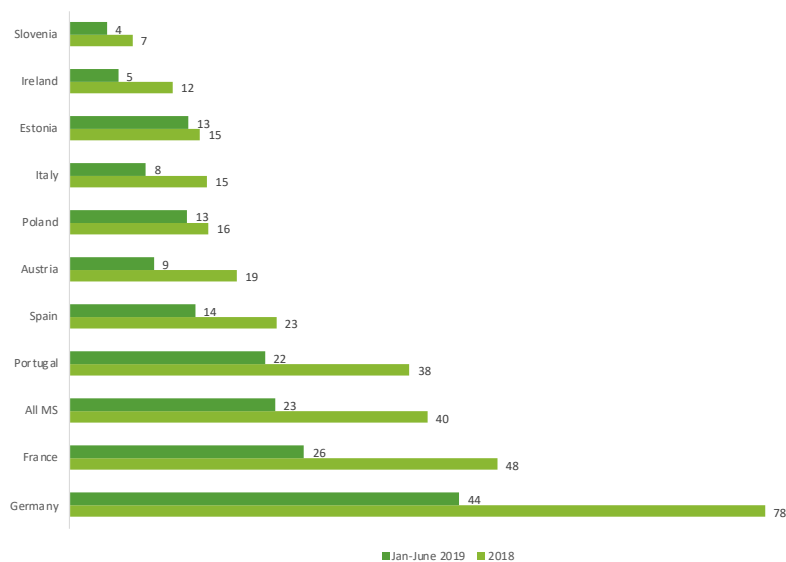
MS	Police authorities		Judicial authorities		Other national authorities						
	Police authorities	Military police	Public Prosecutors	Investigating and other judges	Tax authorities	Intelligence agencies	Customs authorities	Border guard	Competition authorities	Anti-corruption authorities	Financial authorities
AT	For security police: Review by the legal protection officer at Ministry of Interior	-	None		Review by the legal protection officer at the Ministry of Finance	None	-	-	-	In some cases, review by the legal protection officer	-
DE	None	-	None		None	-	None	-	-	-	-
EE	None		None		None	Committee of the Estonian Parliament	None				
ES	None	-	None		-	None		-	-	-	-
FR	None	-	None		None	-	-	-	None	-	None
IE	Review by High Court Judge	-	-	-	Review by High Court Judge	-	Review by High Court Judge	-	Review by High Court Judge	-	-
IT	Access linked to Public Prosecutor	-	None	-	-	-	-	-	-	-	-
PL	Review by district court		Review by district court		Review by district court		-	Review by district court	-	Review by district court	-
PT	None		None		-	-	-	None	-	-	-
SI	Mandatory control by the investigative judge	-	Mandatory control by the investigative judge	None	-	-	-	-	-	-	-

Source: Milieu elaboration, from desk research and stakeholders' input

Retention and access to OTTs

This section of Annex III presents the detailed analysis materials referred to in section 8 of the report.

Figure 36: Number of requests sent to OTTs per 100 000 population in 2018 and in Jan-June 2019



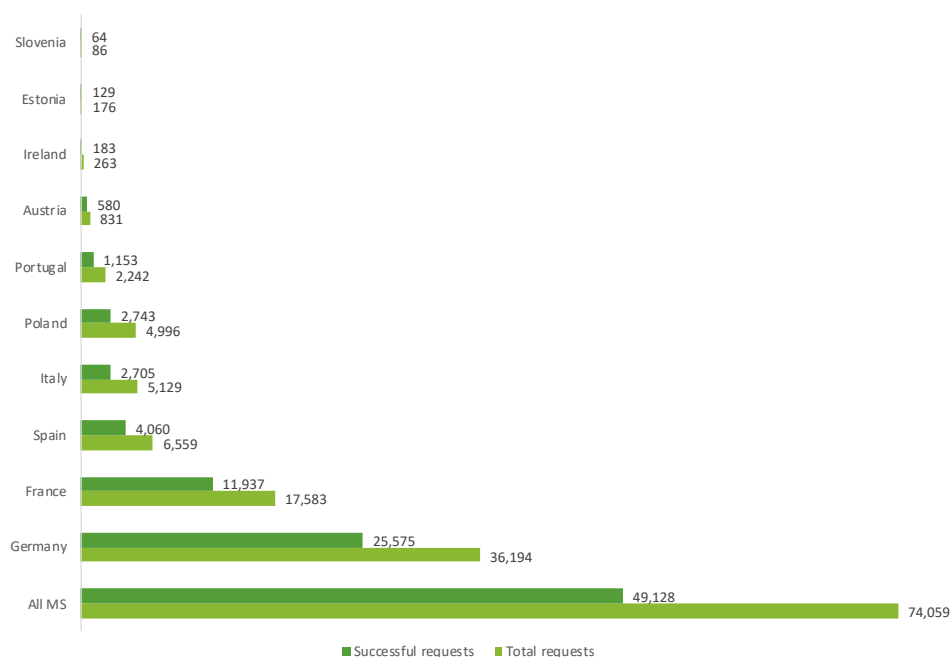
Source: Milieu elaboration from the transparency reports of OTTs and Eurostat data

Figure 37: Number of requests sent to OTTs vs number of accounts specified in Jan-June 2019



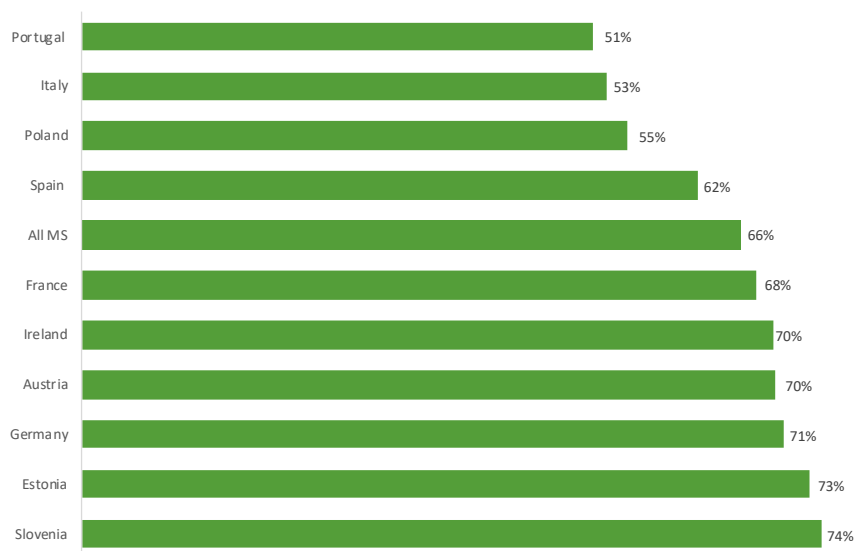
Source: Milieu elaboration from the transparency reports of OTTs

Figure 38: Successful vs total requests sent to OTTs between January and June 2019 in absolute numbers



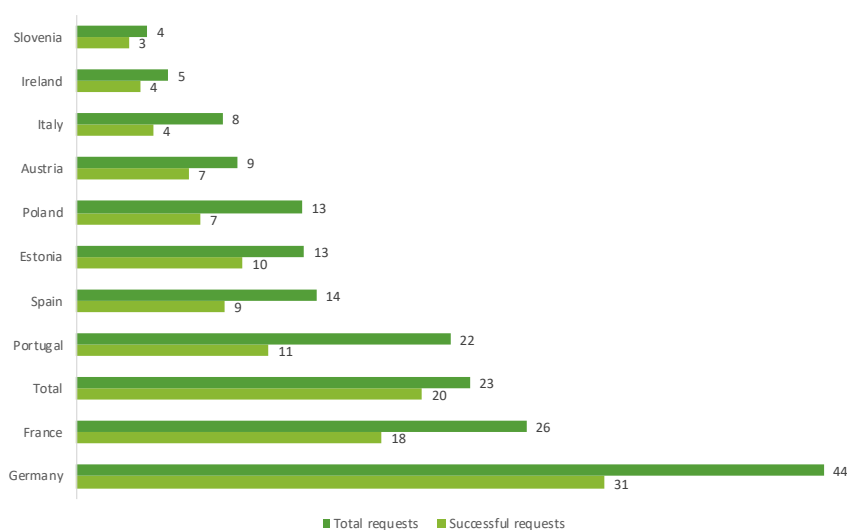
Source: Milieu elaboration from the transparency reports of OTTs

Figure 39: Success rate of requests sent to OTTs between January and June 2019 in percentages



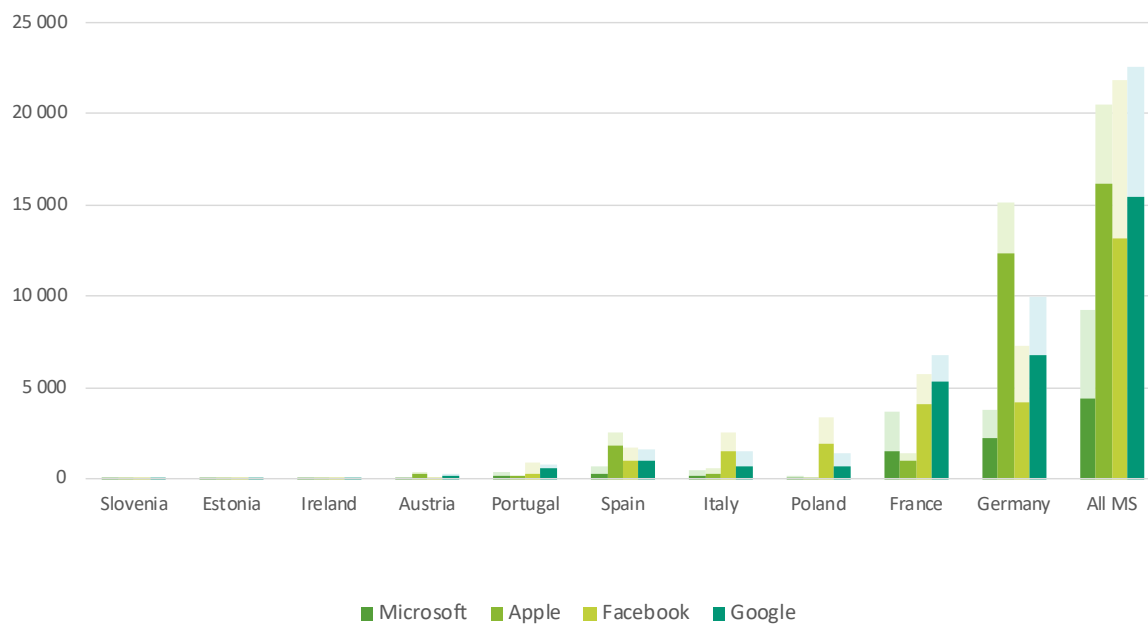
Source: Milieu elaboration from the transparency reports of OTTs

Figure 40: Successful vs total requests sent OTTs between January and June 2019 per 100,000 population



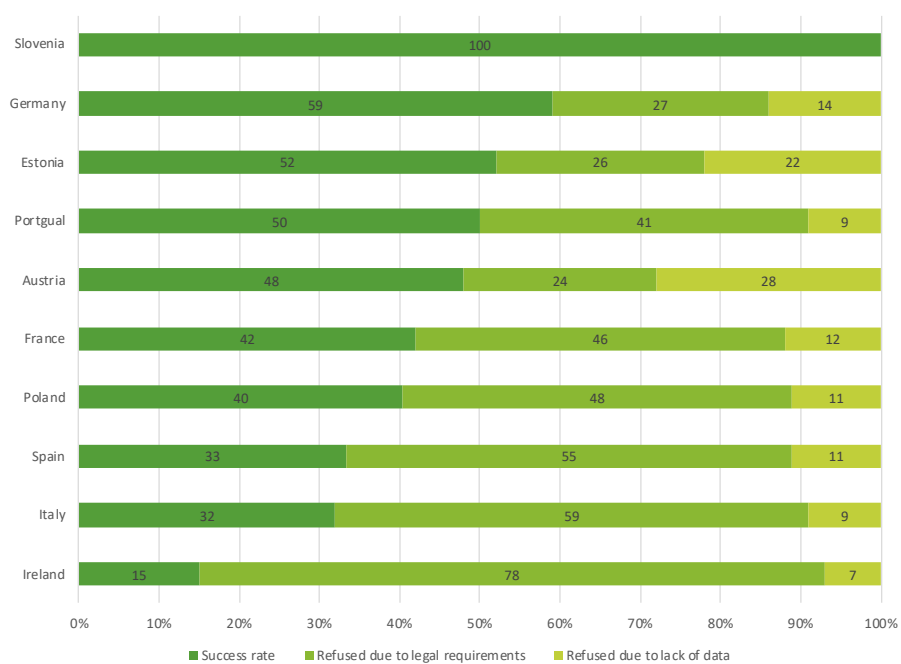
Source: Milieu elaboration from the transparency reports of OTTs and Eurostat data

Figure 41: Successful vs total requests sent to individual OTTs between January and June 2019



Note: The darker colour shades represent the total number of successful requests whereas the lighter colour shades represent the total number of requests sent.

Source: Milieu elaboration from the transparency reports of OTTs

Figure 42: Reasons for rejecting requests sent to Microsoft between January and June 2019

Source: Milieu elaboration from OTTs transparency reports

Lessons learnt and future challenges

Table 23: Comparing the state of play at the ESPs/OTTs and the needs of LEAs as to the types of non-content data

Member State	Non-content data retained by the ESPs		Non-content retained by the OTTs	Non-content data needed by the LEAs
	Retained for law enforcement purposes	Retained for business and other purposes		
AT	✗	All data is retained for at least one internal purpose. The most relevant is to look at data retained for invoicing purposes as these are retained longer and for more stable periods of time given the legal threshold for bill contestation. Most ESPs retain subscriber data and traffic data for invoicing purposes. The 'problematic' data points are identification and location data that are generally not retained for invoicing.		All LEAs stated that they use all type of data. Data most frequently requested are subscriber data and traffic data – but overall data are generally requested as a package (several data points at the same time). The types of data most frequently needed vary with type of crime investigated – the investigation of cybercrimes for example needs IP addresses more than for other crimes. From the experiences of LEAs in Member States without data retention, the most problematic data points are IP addresses and port numbers for dynamic IP addresses. German LEAs also indicated that they have difficulties accessing location data which are rapidly deleted by ESPs, as they have no business value.
DE	✗			
EE	All data – however ESPs do not have a legal obligation to retain port numbers for dynamic IP addresses			
ES	All data			
FR	All data			
IE	All data – however ESPs generally do not retain port numbers for dynamic IP addresses due to differences in the interpretation of the national law.			
IT	All data			
PL	All data			
PT	All data			
SI	✗			

Source: Milieu elaboration, from desk research and stakeholders' input

Table 24: Comparing the state of play at the ESPs/OTTs and the needs of LEAs as to the retention periods

Member State	Retention period of non-content data retained by the ESPs		Retention period of non-content data retained by the OTTs	Average 'age' of data needed by the LEAs
	Retained for law enforcement purposes	Retained for business and other purposes		
AT	x			Depends on the type of crime investigated. For some types of crimes, such as robberies, when the crime can be detected rapidly 3 months is reportedly enough. For other types of crimes, notably cybercrimes, child pornography and fraud, the retention periods are reportedly not long enough, as these crimes are often only detected much later. The most common types of data that seem to be an issue for MS without data retention are IP addresses, port numbers for IP addresses and location data – which, even if they are retained by some ESPs for internal purposes, are usually deleted rapidly.
AT	x	Average 3 months		
DE	x	Maximum 6 months, many types of data are deleted within 7 days		
EE	12 months	1-3 months		
ES	12 months	12 months		Same as above, it depends on the type of crime. French stakeholders do not want the data retention period to change – they advocate for long data retention periods.
FR	12 months	12 months		
IE	12 months internet data 24 months telephone data	No stakeholder input		
IT	De facto 72 months	Maximum 6 months		
PL	12 months	No stakeholder input		Same as above, it depends on the type of crime.
PT	12 months	Maximum 6 months		
SI	x	Average of 3 months		

Source: Milieu elaboration, from desk research and stakeholders' input

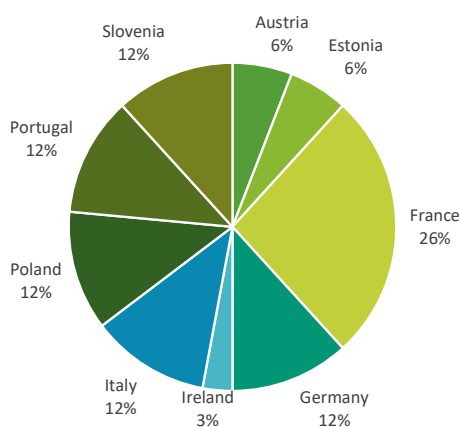
ANNEX IV: RESULTS OF THE SURVEY TO LAW ENFORCEMENT AUTHORITIES (LEAS)

Annex IV presents the aggregated results for all closed survey questions addressed to LEAs, processed on aggregated level and anonymised. The total number of respondents is 34. Only the graphs for closed questions are presented in Annex IV. Answers to open-ended questions were taken into account in the overall analysis in the body of the text.

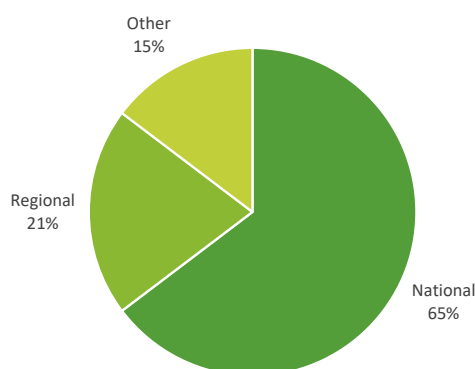
Profiling questions

The first section of the survey asked respondents questions about their profile – e.g. country, territorial scope, types of crimes investigated etc.

Q.1 - In which country is your organisation based?

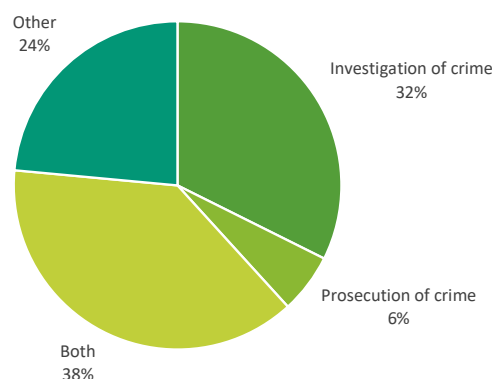


Q.3 - What is the territorial scope of your activities?



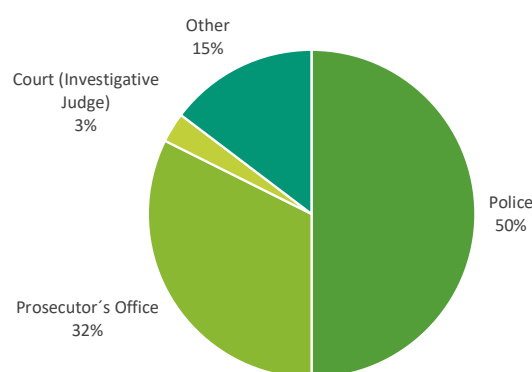
Those respondents who answered 'Other' specified both regional and national, national and international or provincial.

Q.4 - What is your organisation's role in the criminal procedure?



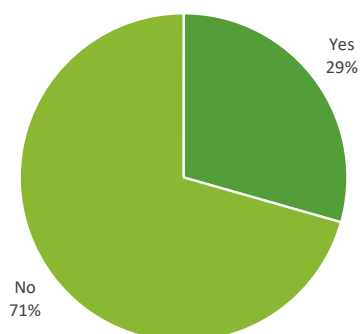
Those respondents who answered 'Other' specified the following other roles, investigations on cases of flagrante delicto (crimes caught red-handed) or central/coordination bureaus and organisations responsible for certain types of offences that are not considered criminal offences.

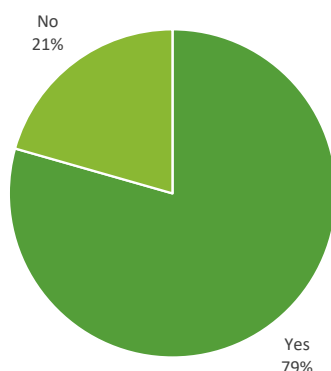
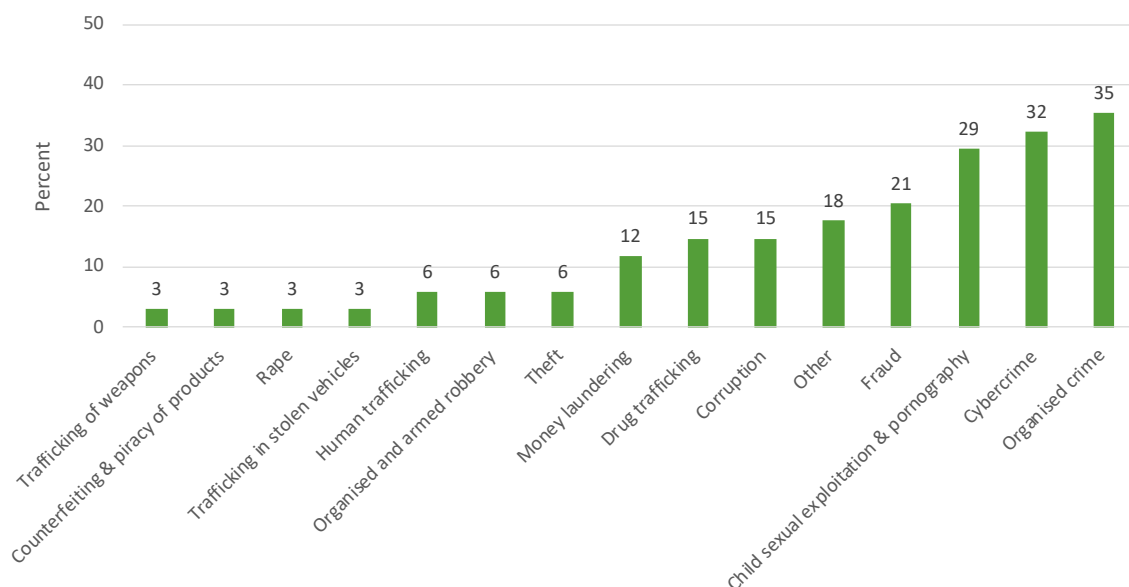
Q.5 - What type of law enforcement authority do you belong to?



Those respondents who answered 'Other' specified that they are either central/coordination bodies that are not investigation/prosecution bodies, regulatory authorities or tax and customs authorities.

Q.6 - Do your activities include the preventive safeguarding of national security?



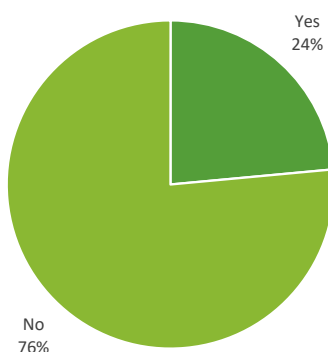
Q.7 - Does your organisation investigate and/or prosecute specific types of crimes?**Q.8 - Which types of crime does your organisation investigate and/or prosecute? Please select up to three (3) types of crimes, which are the focus of your activities.**

Those respondents who answered 'Other' specified the following other crimes, terrorism, immigration, market abuse, tax offences, environmental crimes, embezzlement of public funds, and some respondents stated that they investigate all of the listed crimes.

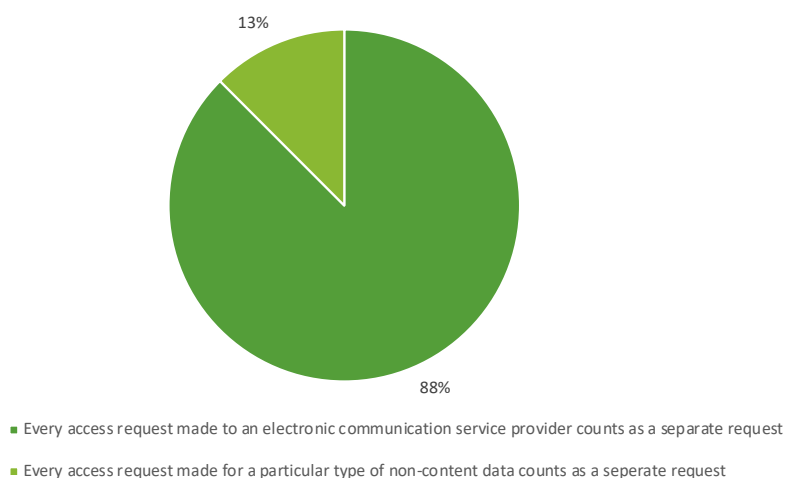
National practices of using electronic communications non-content data (metadata) in investigation and/or prosecution

This section focuses on the frequency of use of non-content data (metadata) in the investigation and/or prosecution of criminal cases.

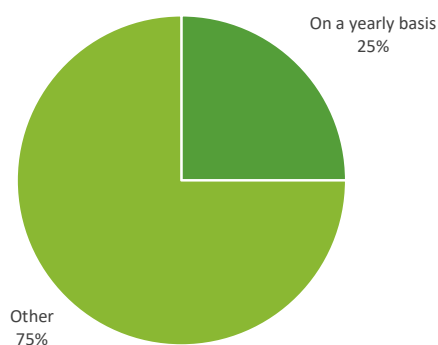
Q.9 - Do you hold any statistics on the number of requests for non-content data to electronic communication service provider? (N=34)



Q.10 – If yes in Q.9, how do you record the number of access requests? (N=8)



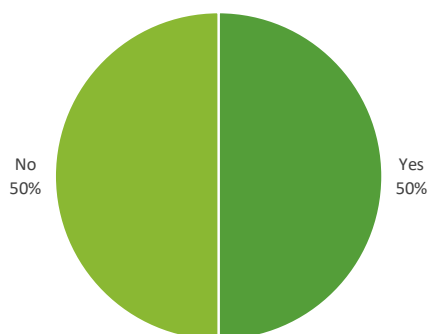
Q.11 - How often do you record requests to access such non-content data? (N=8)



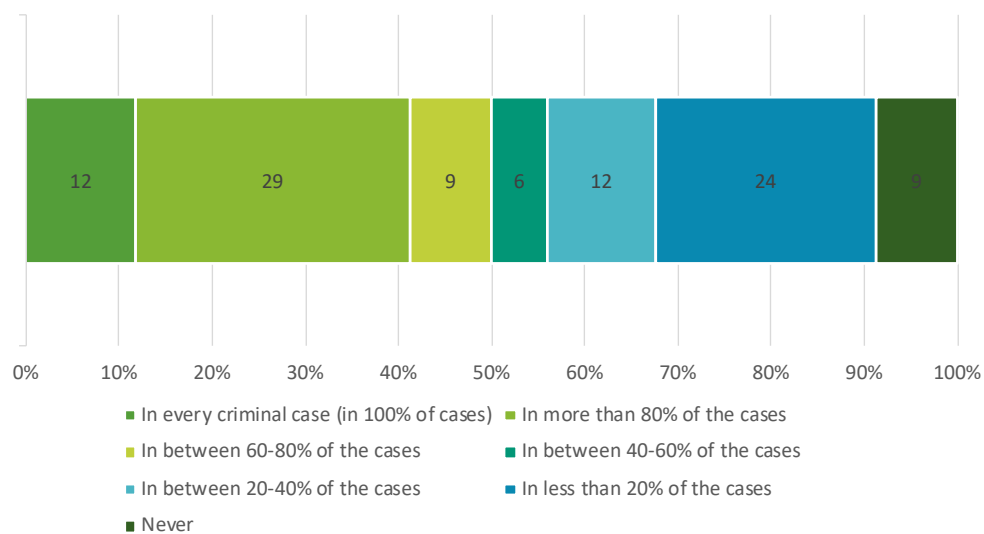
Most of the respondents who answered 'Other' specified that requests are recording on an ongoing basis – i.e. immediately after submitting the request. One respondent stated that requests are

recorded on a bi-annual basis. Another respondent specified that there is a national processing system which records requests.

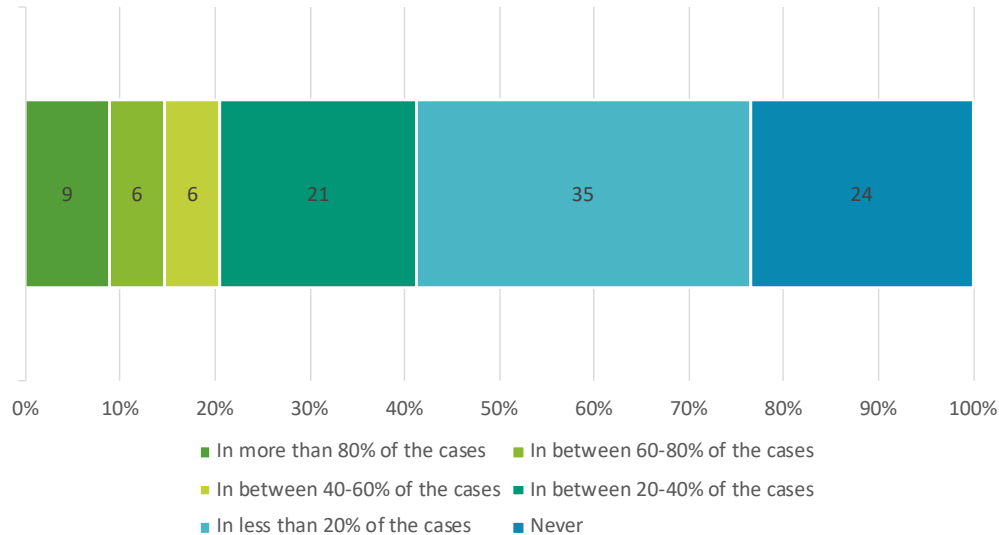
Q.12 - Do you publish any transparency or other types of reports on the number of requests to access non-content data? Alternatively, do you make data on the number of requests publicly available? (N=8)



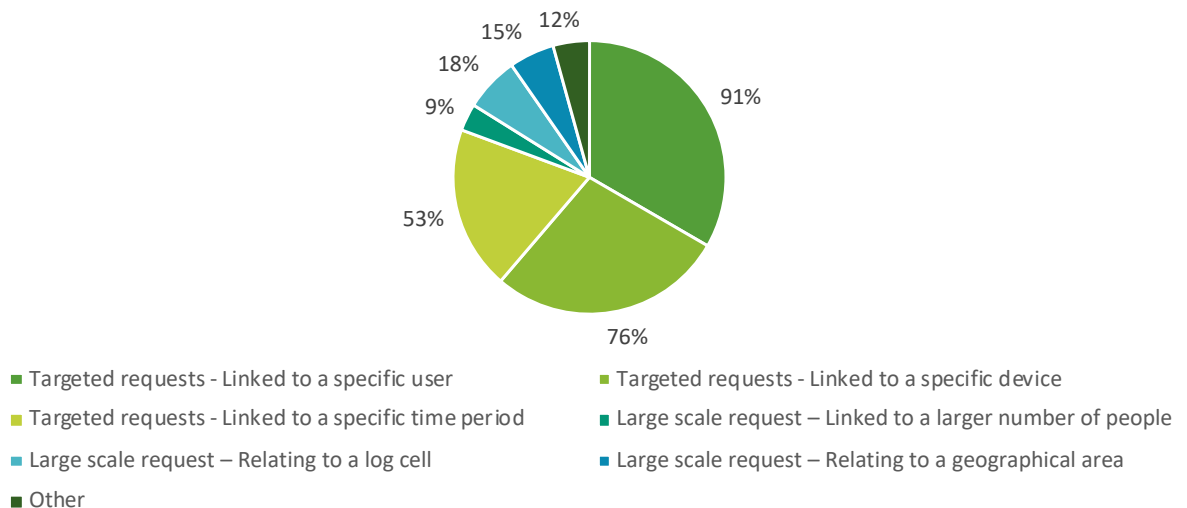
Q.14 - On average, how often did you request access to non-content data in the course of a criminal investigation/prosecution in the last two (2) years (2018 and 2019)? If data for 2019 are not yet available, please provide data for the years 2017 and 2018. (In the absence of official statistics, please provide an estimation, based on your own experience.) (N=34)



Q.15 - On average, to what extent did you request non-content data retained by 'Over-the-Top' communication service providers (e.g. WhatsApp, Telegram communications etc.) in the course of a criminal investigation/prosecution in the last two (2) years (2018 and 2019)? If data for 2019 are not yet available, please provide data for the years 2017 and 2018. (In the absence of official statistics, please provide an estimation, based on your own experience.) (N=34)



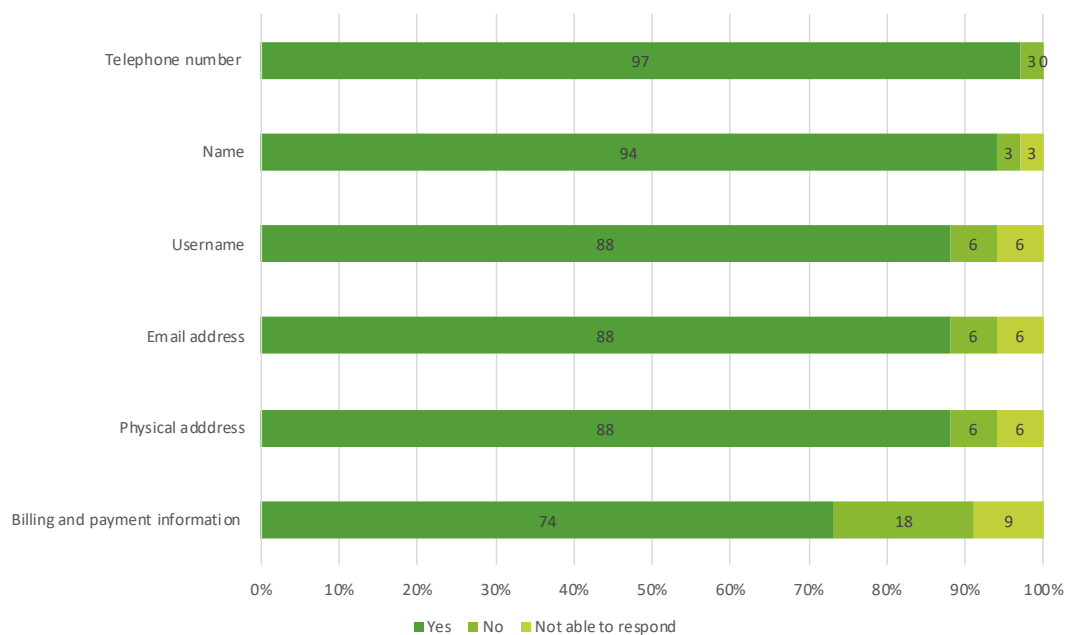
Q.17 - What is the most frequent practice to request non-content data? Please select up to three (3) types of practices. (N=34)



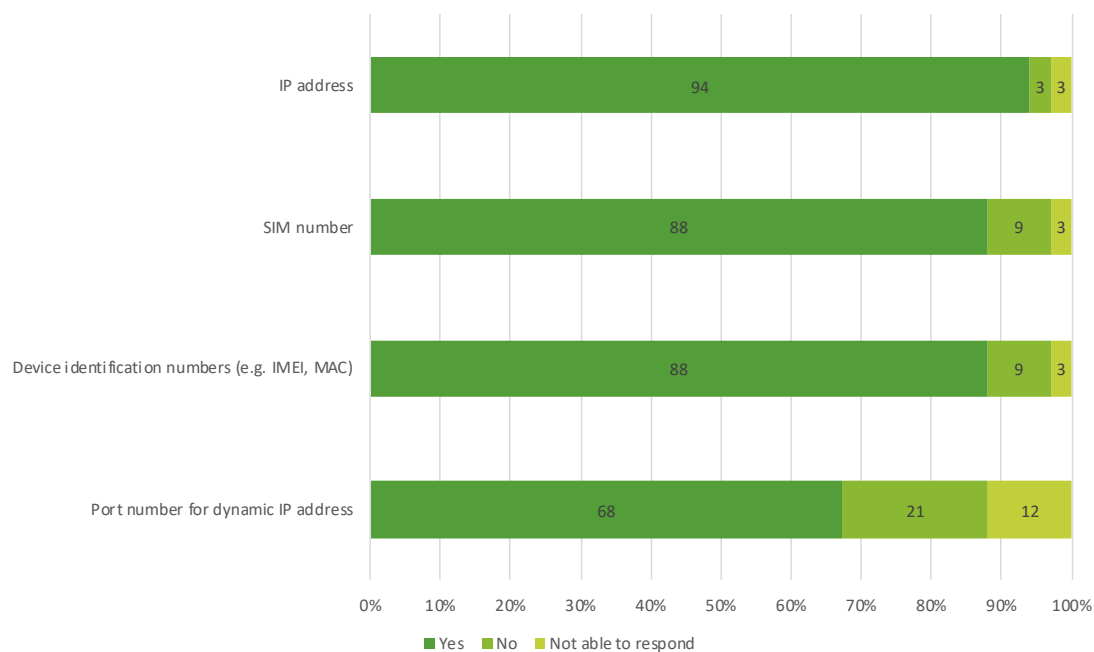
Six respondents answered 'Other': for four of these respondents the question was not applicable/cannot answer. One respondent specified 'targeted requests - linked to a phone number' and another respondent specified 'Geolocated traffic requests'.

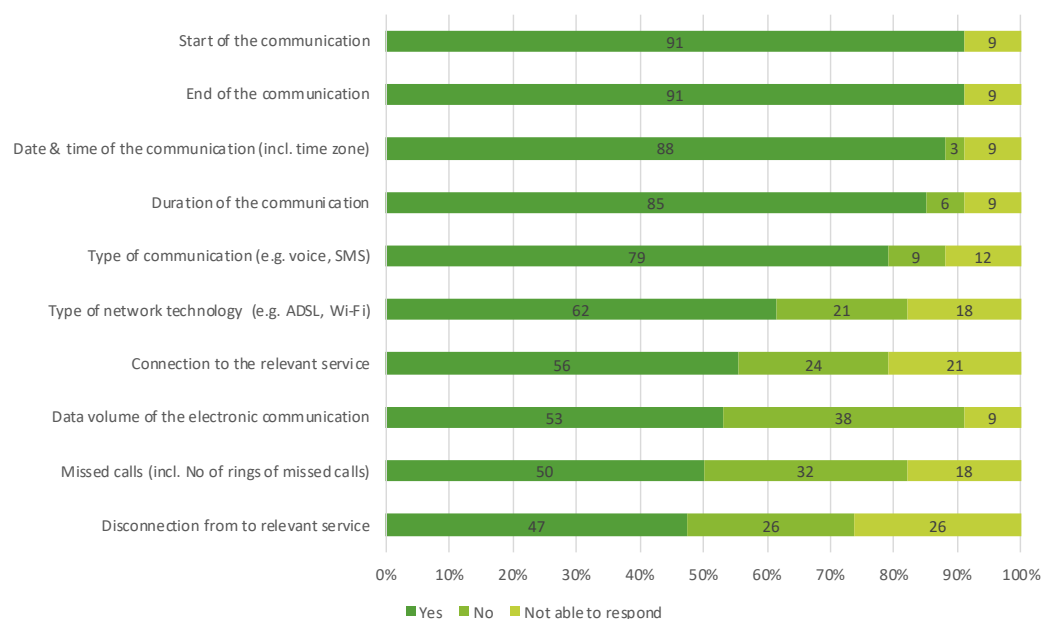
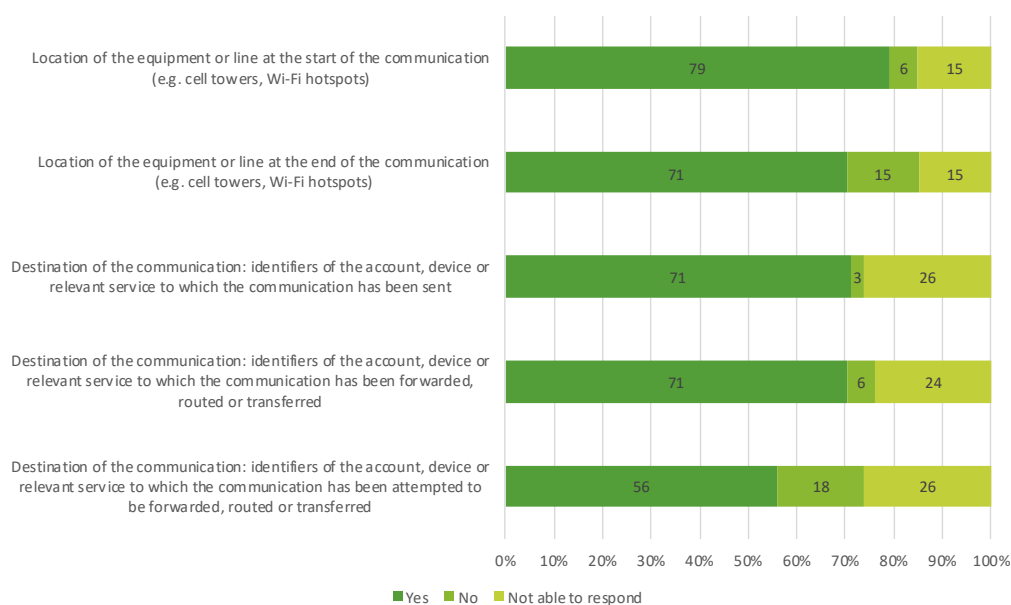
Q.22.a - Which types of non-content data do you request in the course of an investigation/prosecution? Please provide an estimation of the use of different types of non-content data during the course of one year. (N=34)

Subscriber data – use (Y/N)



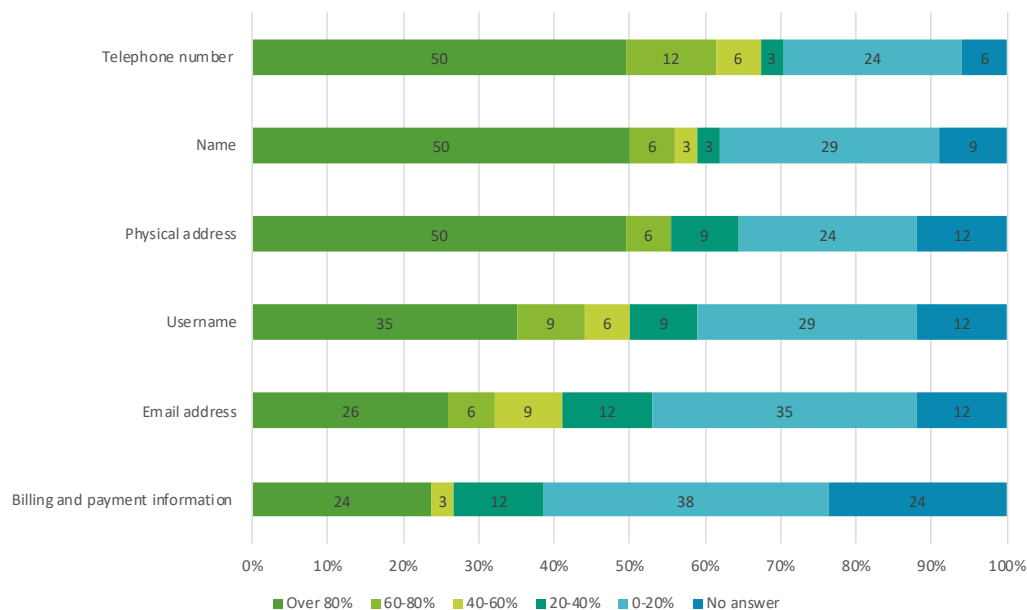
Identification data – use (Y/N)



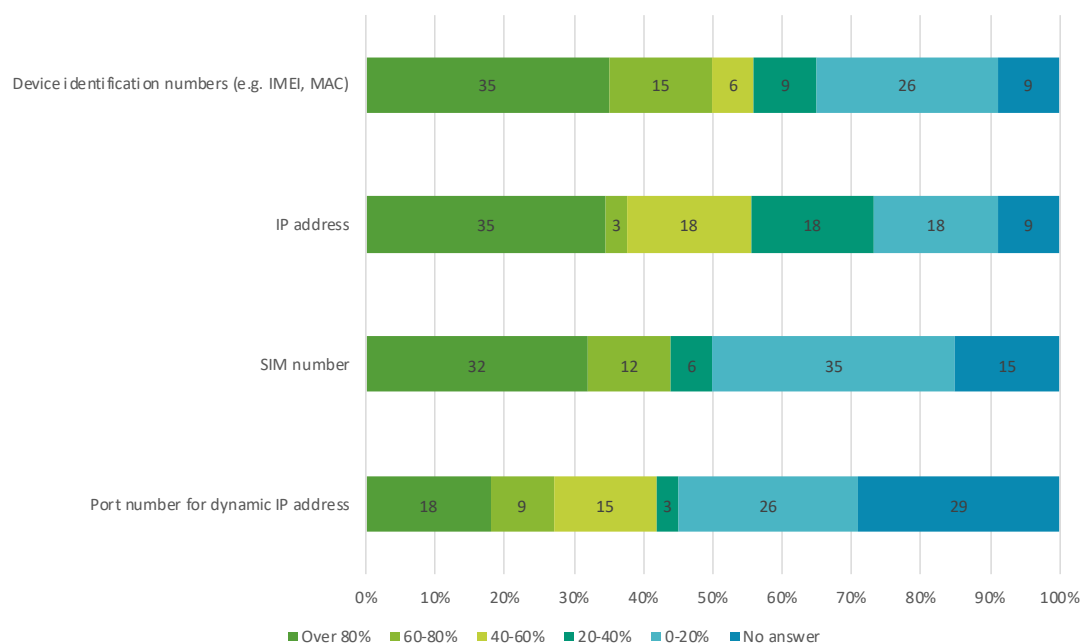
Traffic data – use (Y/N)**Location data and data on the destination of a communication – use (Y/N)**

Q.22.b - In how many cases on average do you request the non-content data listed below in the course of an investigation/prosecution? Please provide an estimation of the use of different types of non-content data during the course of one year. (N=34)

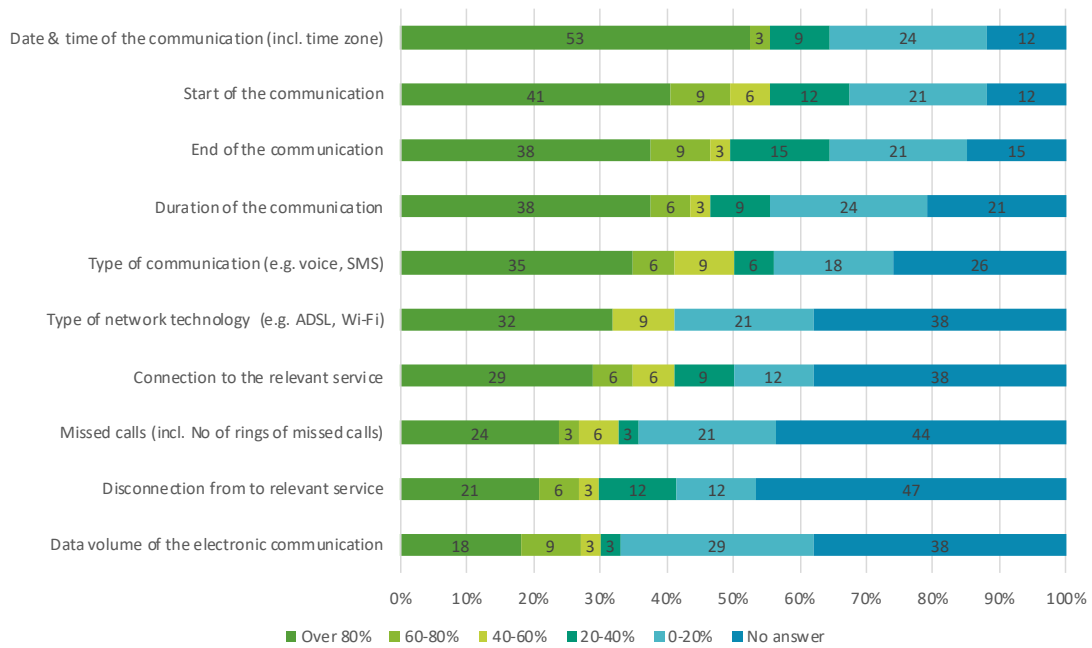
Subscriber data – frequency of use



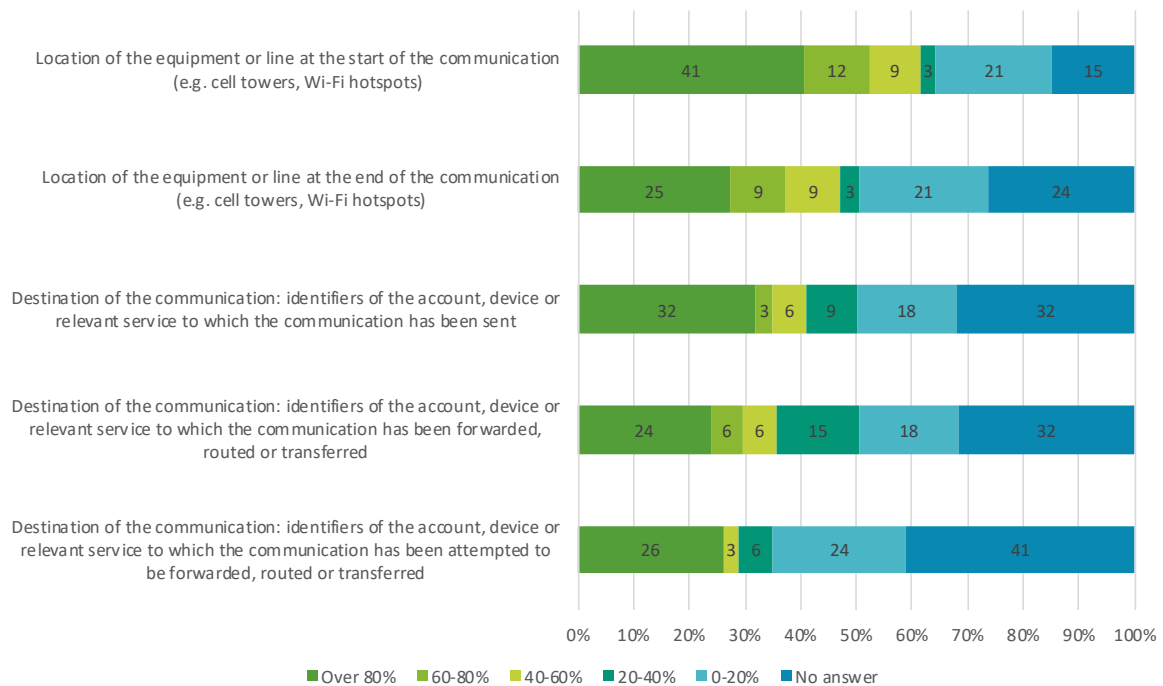
Identification data – frequency of use



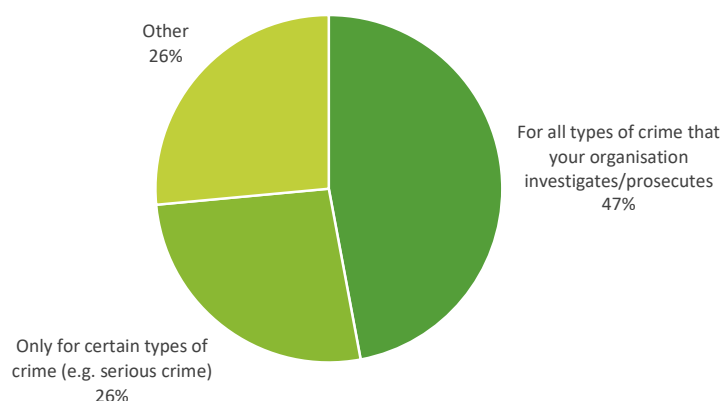
Traffic data – frequency of use



Location data and data on the destination of a communication – frequency of use

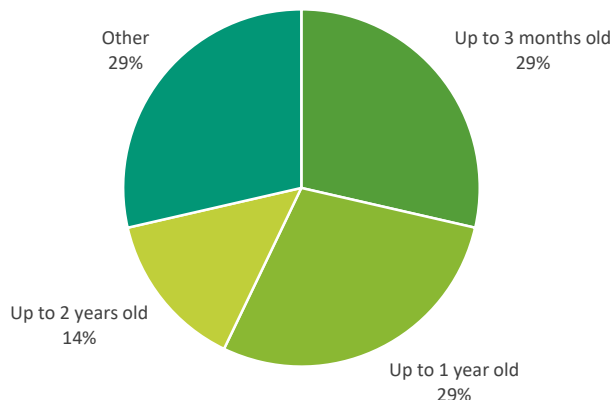


Q.23 - For what types of crimes do you usually request non-content data from the electronic communication service providers? (N=34)



Six respondents answered 'Other': for four of these respondents the question is not applicable. Two German and one Italian respondent specified that non-content is only requested for serious crimes (not minor offences). A Slovene respondent stated that non-content data is only requested for crimes listed within the legislation.

Q.24 - What is the average 'age' of the requested non-content data counting backwards from the time the relevant communication (e.g. phone call, message, internet access) took place? Respondents who answered only for certain types of crime in question 16 (N=7)



Respondents who answered 'Other' specified that the average age of the data requested depends on when the crime becomes known and proceedings are launched.

Q.25 - Could you provide an estimation of the proportion of requests for non-content data of a different 'age' - counting backwards from the time the relevant communication (e.g. phone call, message, internet access) took place - in the last two (2) years (2018 and 2019) per type of crime? If data for 2019 are not yet available, please provide data for the years 2017 and 2018. By type of crime:

Organised crime

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
France		40-60%			More than 80%		
France	0-20%	0-20%	0-20%	20-40%	60-80%		
Germany	More than 80%	0-20%	0-20%	0-20%	0-20%	0-20%	0-20%
Germany	More than 80%	40-60%	0-20%	0-20%	0-20%	0-20%	0-20%
Portugal	0-20%	0-20%	0-20%	20-40%	40-60%	20-40%	0-20%
Portugal	0-20%	0-20%	0-20%	0-20%	0-20%	0-20%	0-20%
Slovenia				0-20%	0-20%	0-20%	0-20%

Human trafficking

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
France	0-20%				More than 80%		

Child sexual exploitation and child pornography

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
France			0-20%	20-40%	60-80%		
France				0-20%	40-60%	20-40%	
France	More than 80%	More than 80%	More than 80%	More than 80%	More than 80%		
Portugal	0-20%	20-40%	More than 80%	More than 80%	60-80%	0-20%	0-20%
Portugal	0-20%	0-20%	20-40%	20-40%	40-60%		

Drug trafficking

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
France		40-60%	60-80%	60-80%	More than 80%		
Slovenia				0-20%	0-20%	0-20%	0-20%

Trafficking of weapons

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
France	0-20%	0-20%	0-20%	20-40%	40-60%		

Corruption

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
Italy	0-20%	40-60%	20-40%	40-60%	20-40%	40-60%	0-20%
Portugal	0-20%	0-20%	0-20%	20-40%	20-40%	20-40%	0-20%
Portugal			0-20%	0-20%	0-20%	0-20%	

Fraud

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
France		20-40%		40-60%	60-80%		
France				0-20%	40-60%	0-20%	
Italy	0-20%	0-20%	0-20%	20-40%	0-20%	0-20%	40-60%
Portugal	0-20%	60-80%	More than 80%	More than 80%	0-20%	0-20%	0-20%

Money laundering

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
Portugal	0-20%	0-20%	0-20%	40-60%	60-80%	60-80%	60-80%
Portugal		0-20%	0-20%	0-20%	0-20%		

Cybercrime

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
France		20-40%		60-80%	20-40%		
France				0-20%	40-60%	20-40%	
France	More than 80%	More than 80%	More than 80%	More than 80%	More than 80%		
Portugal	0-20%	60-80%	More than 80%	More than 80%	0-20%	0-20%	0-20%
Slovenia	0-20%	0-20%	20-40%	20-40%	0-20%	0-20%	

Organised and armed robbery

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
Germany	More than 80%	0-20%	0-20%	0-20%	0-20%	0-20%	0-20%
Germany	40-60%	40-60%	20-40%	0-20%	0-20%	0-20%	0-20%

Rape

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
France	More than 80%	More than 80%	More than 80%	More than 80%	More than 80%		

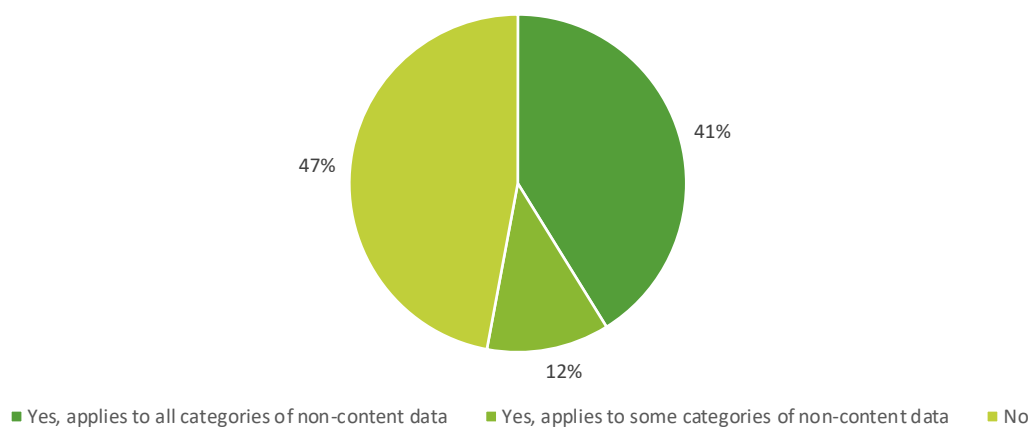
Trafficking in stolen vehicles

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
Germany	More than 80%	0-20%	0-20%	0-20%	0-20%	0-20%	0-20%

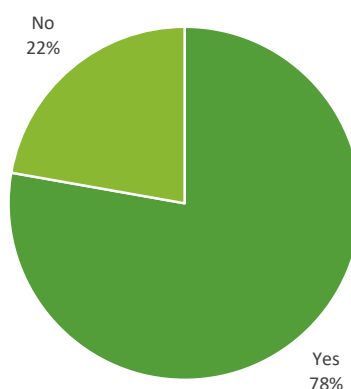
Theft

Member State	Less than 1 week old	Less than 1 month old	Up to 3 months old	Up to 6 months old	Up to 1 year old	Up to 2 years old	More than 2 years old
Germany	0-20%	0-20%	0-20%	0-20%	0-20%	0-20%	0-20%
Slovenia				0-20%	0-20%	0-20%	0-20%

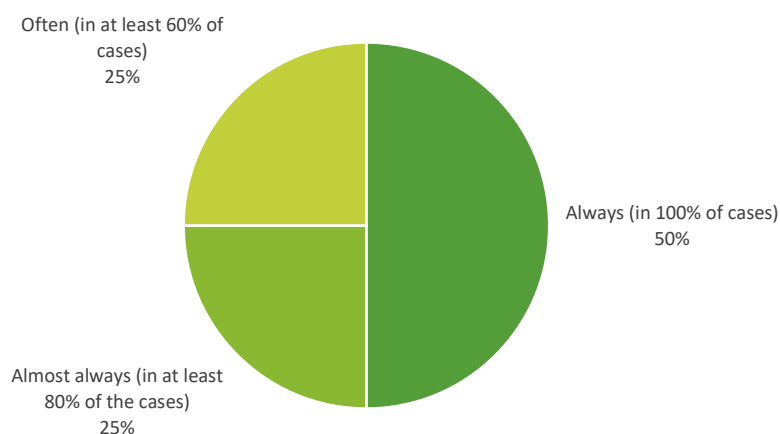
Q.26 - Does the procedure for requesting access to non-content data provide for a usage of a Single Points of Contact (SPOCs) for the law enforcement authorities? (N=34)



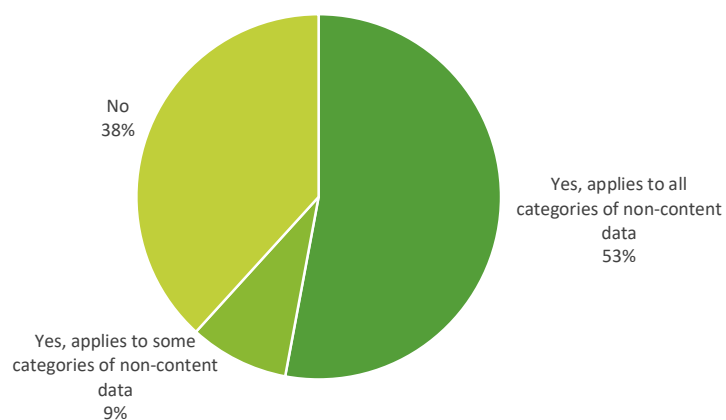
Q.27 – If yes in Q.26, is the usage of the SPOC obligatory for the law enforcement authorities? (N=18)



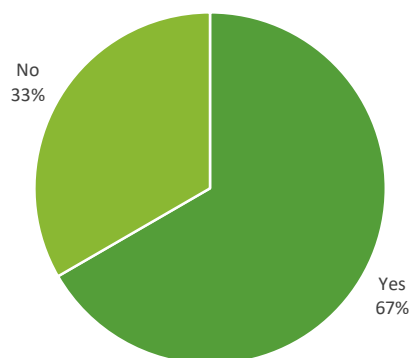
Q.28 – On average, how frequently do you make use of the SPOCs to request non-content data? (N=4)



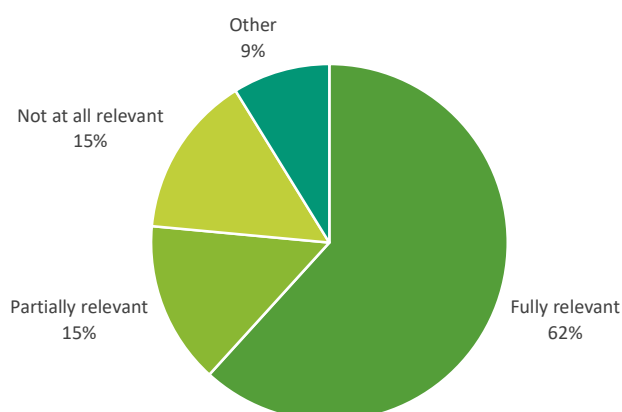
Q.29 - Does the procedure for requesting access to non-content data provide for a usage of a Single Points of Contact (SPOCs) for the electronic communication service providers? (N=34)



Q.30 - If yes in Q.29, is the usage of the SPOC obligatory for the electronic communication service providers? (N=21)

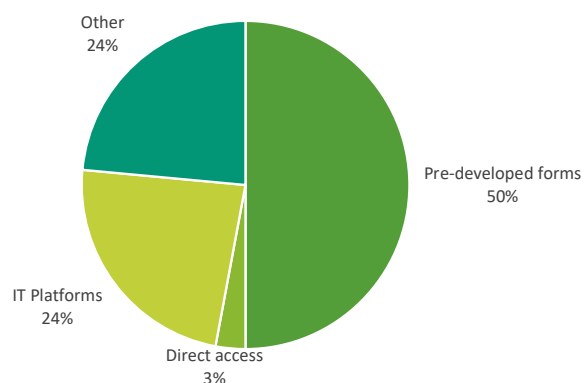


Q.31 - How would you describe the relevance of the use of SPOCs as a tool to access non-content data? (N=34)



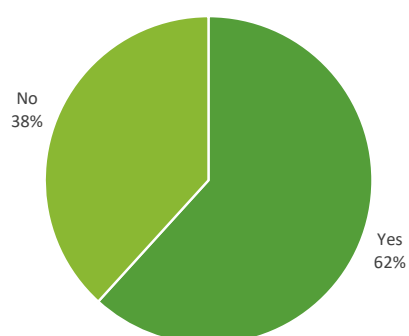
Those respondents who answered 'Other' specified either that the question is not applicable.

Q.32 - What are other practical arrangements/tools in place between the law enforcement authorities and the electronic communication service provider to access non-content data? (N=34)

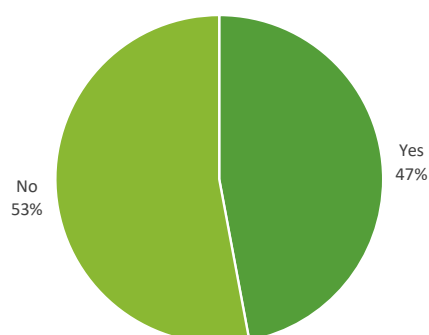


Those respondents who answered 'Other' specified either that the question is not applicable or that other practical arrangements apply including: procedure through Public Prosecutors (EE); encrypted emails (IE); one-stop-shop interface (FR).

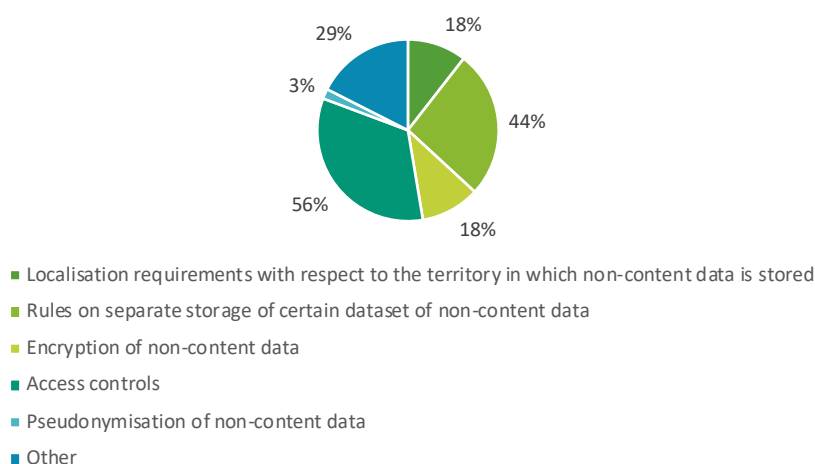
Q.33 - Does your organisation have an internal procedure in place for requesting non-content data? (N=34)



Q.34 - Does your organisation have an internal procedure in place for accessing non-content data received from the electronic communication service providers? (N=34)

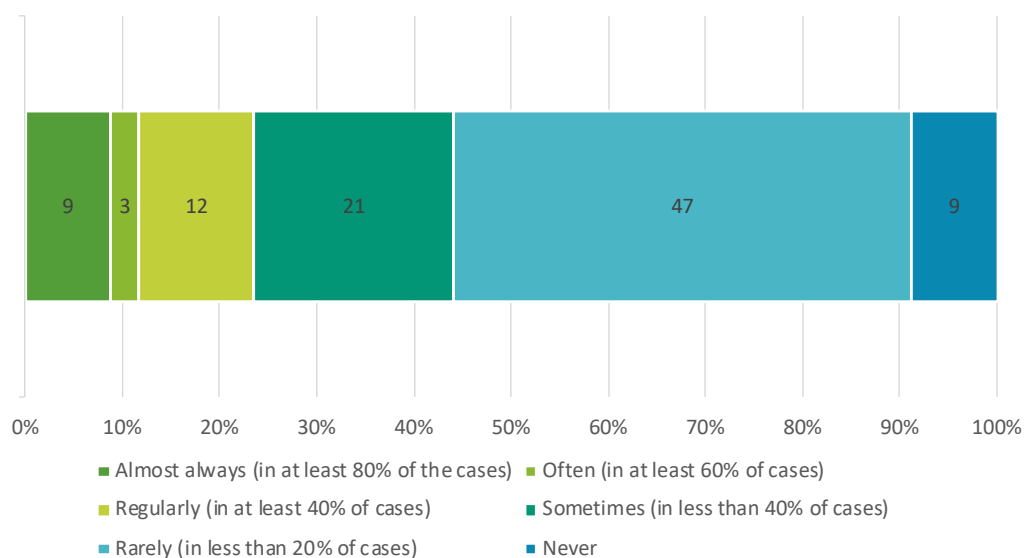


Q.35 - What kind of security requirements does the national framework require when it comes to retention of non-content data for law enforcement purposes? (Multiple answers are possible). (N=34)

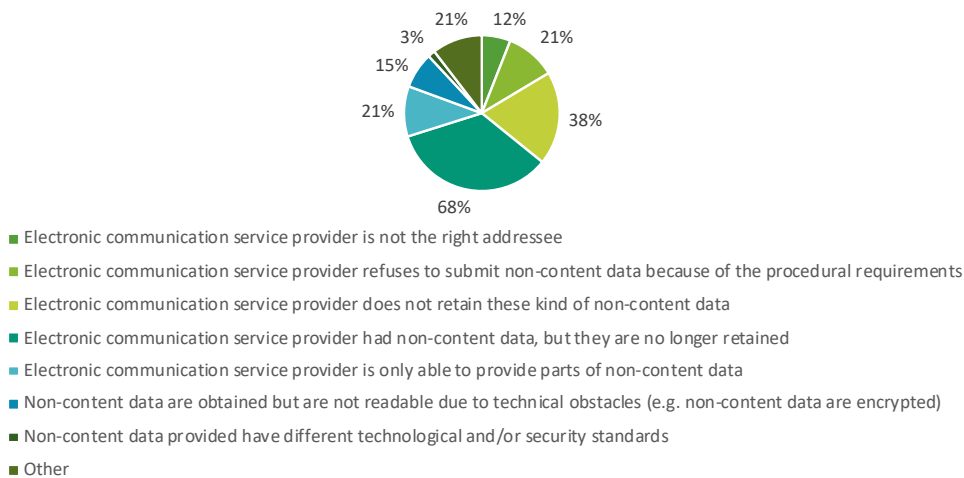


Those respondents who answered 'Other' specified that security requirements also include the deletion of data after retention period expires; storage on a secure police server; confidentiality of requests; proof of receipt.

Q.36 - On average, how often is your request for non-content data unsuccessful? (An unsuccessful request is a request where you were unable to obtain any non-content data requested or where you were able to obtain only a limited amount of non-content data that did not suffice to progress with investigation/prosecution in the case in question). (N=34)

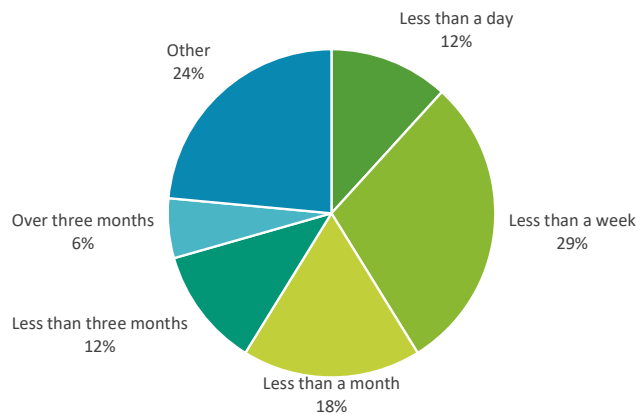


Q.37 - What are the most frequent reasons for NOT being able to access part of or the entire dataset of non-content data from the electronic communication service provider? Please select maximum three (3) reasons, which in your experience are the most frequent. (N=34)

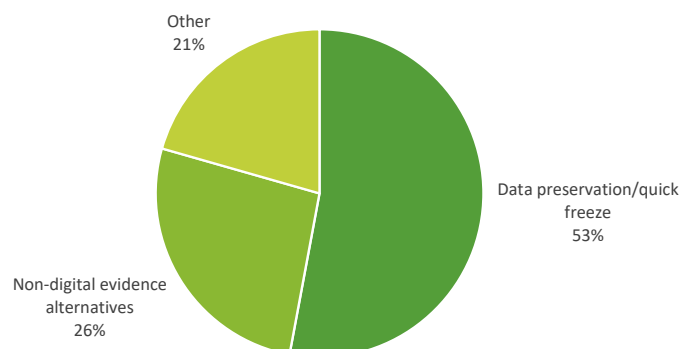


Those respondents who answered 'Other' specified either that the question is not applicable or that the electronic communication service provider is based in a foreign country, the provider never responds/forgets to process request.

Q.38 - How long does it take for your organisation on average to obtain non-content data requested? (N=34)

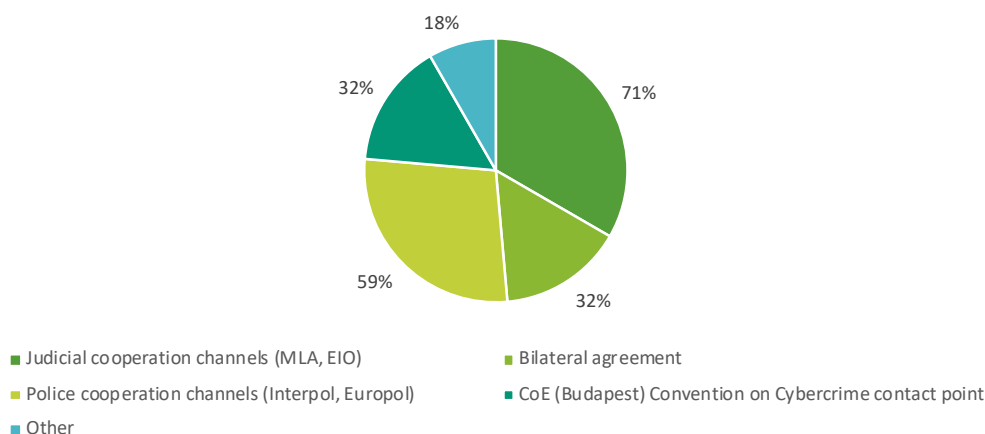


Those respondents who answered 'Other' specified either that the question is not applicable or that it depends on a variety of factors including: the type of information requested, the platform used and the urgency of the request. In France, for example, requests sent through the automated platform are processed in less than one week, manual requests on the other hand are processed within 15 days to three months.

Q.40 - What other alternatives to requesting non-content data are available? (N=34)

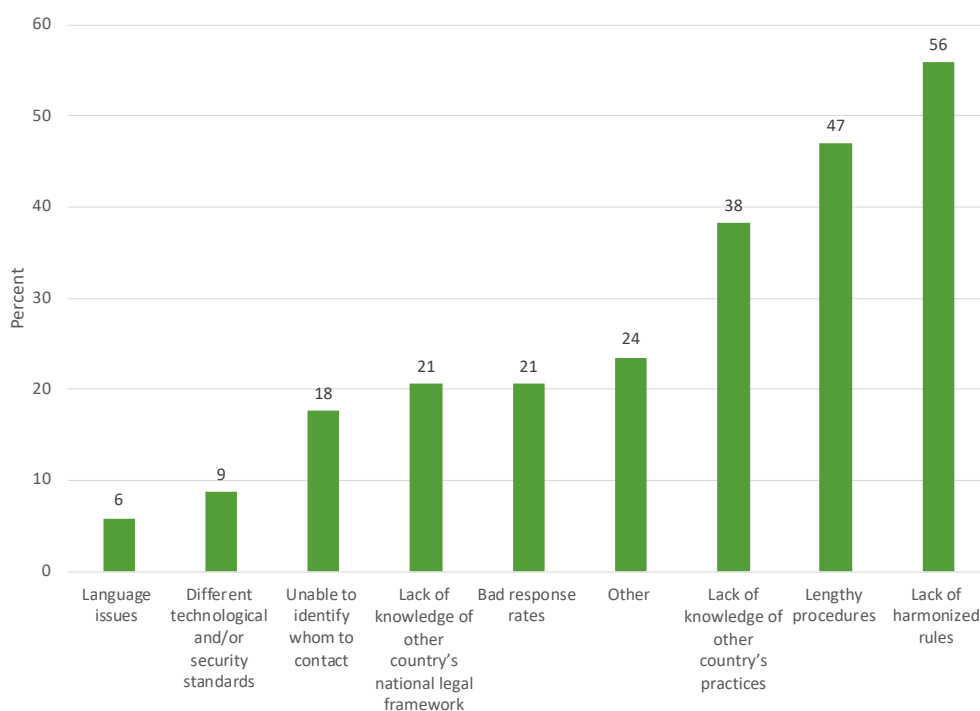
Those respondents who answered 'Other' specified either that the question is not applicable or that there are no alternatives to requesting non-content data.

Q.43 - Which legal procedures do you use and to what kind of legal instruments do you resort to in order to obtain non-content data from electronic communication service providers in other Member States? Please select up to three answers, which in your opinion are the most relevant. (N=34)



Those respondents who answered 'Other' specified either that the question was not applicable or added the following channels: Common centres / departments, Naples II convention on mutual assistance and cooperation between customs administrations and multilateral agreements (ESMA – European Securities and Markets Authority and IOSCO – International Organisation of Securities Commission).

Q.44 - What are the main challenges in accessing non-content data in case of cross-border criminal cases from electronic communication service providers from other Member States? Please select up to three (3) answers, which in your opinion are the most relevant.

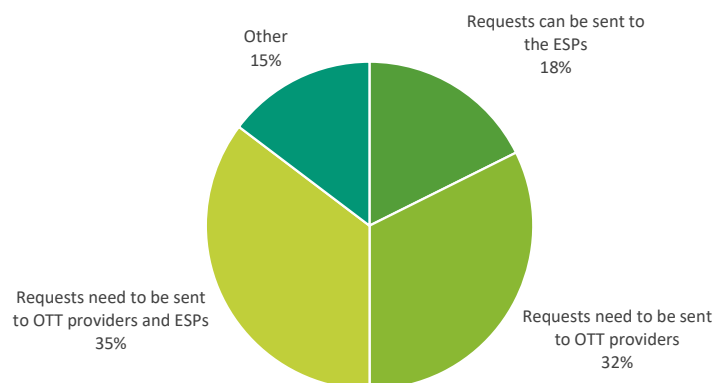


Those respondents who answered 'Other' specified either that the question is not applicable, or that they do not encounter issues, one respondent stated that the data retention periods are too short in other Member States.

Technological challenges

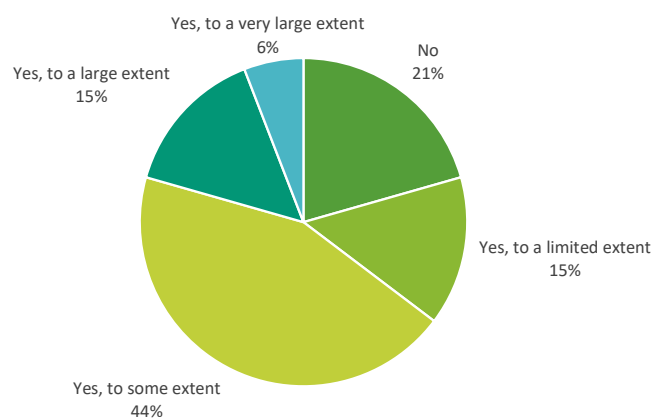
This section seeks to understand the impact of new technological developments on the access to non-content data for law enforcement purposes. A particular focus is on the impact (if any) of end-to-end encryption. Certain 'Over-the-Top' communication service providers, such as WhatsApp or Telegram, subject all messages, phone calls, videos and any other form of information exchanged on their platforms to end-to-end encryption. This means that the communication is encrypted directly by the sender's device and can only be decrypted by the receiver's device. The electronic communication service providers involved in the transmission of the communication do not possess the cryptographic keys necessary to decrypt the communication. Although only the content of the communication is encrypted, this section seeks to understand whether additional challenges arise for law enforcement authorities when accessing the non-content data generated by these new types of communications subject to end-to-end encryption (e.g. uncertainties as to whom to address non-content data access requests, partial encryption of the non-content data, etc.).

Q.45 - What is the procedure to request access to non-content data generated by communications subject to end-to-end encryption? (N=34)

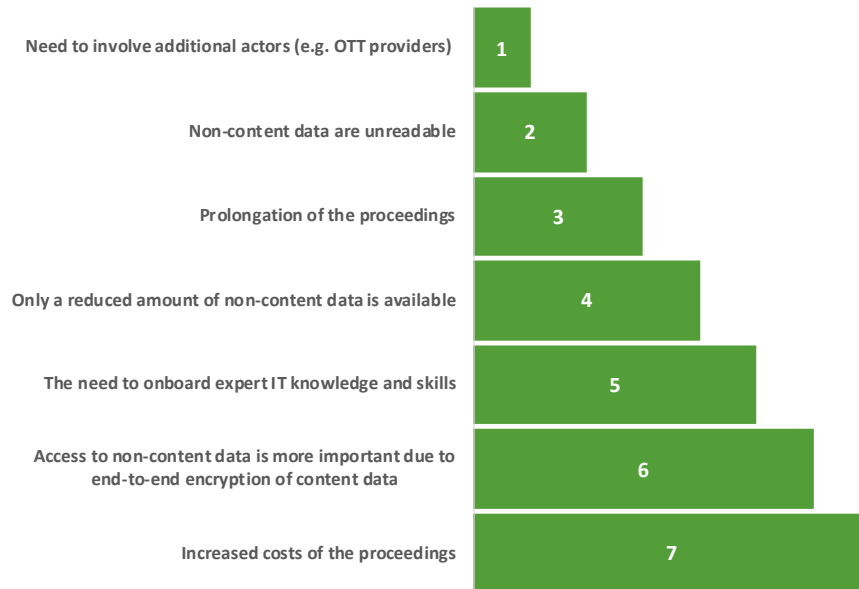


Those respondents who answered 'Other' specified either that the question is not applicable or that there is no procedure because encrypted data cannot be accessed. One respondent stated that currently it is only possible by evaluating the end device.

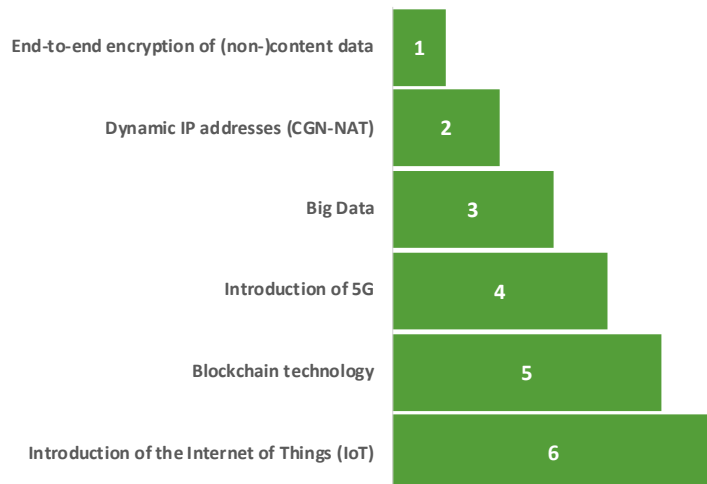
Q.46 - Has the number of requests for accessing encrypted non-content data increased in the last couple of years? (N=34)



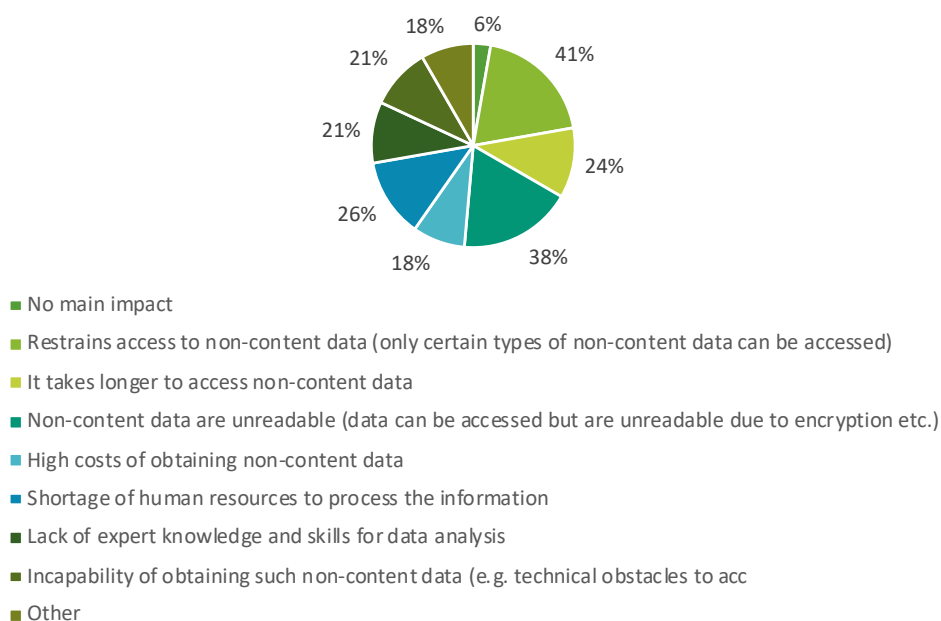
Q.47 - What type of impact does the end-to-end encryption of data have on the access to non-content data? Please rank the top three answers, which in your opinion are the most relevant. (N=34)



Q.48 - What are the biggest technological challenges in accessing non-content data in the investigation and/or prosecution of criminal cases? (Please rank the three most important challenges in your opinion) (N=34)



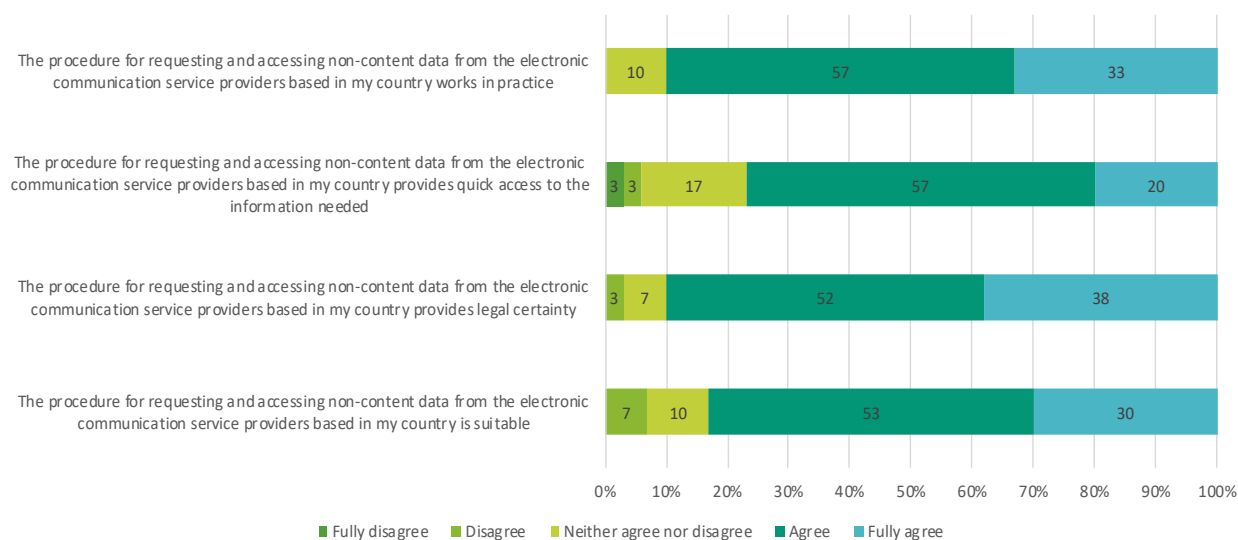
Q.49 - In your opinion, what is the likely impact of new technological trends (such as 5G and IoT) on access to non-content data? Please select up to three answers, which in your opinion are the most relevant. (N=34)



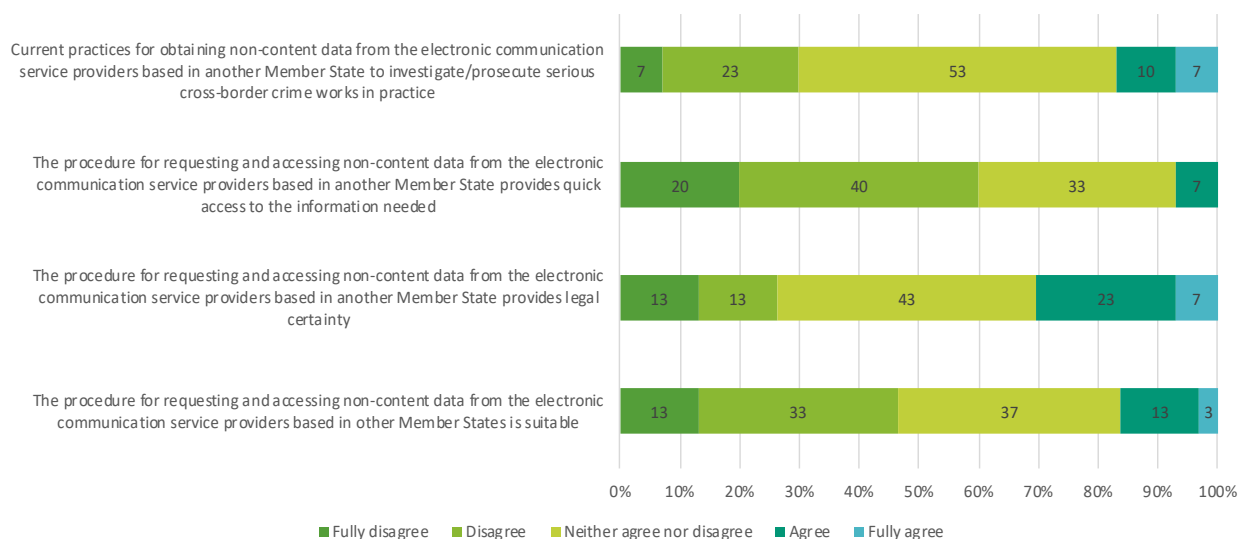
Main issues/obstacles of the current system to access non-content data

While the study does not aim to assess the functioning of the current system for retention of and access to non-content data in the Member States, it is important to understand the opinions of its users. The following section presented a set of statements about the functioning of the procedure of requesting and accessing non-content data from electronic communication service providers nationally and cross-border. Respondents were asked to state to what extent they agree with those statements, on a scale from 1 (fully disagree) to 5 (fully agree).

Q.51 - National system for accessing non-content data: to what extent do you agree with the following statements? (N=34)



Q.52 - Cross-border access to non-content data (within the EU): to what extent do you agree with the following statements? (N=34)



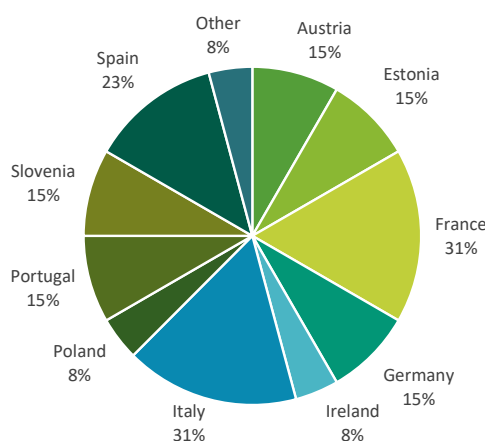
ANNEX V: RESULTS OF THE SURVEY TO ELETRONIC COMMUNICATION SERVICE PROVIDERS (ESPS)

Annex V presents the aggregated results for all closed survey questions addressed to ESPs, processed on aggregated level and anonymised. The total number of respondents is 13. Only the graphs for closed questions are presented in Annex V. Answers to open-ended questions were taken into account in the overall analysis in the body of the text.

Profiling questions

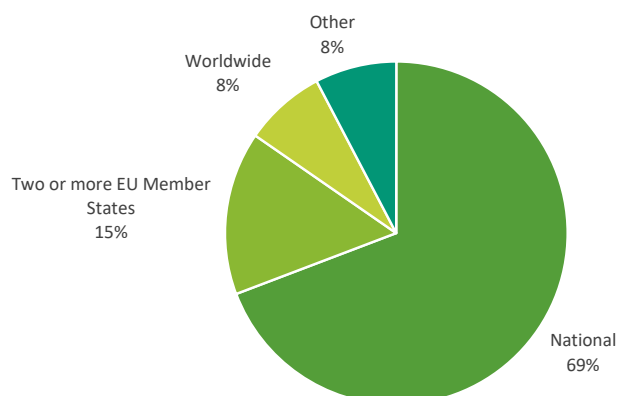
The first section of the survey asked respondents questions about their profile – e.g. country, size, services provided etc.

Q.1 - In which country are you based? (Multiple answers possible, in case of cross-border activities.) (N=13)

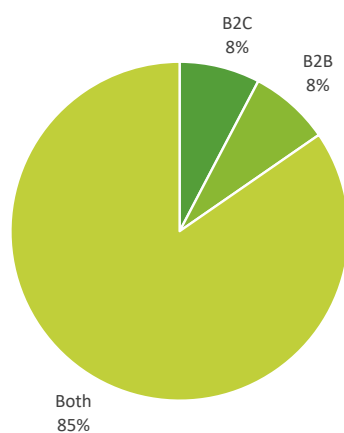


Respondents who answered 'Other' specified worldwide.

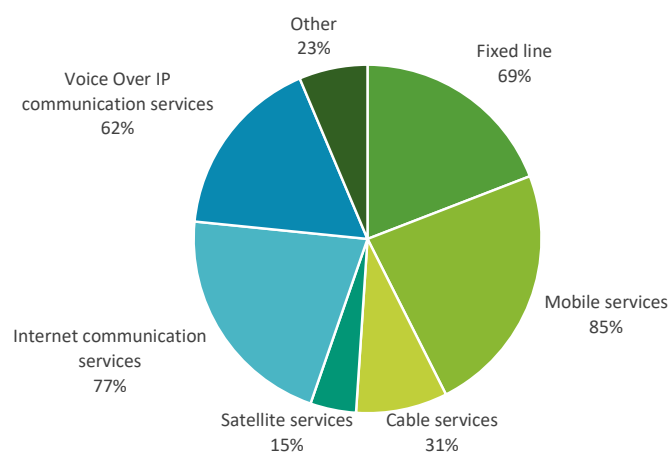
Q.3 - What is the territorial scope of your company's activities? (N=13)



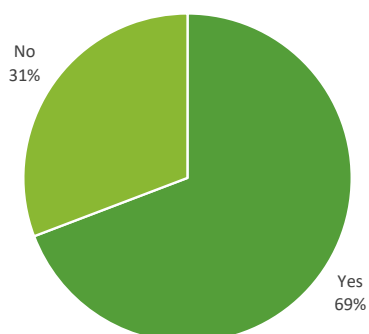
Q.5 - What is your company's business model? (N=13)



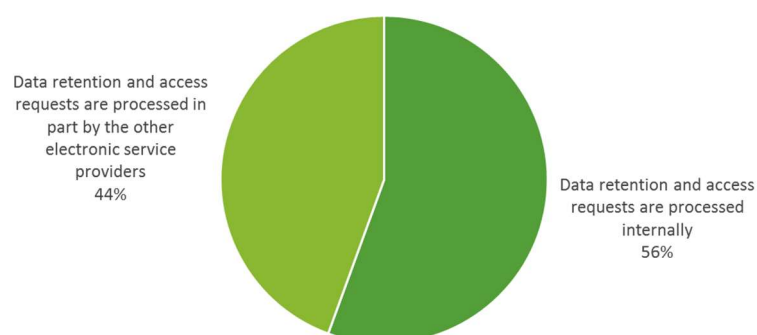
Q.6 - Which types of electronic communication services does your organisation provide? (N=13)



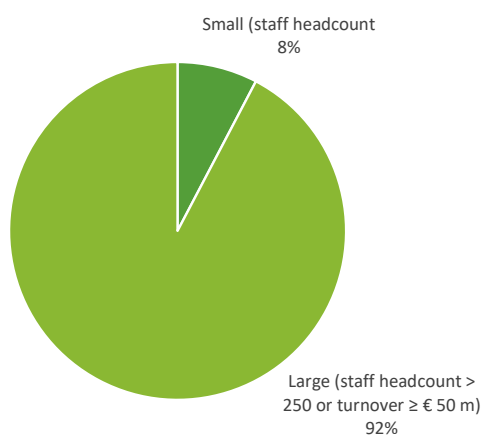
Q.7 - Are any of these electronic communication services provided through the resources (i.e. network) of another electronic communication service provider? (N=13)



Q.8 - Who controls the data retention and processes the access requests to non-content data for law enforcement purposes linked to these services? (N=13)



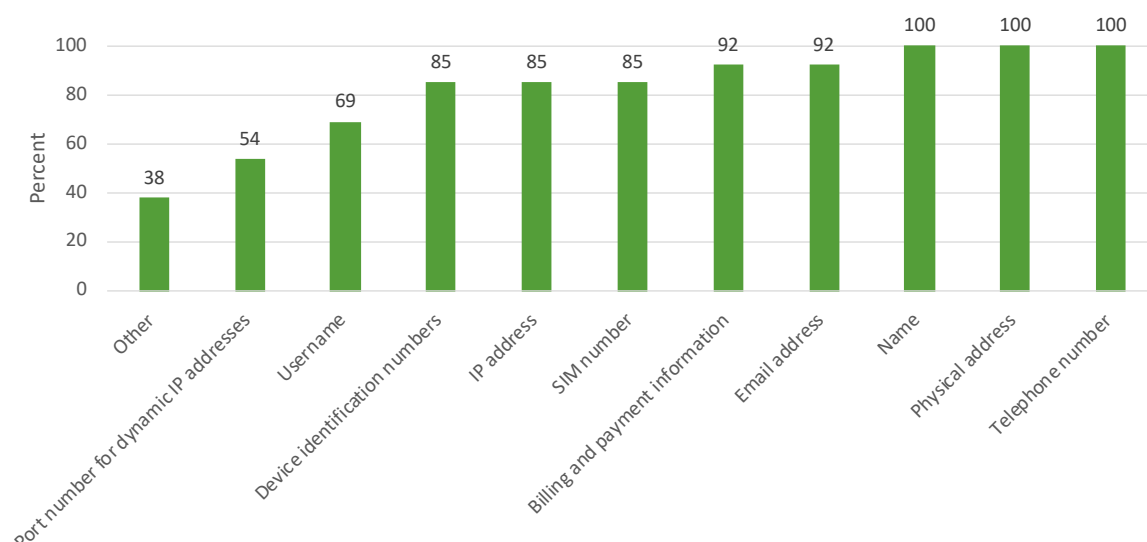
Q.9 - What is the size of your organisation? (N=13)



National practices of retaining electronic communications non-content data (metadata) by electronic communication service providers

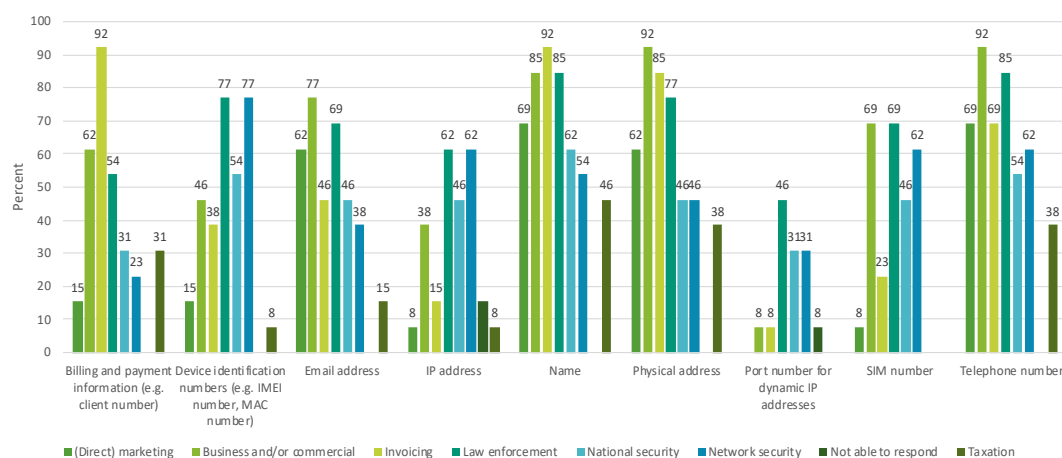
This section focuses on the types of retained non-content data, their purposes and the retention periods.

Q.11 - What type of subscriber non-content data (service-associated information) does your organisation retain? (Please select all applicable answers.) (N=13)

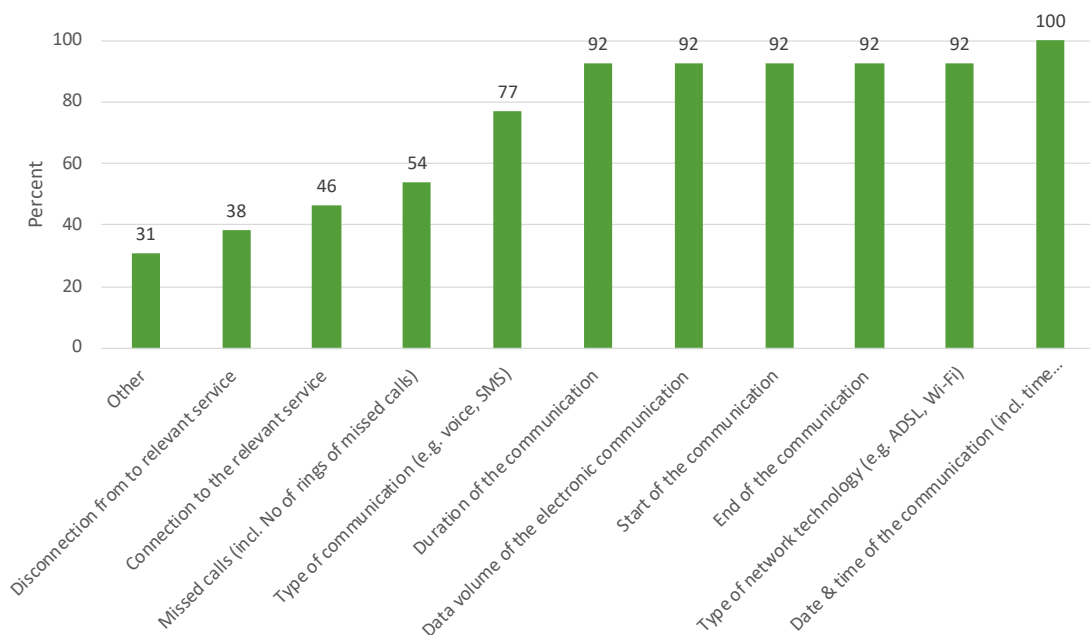


'Other' includes: ID number, date of birth, nationality, tax number. Note: Some respondents did not respond in this question that they retain IP addresses, device identification numbers and port numbers for dynamic IP addresses but specified in question 12 that they retain these data points as traffic data.

Q.12 - Please specify in the table below what are the purposes for which you retain the above listed subscriber data (including but not limited to IP address, port number for dynamic IP addresses, device identification numbers)? (N=13)

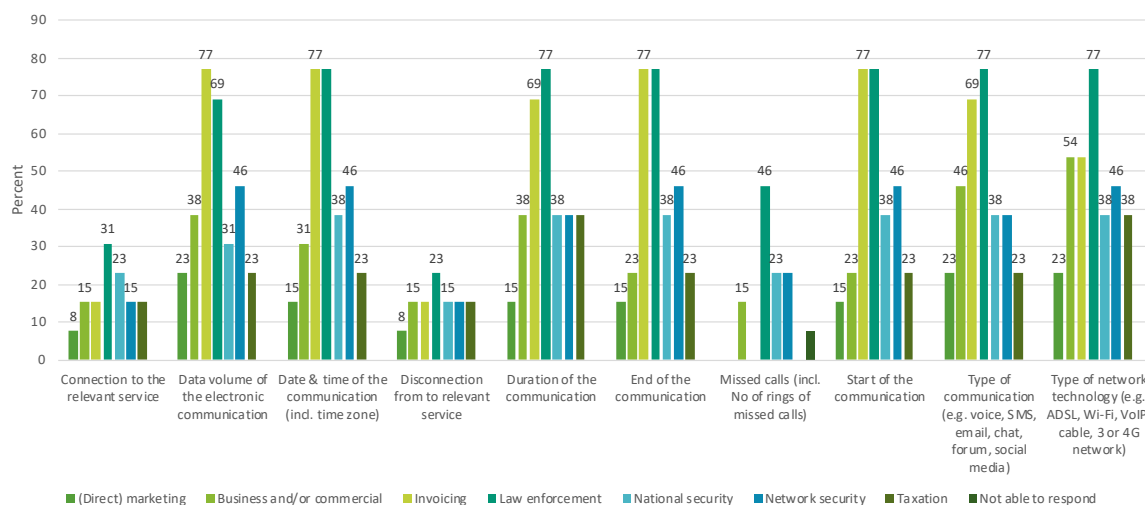


Q.13 - What type of traffic non-content data (communication-associated information) does your organisation retain? (Please select all applicable answers.) (N=13)



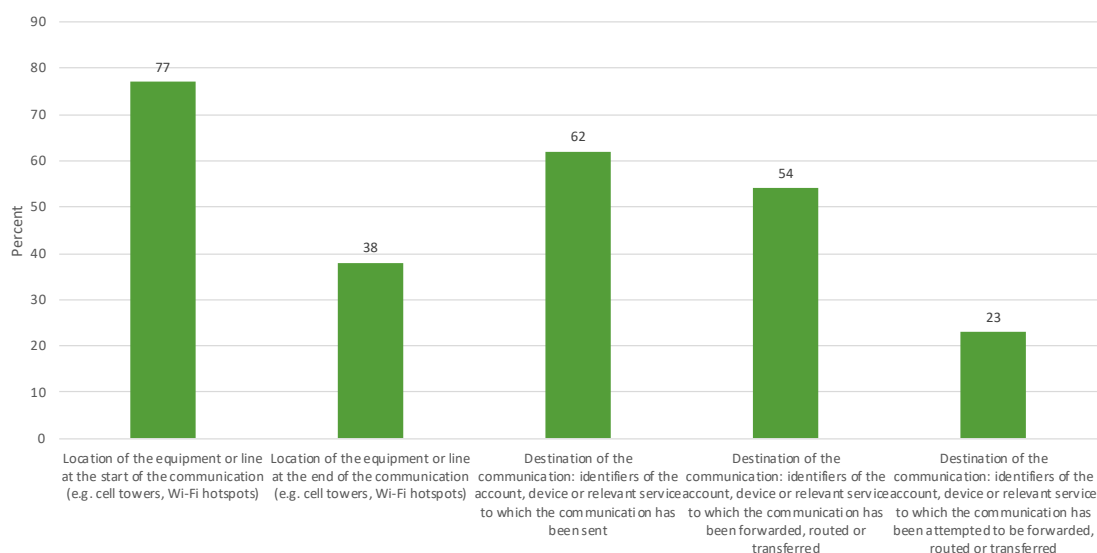
'Other' includes: IP address, port number for dynamic IP address and device identification numbers.

Q.14 - Please specify in the table below what are the purposes for which you retain the above listed traffic data. (N=13)

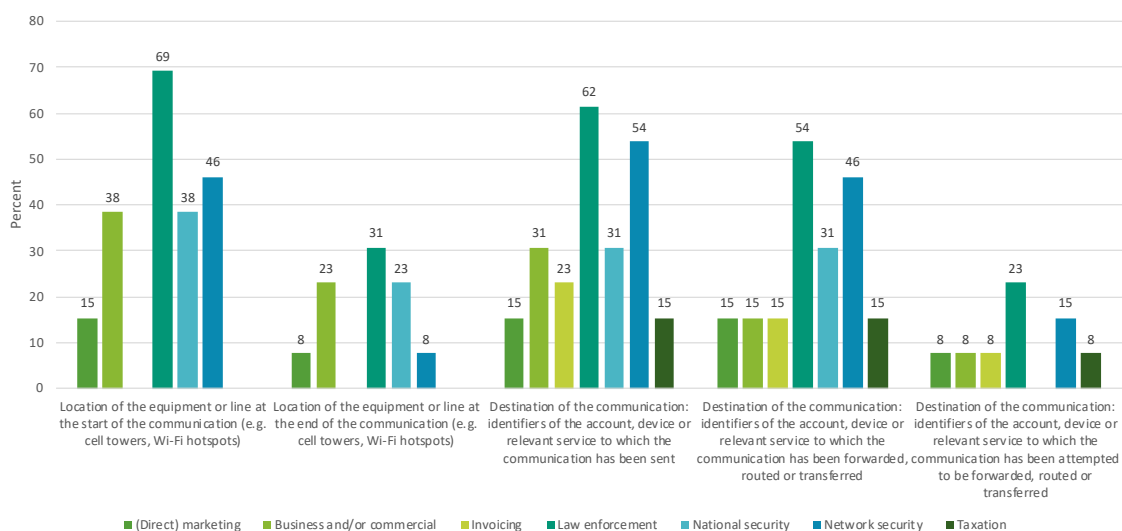


Q.15 and Q.17 - What type of location and other non-content data does your organisation retain? (Please select all applicable answers.) (N=13)

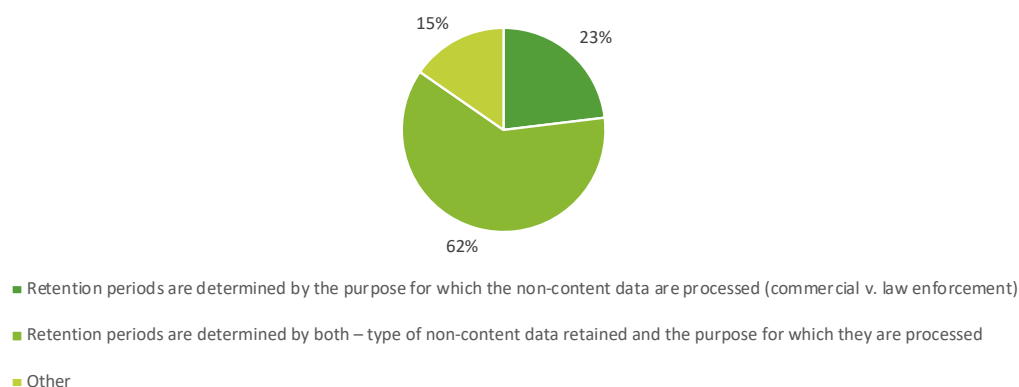
Data retention for law enforcement purposes – Final report



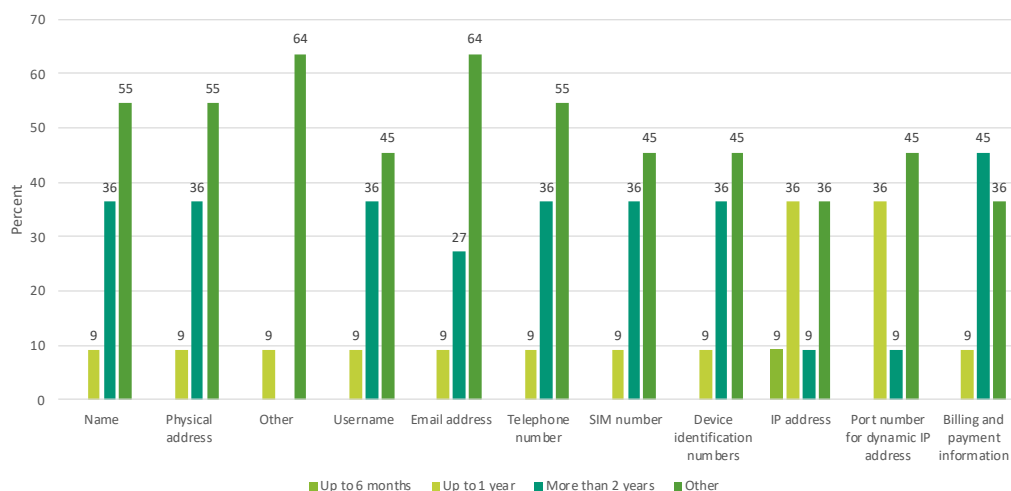
Q.16 and Q.18 - Please specify in the table below what are the purposes for which you retain the above listed location and other data. (N=13)



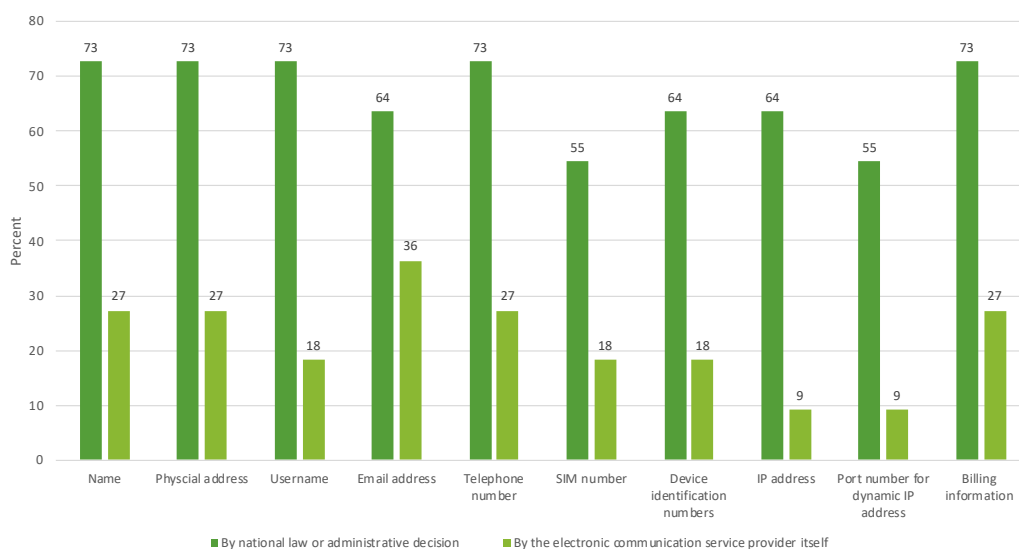
Q.19 - What determines the length of the retention periods of non-content data? (N=13)



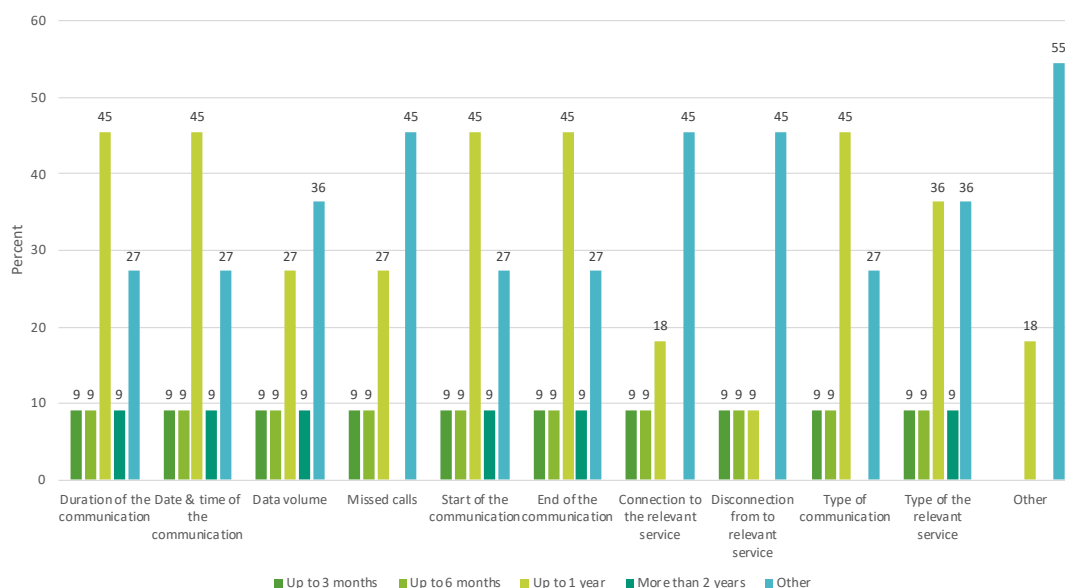
Q.20 - Please indicate in the table below the retention period for subscriber (service-associated information) non-content data and whether the retention periods have been set by law or not. (N=11)



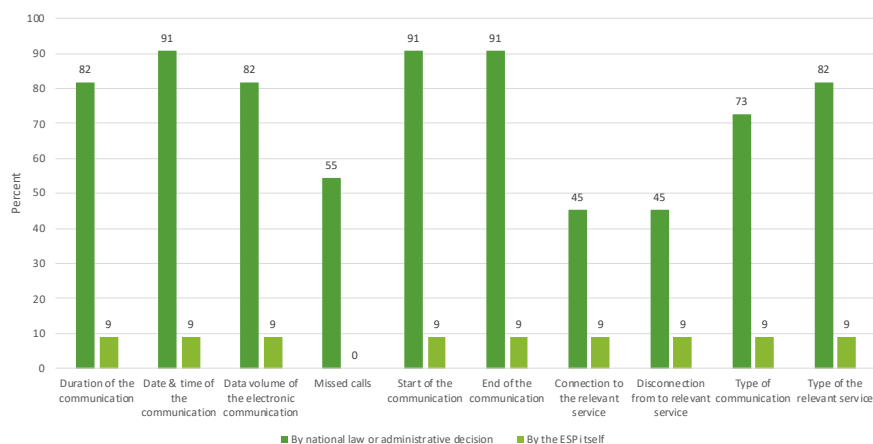
How retention periods are set



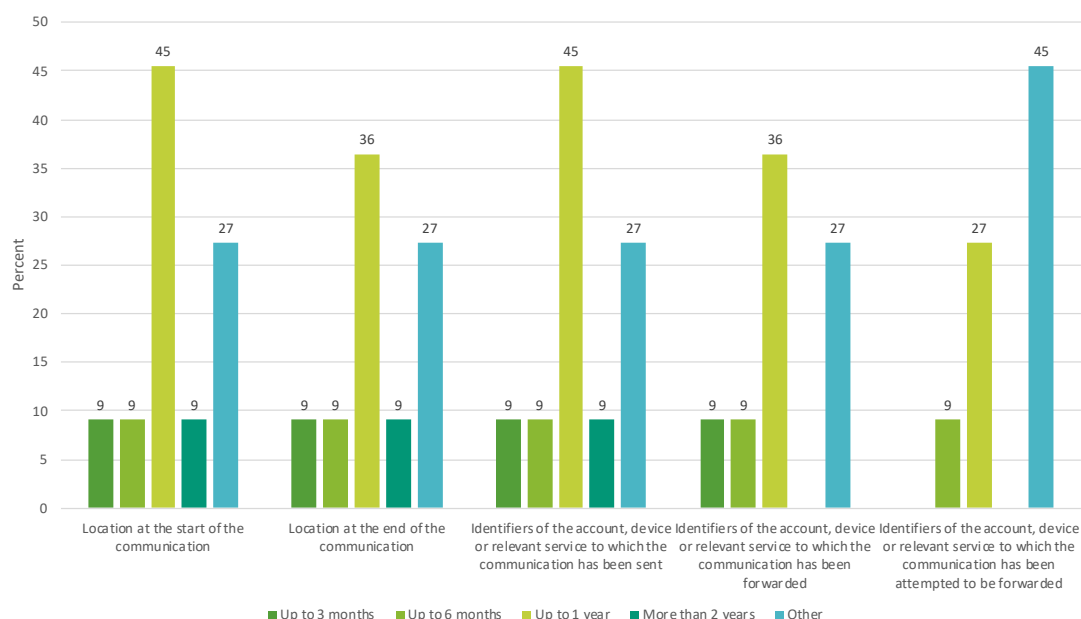
Q.21 - Please indicate in the table below the retention period for traffic non-content data and whether the retention periods have been set by law or not. (N=11)



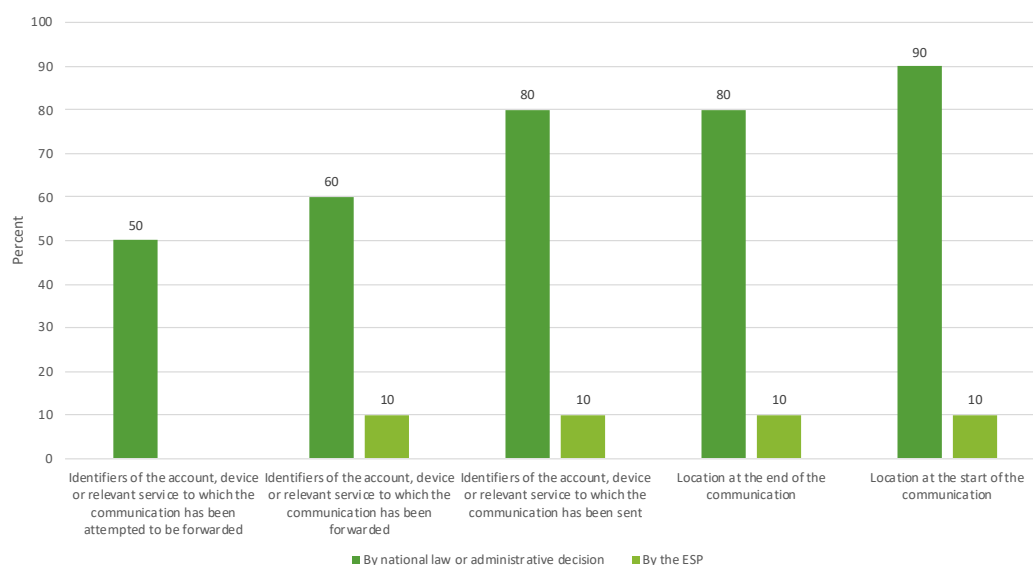
How retention periods are set



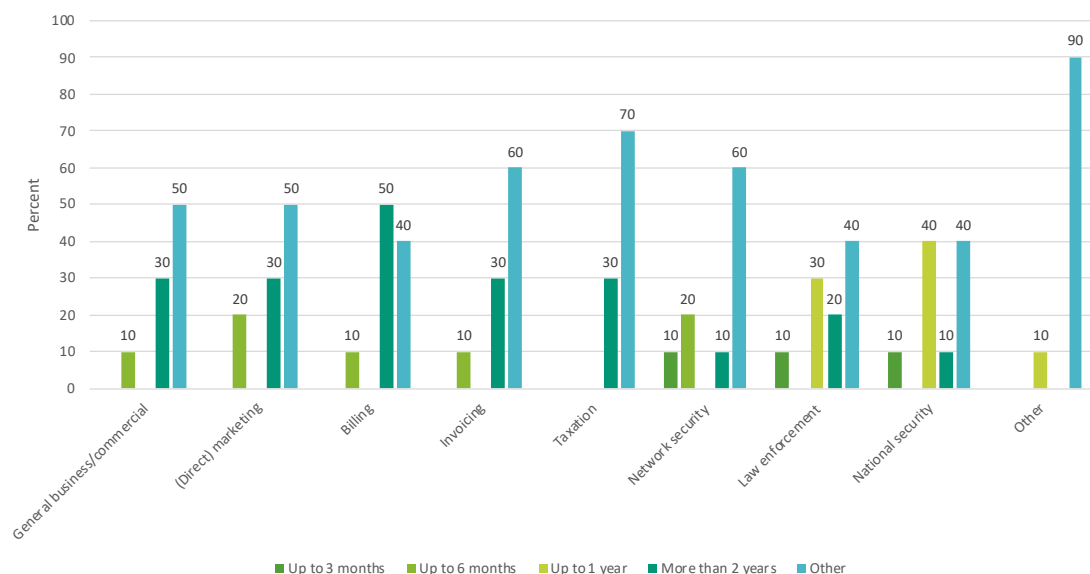
Q.22 and Q.23 - Please indicate in the table below the retention period for location and other non-content data and whether the retention periods have been set by law or not. (N=11)



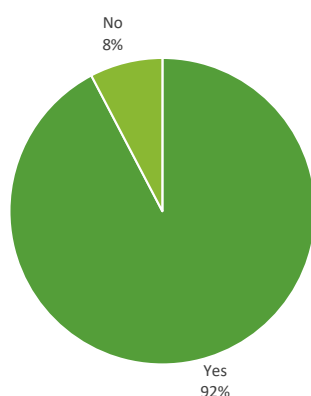
How retention periods are set



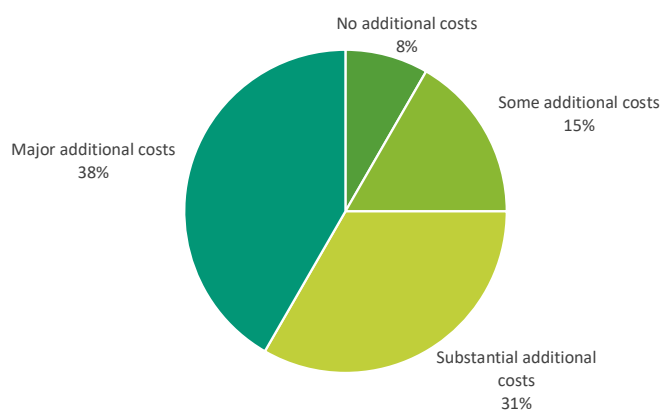
Q.24 - Please indicate in the table below the retention period for each specific purpose for which the non-content data are processed and whether this retention period has been set by law or not. (N=11)



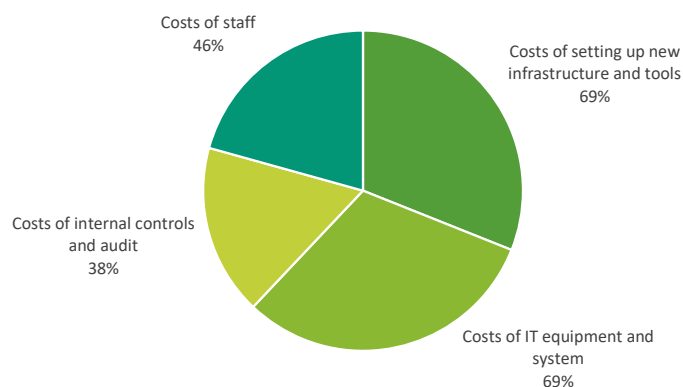
Q.25 - Does your company have the legal obligation to retain certain types of non-content data exclusively for law enforcement purposes? (Please consider only legislation currently in force) (N=13)



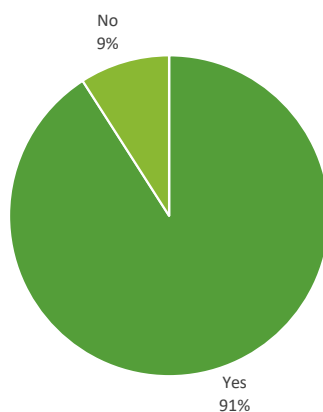
Q.26 - Has your business incurred any additional costs directly linked to the retention of non-content data for law enforcement purposes in the last few years (i.e. since the national legal framework has been put in place)? (N=13)



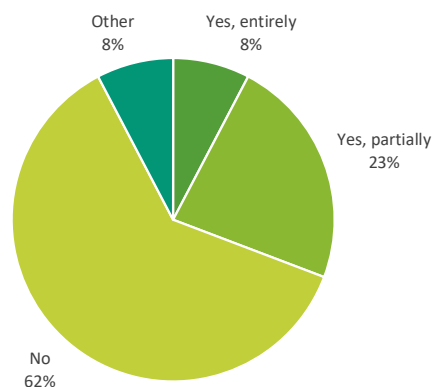
Q.27 - Please select the three (3) most relevant reasons for these additional costs. (N=11)



Q.28 - Are the additional costs incurred similar for your B2B activities? (N=11)



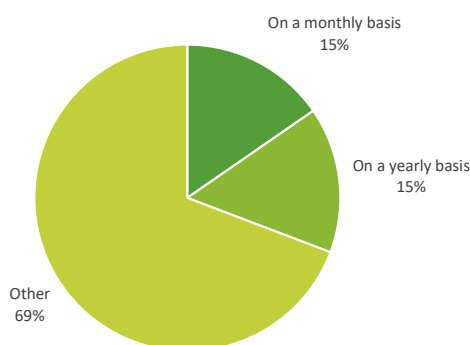
Q.30 - Do you receive reimbursement for these costs under the current legal national framework? (N=11)



National practices of requesting access to electronic communications non-content data (metadata) by the law enforcement authorities

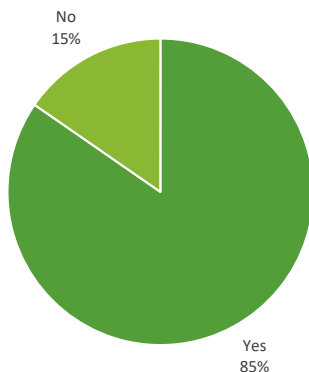
This section focuses on ESPs internal systems for responding to non-content data requests from LEAs.

Q.31 - How do you record requests to access non-content data? (N=13)

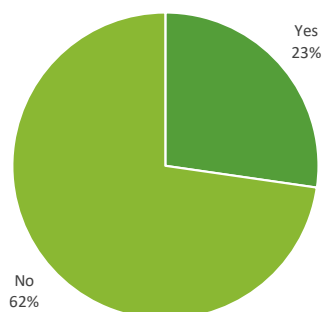


'Other' includes not applicable or on an ongoing basis – i.e. as soon as requests are received.

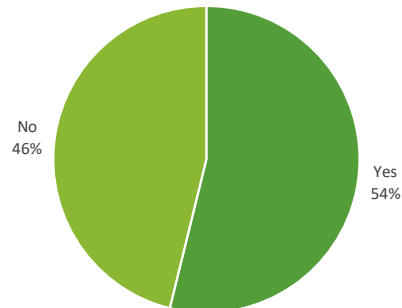
Q.32 - Do you hold any statistics on the number of requests for non-content data by law enforcement authorities? (N=13)



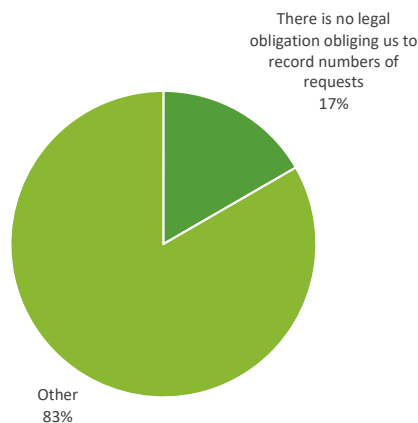
Q.33 - Do you publish any transparency or other types of reports on the number of requests to access non-content data or do you make data on the number of requests to access non-content data public? (N=13)



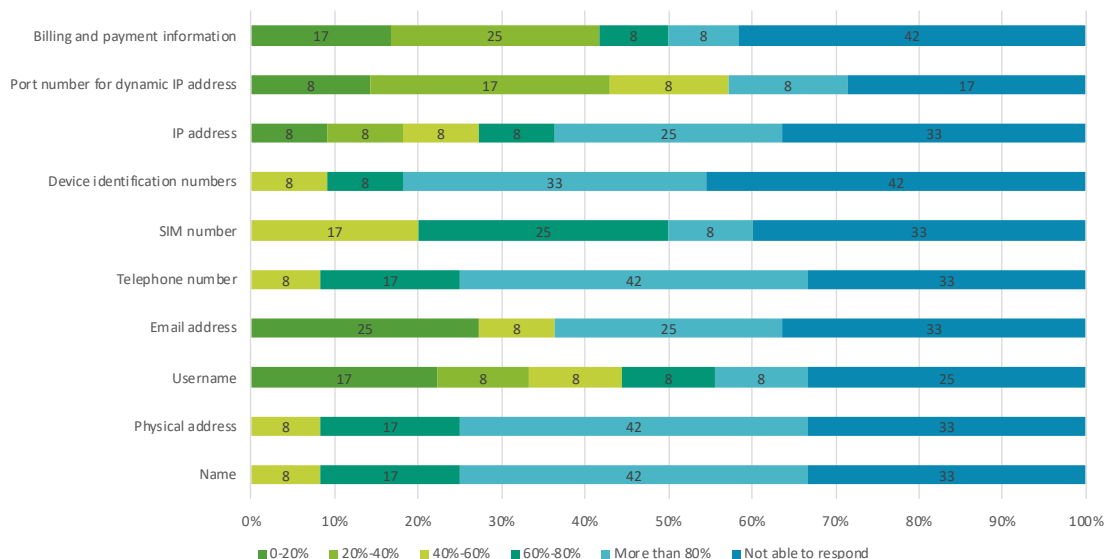
Q.35 - Could you please provide the number of requests for non-content data in the last two (2) years (2018 and 2019) by the national law enforcement authorities, in the table below. If data for 2019 are not yet available, please provide data for the years 2017 and 2018. (N=13)



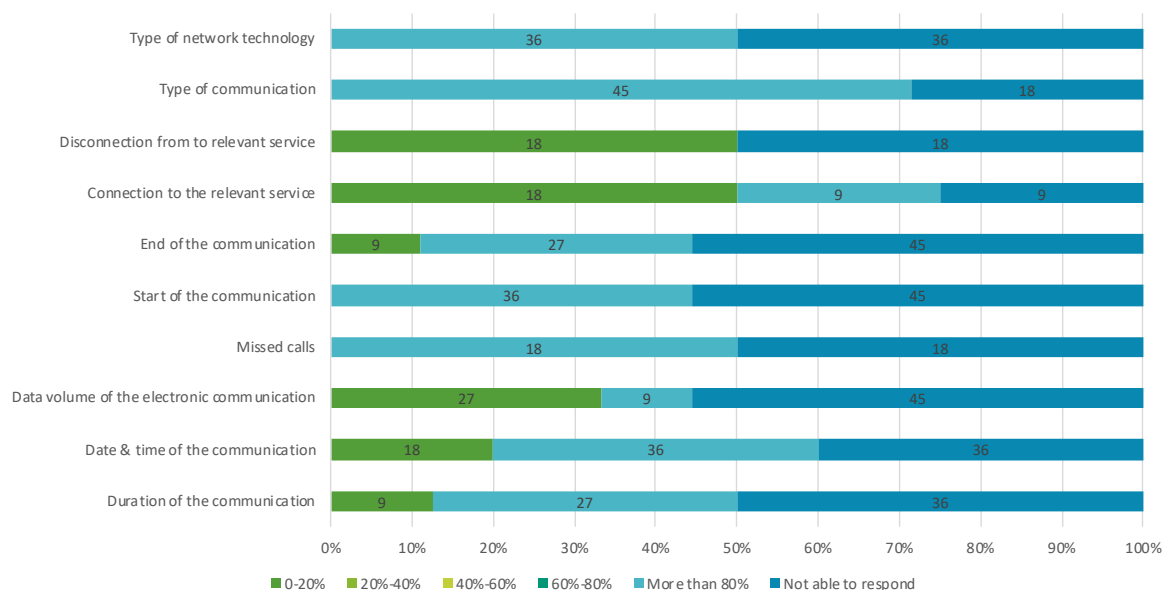
Q.36 – If no in Q.35, what is the reason that you cannot provide any estimation on the numbers of requests for non-content data? (N=6)



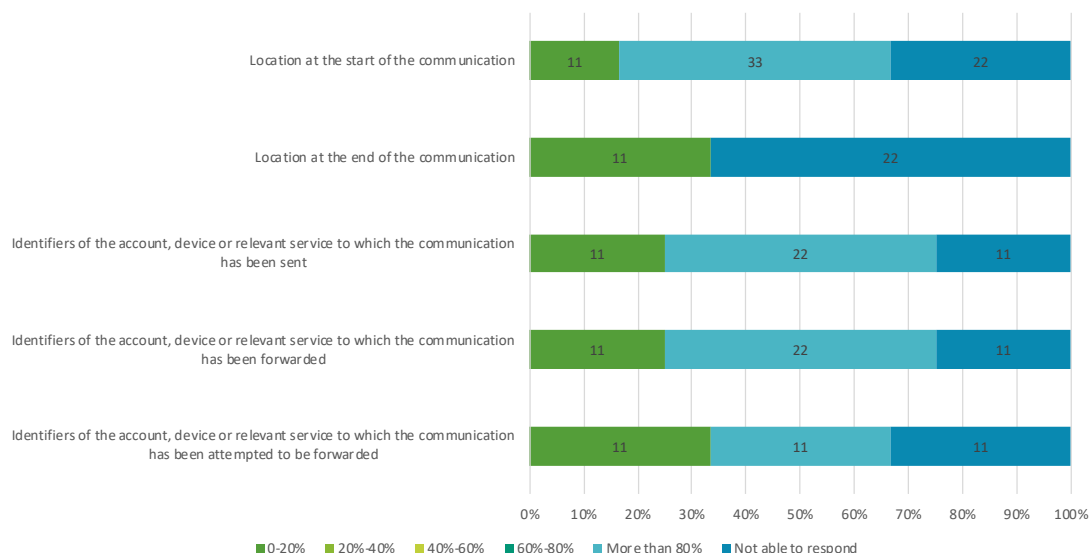
Q.37 - On average, which types of subscriber non-content data are most often requested by the law enforcement authorities. Please provide an estimation of the percentage of requests to access different types of subscriber non-content data during the course of one year (2018 or 2019). (N=12)



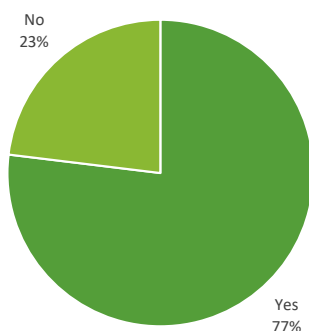
Q.38 - On average, which types of traffic non-content data are most often requested by the law enforcement authorities. Please provide an estimation of the percentage of requests to access different types of traffic non-content data during the course of one year (2018 or 2019). (N=11)



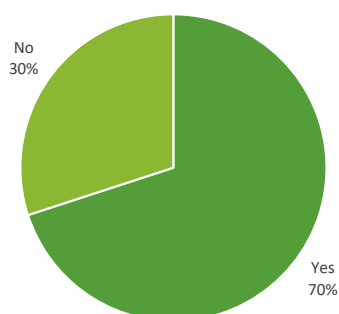
Q.39 and Q.40 - On average, which types of location and other non-content data are most often requested by the law enforcement authorities. Please provide an estimation of the percentage of requests to access different types of location non-content data during the course of one year (2018 or 2019). (N=9)



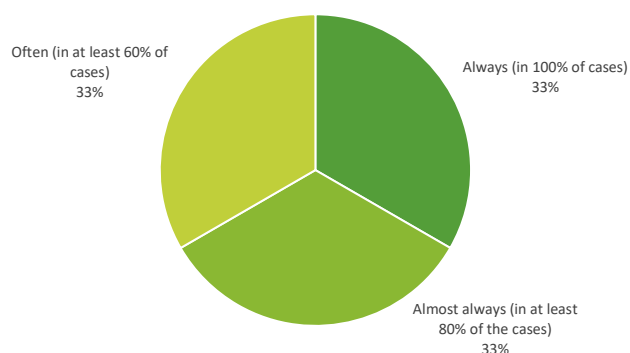
Q.41 - Does the procedure for requesting access to non-content data provide for a usage of a Single Points of Contact (SPOCs)? (N=13)



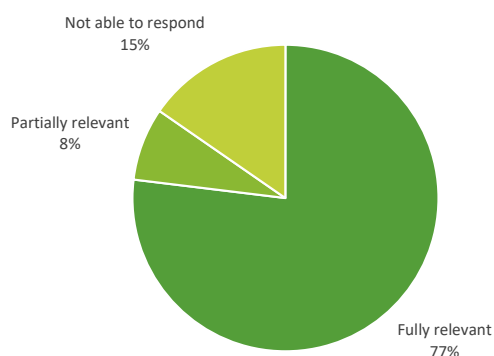
Q.42 - If yes in Q.41, is the usage of the SPOC mandatory for the electronic communication service providers? (N=10)



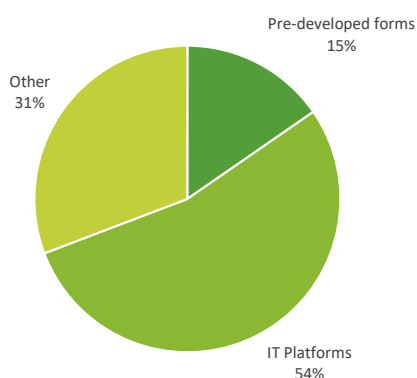
Q.43 - If no in Q.42, on average, how frequently do you get a request for non-content data via the SPOCs? (N=3)



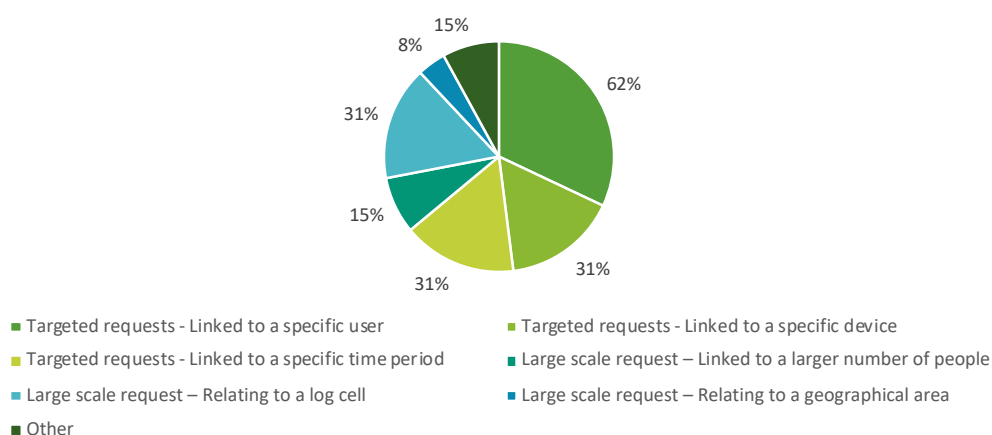
Q.44 - How would you describe the relevance of the use of the SPOCs as a tool to access non-content data? (N=13)



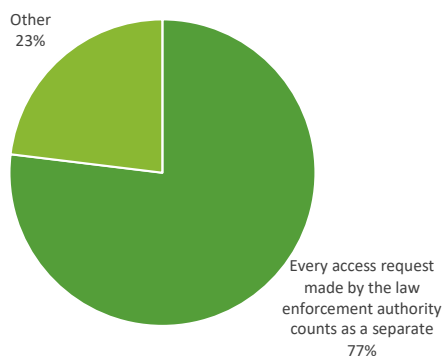
Q.45 - What are other practical arrangements/tools in place between the law enforcement authorities and the electronic communication service providers to access non-content data? (N=13)



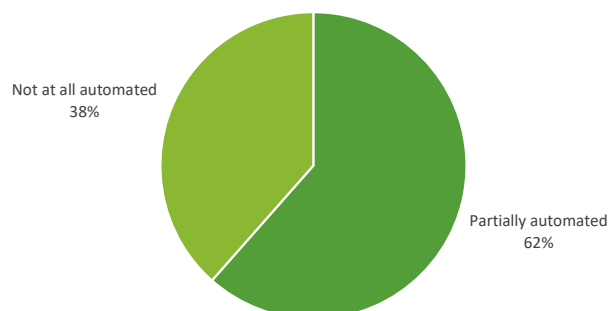
Q.46 - What is the most frequent practice used by law enforcement authorities to request non-content data? (Please select up to three answers) (N=13)



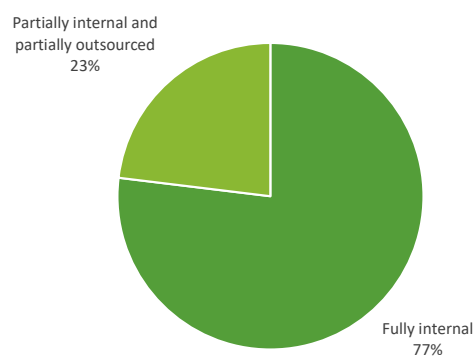
Q.48 - How do you record the number of access requests? (N=13)



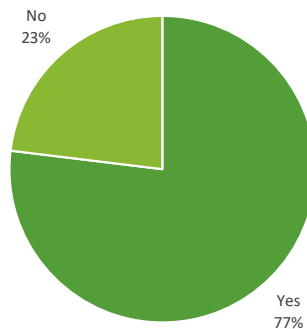
Q.49 - Is the procedure to respond to the requests for non-content data from law enforcement authorities automated? (N=13)



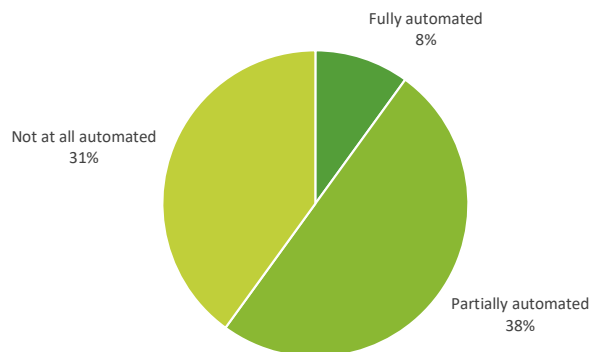
Q.50 - Is the procedure to process request for non-content data carried out internally within your organisation or is this process outsourced? (N=13)



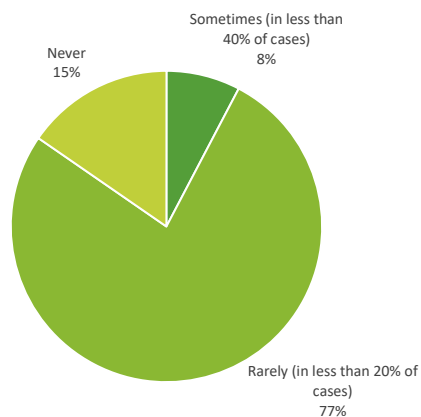
Q.51 - Does your organisation have a vetting system in place to perform a background check on whether the request for non-content data was submitted lawfully and from a credible source? (N=13)



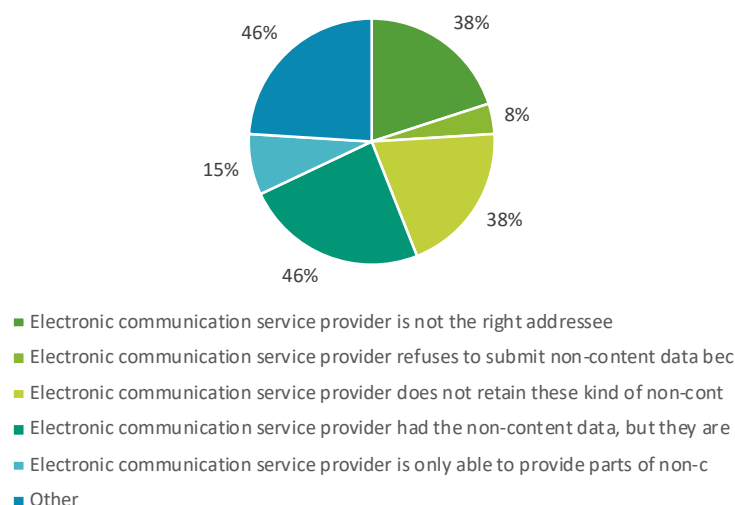
Q.52 - Is such a vetting system (e.g. verification process) automated?



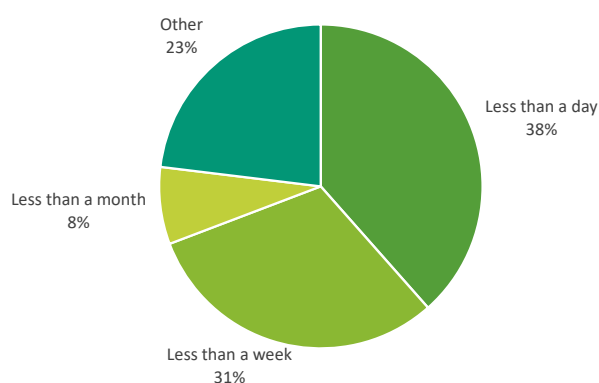
Q.53 - On average, what is the proportion of requests for non-content data which are refused? (A refused request is a request where you did not disclose any non-content data requested or where you disclosed only a limited amount of non-content data that did not suffice for the law enforcement authority to pursue the criminal case.) (N=13)



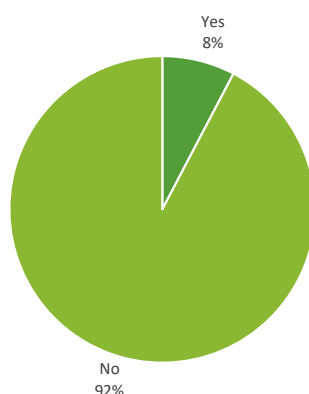
Q.54 - What are the most frequent reasons for NOT being able to answer (entirely or in part) to the request for non-content data from law enforcement authorities? Please select maximum three (3) reasons, which in your experience are the most frequent (N=13)



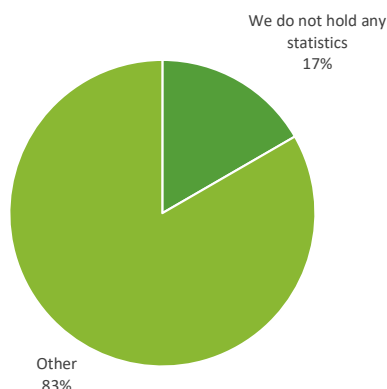
Q.55 - How long does it take for your company on average to disclose the non-content data that were requested? (N=13)



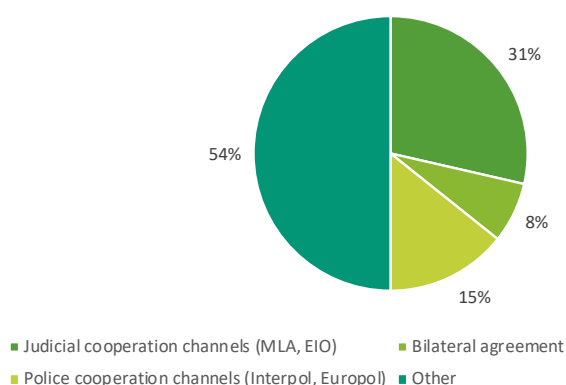
Q.57 - Could you please provide the number of requests to access non-content data in the last two (2) years (2018 and 2019) by the law enforcement authorities from other Member States, in the table below. If data for 2019 are not yet available, please provide data for the years 2017 and 2018. (N=13)



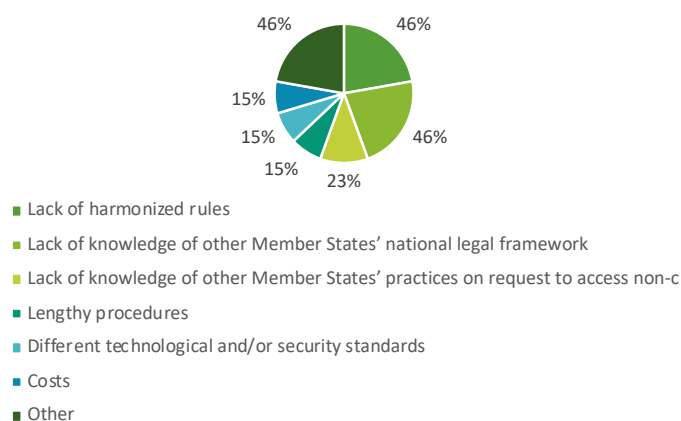
Q.58 – If no in Q.57, what is the reason that you cannot provide any estimation on the numbers of requests to access non-content data by the law enforcement authorities from other Member States? (N=12)



Q.59 - Which legal procedures do law enforcement authorities from other Member States use and what kind of legal instruments do they resort to in order to request access to non-content data? Please select up to three (3) answers, which in your opinion are the most relevant. (N=13)

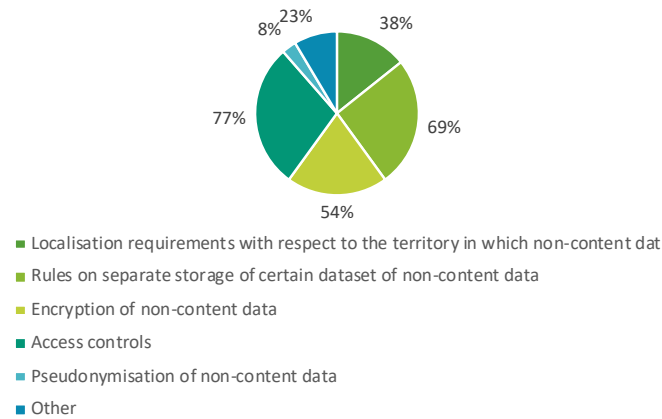


Q.60 - What are the main challenges in responding to requests for non-content data from law enforcement authorities from other Member States? Please select up to three (3) answers, which in your opinion are the most relevant. (N=13)

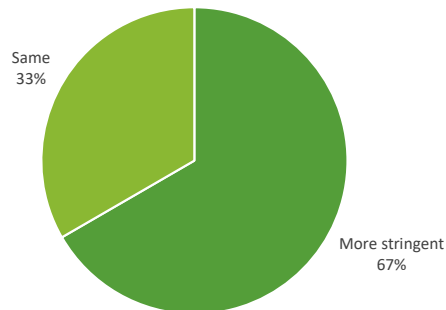


Technological challenges in retaining and accessing non-content data

Q.61 - What kind of security requirements does your organisation need to adhere to when it comes to retention of non-content data for law enforcement purposes? (Multiple answers are possible). (N=13)



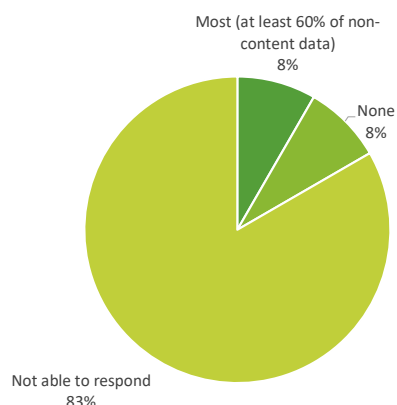
Q.62 - Are the security requirements that your organisation need to adhere to for law enforcement purposes more or less stringent than those in place for business purposes? (N=12)



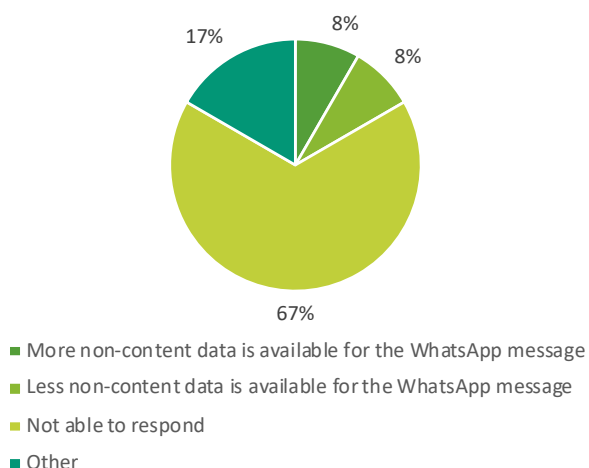
Q.63 - What is your organisation's role in the treatment of requests for non-content data from communications that occur via an Over-the-Top (OTT) platform (e.g. WhatsApp, Telegram)?

100% of respondents answered that they have no role, requests are processed by OTTs only.

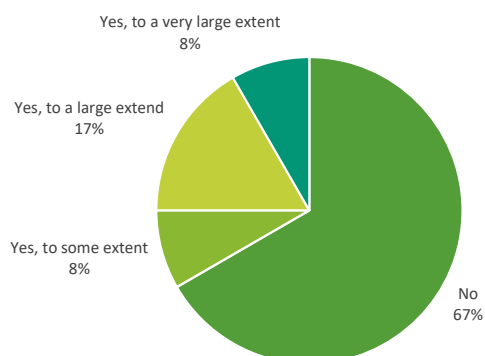
Q.64 - What is the proportion of non-content data transmitted through your network that stems from communications that occur via an Over-the-Top (OTT) platform (e.g. WhatsApp, Telegram)? (N=12)



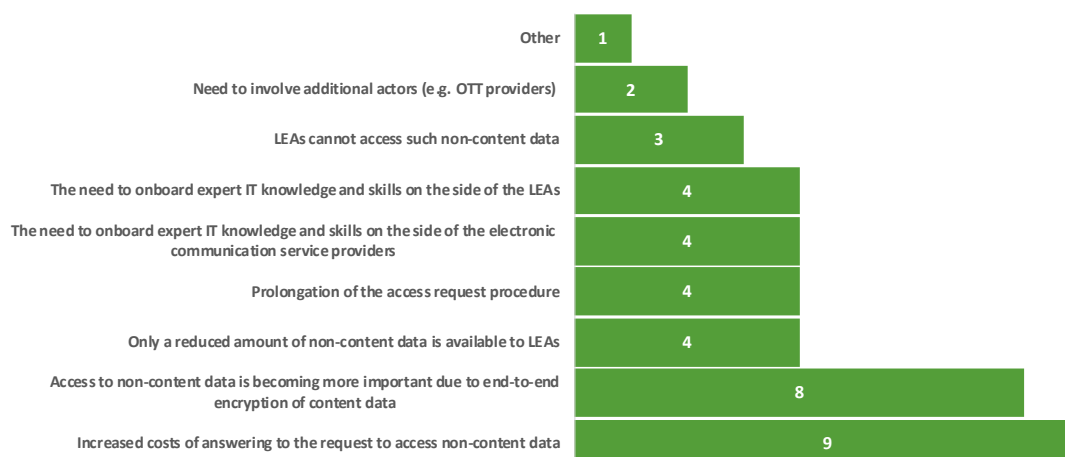
Q.65 - What changes in terms of the amount of non-content data available for the WhatsApp message compared to the traditional SMS? (N=12)



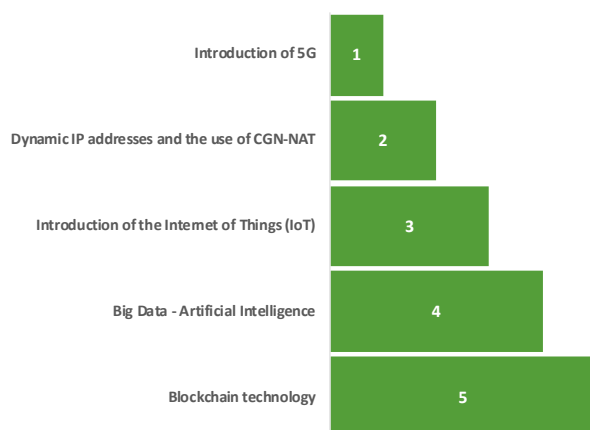
Q.67 - Does the end-to-end encryption of content data impact the access to non-content data by law enforcement authorities? (N=12)



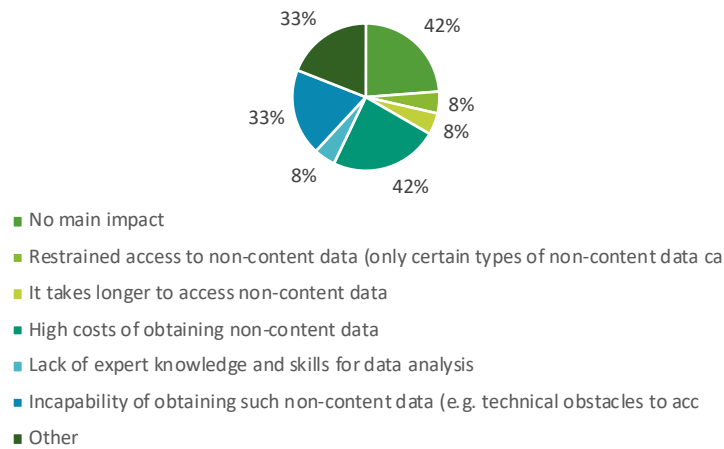
Q.68 - If yes, what type of impact does the end-to-end encryption of content data have on the access to non- content data? Please rank the top three answers, which in your opinion are the most relevant. (N=12)



Q.69 - What are the biggest technological challenges in your ability to retain and provide access to non- content data by the law enforcement authorities? Please rank the top three answers, which in your opinion are the most relevant. (N=12)



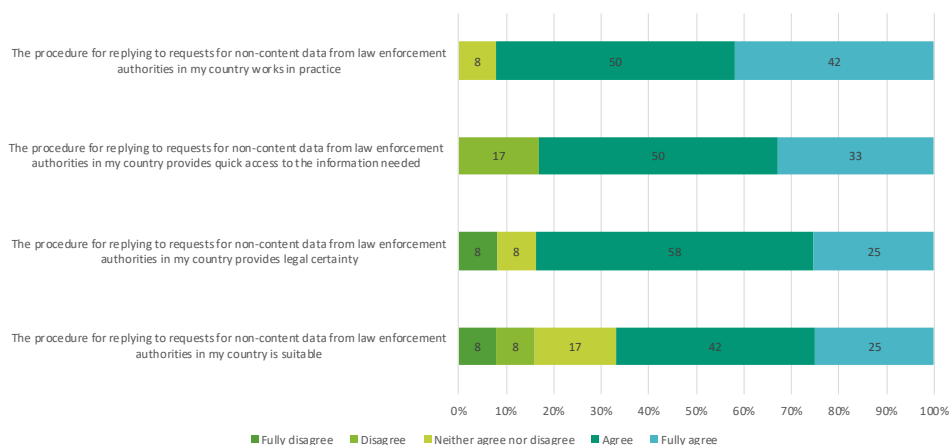
Q.70 - In your opinion, what is the likely impact of new technological trends (such as 5G or IoT) on access to non-content data? Please select up to three answers, which in your opinion are the most relevant. (N=12)



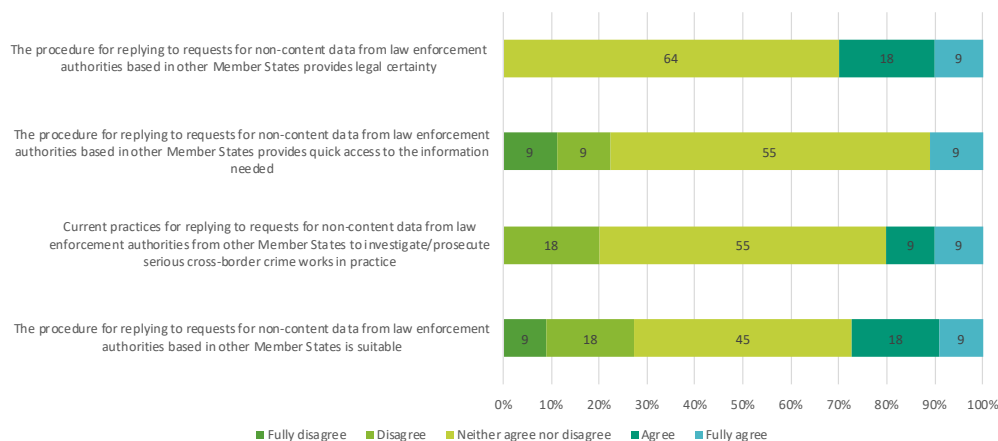
Main issues/obstacles of the current system to access non-content data

While the study does not aim to assess the functioning of the current system for retention of and access to non-content data in the Member States, it is important to understand the opinions of its users. The following section presented a set of statements about the functioning of the procedure of requesting and accessing non-content data from electronic communication service providers nationally and cross-border. Respondents were asked to state to what extent they agree with those statements, on a scale from 1 (fully disagree) to 5 (fully agree).

Q.72 - National system for replying to requests of non-content data from law enforcement authorities in the same Member State. (N=12)



Q.73 - National system for replying to requests of non-content data from law enforcement authorities in other Member States.(N=11)



ANNEX VI: SURVEY QUESTIONNAIRE TO LAW ENFORCEMENT AUTHORITIES (LEAS)

Profiling questions

1. In which country is your organisation based?*

- Austria
- Estonia
- France
- Germany
- Ireland
- Italy
- Poland
- Portugal
- Slovenia
- Spain

2. Please provide the name of your organisation and your position within the organisation in the box below.*

3. What is the territorial scope of your activities?*

- National
- Regional
- Other

If other, please specify your organisation's territorial scope of activity.

4. What is your organisation's role in the criminal procedure?*

- Investigation of crime
- Prosecution of crime
- Both
- Other

If other, please specify your organisation's main role in the national criminal procedure in the box below.

5. What type of law enforcement authority do you belong to?*

- Police
- Prosecutor's Office
- Court (Investigative Judge)
- Other

If other, please specify your organisation's type in the box below.

6. Do your activities include the preventive safeguarding of national security?*

- Yes

¹⁴⁴ If some of the information would be gathered in the course of the mapping exercise, we would refrain from asking additional questions like this one.

- No

If yes, please specify which of your activities fall under national security.

7. Does your organisation investigate and/or prosecute specific types of crimes?

- Yes
- No

If yes to question 7

8. Which types of crime does your organisation investigate and/or prosecute? Please select up to three (3) types of crimes, which are the focus of your activities.*¹⁴⁵ (*can ask to select the most relevant ones, e.g. up to three*)

- Organised crime
- Human trafficking
- Child sexual exploitation and child pornography
- Drug trafficking
- Trafficking of weapons
- Corruption
- Fraud
- Money laundering
- Cybercrime
- Murder, grievous bodily injury
- Kidnapping
- Organised and armed robbery
- Trafficking of cultural goods
- Counterfeiting and piracy of products
- Rape
- Trafficking in stolen vehicles
- Theft
- Other

If dealing with other types of crimes, please specify which one(s) in the box below.

Please provide your name and contact details that would enable us to contact you for a potential follow-up interview.

Name

Email

Telephone number

National practices of using electronic communications non-content data (metadata) in investigation and/or prosecution

Frequency of use of non-content data (metadata) in the investigation and/or prosecution of criminal cases

¹⁴⁵ For organisations dealing with more types of crime some of the subsequent questions in this survey e.g. on national practices, procedural aspects would need to be asked for every type of crime separately.

9. Do you hold any statistics on the number of requests for non-content data to electronic communication service provider?*

- Yes
- No

If yes to question 9

10. How do you record the number of access requests? *

- Every access request made to an electronic communication service provider counts as a separate request
- Every access request made for a particular type of non-content data counts as a separate request
- Every access request linked to a specific suspect counts as a separate request
- Other

If other, please explain such practice(s) in the box below.

If yes to question 9

11. How often do you record requests to access such non-content data?*

- On a monthly basis
- On a quarterly basis
- On a yearly basis
- Other

If other, please explain such practice(s) in the box below.

If yes to question 9

12. Do you publish any transparency or other types of reports on the number of requests to access non-content data or do you make data on the number of requests to access non-content data public?*

- Yes
- No

If yes to question 12

13. Please explain the basis of such a reporting obligation (e.g. mandatory by law, established practice) and how often do you publish such reports/information in the box below.*

14. **On average**, how often did you request access to non-content data from the traditional communication service providers (e.g. telephone operators, internet service providers) in the course of a criminal investigation/prosecution in the last two (2) years (2018 and 2019)? If data for 2019 are not yet available, please provide data for the years 2017 and 2018. (*In the absence of official statistics, please provide an estimation, based on your own experience.*)*

- In every criminal case (in 100% of cases)
- In more than 80% of the cases
- In between 60-80% of the cases
- In between 40-60% of the cases
- In between 20-40% of the cases
- In less than 20% of the cases
- Never

15. On average, to what extent did you request non-content data retained by the 'Over-the-Top' service providers (e.g. WhatsApp, Telegram communications etc.) in the course of a criminal investigation/prosecution in the last two (2) years (2018 and 2019)? If data for 2019 are not yet available, please provide data for the years 2017 and 2018. *(In the absence of official statistics, please provide an estimation, based on your own experience.)**

- In every criminal case (in 100% of cases)
- In more than 80% of the cases
- In between 60-80% of the cases
- In between 40-60% of the cases
- In between 20-40% of the cases
- In less than 20% of the cases
- Never

If needed, please explain your answer in the box below.

16. If your organisation has precise records on the use of non-content data in the course of investigation/prosecution in the last two (2) years (2018 and 2019), please provide them in the table below. If data for 2019 are not yet available, please provide data for the years 2017 and 2018. *(In the absence of official statistics, please provide an estimation, based on your own experience.)**

Reference period (Please indicate the year(s) or period(s) the data refer to)	Number of cases (Please provide numeric information)	Comments
2017		
2018		
2019		
Any other shorter period(s) (e.g. quarter, semester, month)		

17. What is the most frequent practice to request non-content data? Please select up to three (3) types of practices.*

- Targeted requests - Linked to a specific user
- Targeted requests - Linked to a specific device
- Targeted requests - Linked to a specific time period
- Large scale request – Linked to a larger number of people
- Large scale request – Relating to a log cell
- Large scale request – Relating to a geographical area
- Other

If other, please specify such types of requests in the box below.

18. **On average**, what is the proportion between targeted and large-scale requests in the last two (2) years (2018 and 2019)? If data for 2019 are not yet available, please provide data for the years 2017 and 2018. *(In the absence of official statistics, please provide an estimation, based on your own experience.)**

Type of request	Percentage of requests in 2017	Percentage of requests in 2018	Percentage of requests in 2019	Any other given period
Targeted				
Large Scale				

If other, please elaborate your answer in the box below.

--

19. **On average**, what is the proportion of cases in the last two (2) years (2018 and 2019) in which non-content data were used as a determinative and/or exclusionary evidence in achieving the purpose of investigation and/or prosecution (i.e.: without this type of evidence the investigation and/or prosecution would be dropped)? If data for 2019 are not yet available, please provide data for the years 2017 and 2018. *(In the absence of official statistics, please provide an estimation, based on your own experience.)**

Reference period (Please indicate the year(s) or period(s) the data refer to)	Number of investigations and/or prosecutions in which non-content data were used as determinative and/or exclusionary evidence (Please provide numeric information)	Comments
2017		
2018		
2019		
Any other shorter period(s) (e.g. quarter, semester, month)		

20. What is the number of investigations and/or prosecutions that were discontinued or dropped due to the problems in accessing non-content data in the last two (2) years (2018 and 2019)? If data for 2019 are not yet available, please provide data for the years 2017 and 2018. *(In the absence of official statistics, please provide an estimation, based on your own experience.)**

Reference period (Please indicate the year(s) or period(s) the data refer to)	Number of investigations and/or prosecutions that were discontinued or dropped due to the problems in accessing non-content data (Please provide numeric information)	Comments
2017		
2018		
2019		
Any other shorter period(s) (e.g. quarter, semester, month)		

21. What is the number of cases that have been dropped in the prosecution phase due to evidence based on non-content data have been declared inadmissible in the last two (2) years (2018 and 2019)? If data for 2019 are not yet available, please provide data for the years 2017 and 2018. *(In the absence of official statistics, please provide an estimation, based on your own experience.)**

Reference period (Please indicate the year(s) or period(s) the data refer to)	Number of prosecution cases that have used non-content data (Please provide numeric information)	Number of prosecutions in which evidence based on non-content data were declared inadmissible (Please provide numeric information)	Comments
2017			
2018			
2019			
Any other shorter period(s) (e.g. quarter, semester, month)			

Information on the characteristics of non-content data used in the investigation and/or prosecution of criminal cases

22. Which types of non-content data do you request and in how many cases **on average** do you request non-content data listed below in the course of an investigation/prosecution? Please provide an estimation of the use of different types of non-content data during the course of one year.*

Non-content data	Use Y/N	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
Subscriber data (service-associated information)							
Name							
Physical address associated							
Username							
Email address							
Telephone number							
SIM number							
Device identification numbers (e.g. IMEI number, MAC number)							
IP address							
Port number for dynamic IP addresses							
Billing and payment information (e.g. client number)							
Other (please specify)							
Traffic data							

Non-content data	Use Y/N	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
(communication-associated information)							
Duration of the communication							
Date & time of the communication (incl. time zone)							
Data volume of the electronic communication							
Missed calls (incl. No of rings of missed calls)							
Start of the communication							
End of the communication							
Connection to the relevant service							
Disconnection from to relevant service							
Type of communication (e.g. voice, SMS, email, chat, forum, social media)							
Type of the relevant service (e.g. ADSL, Wi-Fi, VoIP, cable, 3 or 4 G network)							
Other (please specify)							
Location data							
Location of the equipment or line at the start of the communication (e.g. cell towers, Wi-Fi hotspots)							
Location of the equipment or line at the end of the communication (e.g. cell towers, Wi-Fi hotspots)							
Other (please specify)							
Other data							
Destination of the communication: identifiers of the account, device or relevant service to							

Non-content data	Use Y/N	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
which the communication has been sent							
Destination of the communication: identifiers of the account, device or relevant service to which the communication has been forwarded, routed or transferred							
Destination of the communication: identifiers of the account, device or relevant service to which the communication has been attempted to be forwarded, routed or transferred							
Other (please specify)							

23. For what types of crimes do you usually request non-content data from the electronic communication service providers?

- For all types of crime that your organisation investigates/prosecutes
- Only for certain types of crime (e.g. serious crime)
- Other

If other, please explain your answer in the box below.

24. What is the average 'age' of the requested non-content data counting backwards from the time the relevant communication (e.g. phone call, message, internet access) took place?*

- Less than 1 week old
- Less than 1 month old
- Up to 3 months old
- Up to 6 months old
- Up to 1 year old
- Up to 2 years old
- More than 2 years old
- Other

If other, please elaborate your answer in the box below.

25. Could you provide an estimation for the proportion of requests for non-content data of a different 'age' in the last two (2) years (2018 and 2019) per type of crime. If data for

2019 are not yet available, please provide data for the years 2017 and 2018.* (Question repeated for each of the main types of crime the organisation of the respondents investigates/prosecutes, as selected in question 8)

Type of crime 1

'Age' of data	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
Less than 1 week old						
Less than 1 month old						
Up to 3 months old						
Up to 6 months old						
Up to 1 year old						
Up to 2 years old						

Type of crime 2

'Age' of data	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
Less than 1 week old						
Less than 1 month old						
Up to 3 months old						
Up to 6 months old						
Up to 1 year old						
Up to 2 years old						

Type of crime 3

'Age' of data	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
Less than 1 week old						
Less than 1 month old						
Up to 3 months old						
Up to 6 months old						
Up to 1 year old						

'Age' of data	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
Up to 2 years old						

Procedure for requesting access to non-content data in the investigation and/or prosecution of criminal cases

26. Does a procedure for requesting access to non-content data provide for a usage of a Single Points of Contact (SPOCs) for the law enforcement authorities?*

- Yes, applies to all categories of non-content data
- Yes, applies to some categories of non-content data
- Please, specify in the box below

- No

27. Is the usage of the SPOC obligatory for the law enforcement authorities?

- Yes
- No

If no to question 27

28. On average, how frequently do you make use of the SPOCs to request non-content data?*

- Always (in 100% of cases)
- Almost always (in at least 80% of the cases)
- Often (in at least 60% of cases)
- Regularly (in at least 40% of cases)
- Sometimes (in less than 40% of cases)
- Rarely (in less than 20% of cases)
- Never

29. Does a procedure for requesting access to non-content data provide for a usage of a Single Points of Contact (SPOCs) for the electronic communication service providers?*

- Yes, applies to all categories of non-content data
- Yes, applies to some categories of non-content data

Please, specify in the box below

- No

30. Is the usage of the SPOC obligatory for the electronic communication service providers?

- Yes
- No

31. How would you describe the relevance of the use of SPOCs as a tool to access non-content data?*

- Fully relevant
- Partially relevant
- Not at all relevant
- Not able to respond

Please explain your answer based on your experience in the box below.

32. What are other practical arrangements/tools in place between the law enforcement authorities and the electronic communication service provider to access non-content data?*

- Pre-developed forms
- Direct access
- IT Platforms
- Other

Please specify the way in which such tool(s) are used in the box below.

33. Does your organisation have an internal procedure in place for requesting non-content data?

- Yes
- No

Please specify the way the internal system works in the box below (e.g. special clearance requirements for the purpose of making the request, special person/unit responsible for making the request).

34. Does your organisation have an internal procedure in place for accessing non-content data received from the electronic communication service providers?

- Yes
- No

Please specify the way the internal system works in the box below (e.g. special clearance requirements for accessing and processing data, special person/unit eligible to access such data).

35. What kind of security requirements does the national framework require when it comes to retention of non-content data for law enforcement purposes?* (Multiple answers are possible.)

- Localisation requirements with respect to the territory in which non-content data should be retained
- Rules on separate storage of certain dataset of non-content data
- Encryption of non-content data
- Access controls
- Pseudonymisation of non-content data
- Other

36. On average, how often is your request for non-content data unsuccessful? (*An unsuccessful request is a request where you were unable to obtain any non-content data requested or where you were able to obtain only a limited amount of non-content data that did not suffice to progress with investigation/prosecution in the case in question.*)*

- Always (in 100% of cases)
- Almost always (in at least 80% of the cases)
- Often (in at least 60% of cases)
- Regularly (in at least 40% of cases)
- Sometimes (in less than 40% of cases)
- Rarely (in less than 20% of cases)

- Never

37. What are the most frequent reasons for NOT being able to access part of or the entire dataset of non-content data from the electronic communication service provider ? Please select maximum three (3) reasons, which in your experience are the most frequent.*

- Electronic communication service provider is not the right addressee
- Electronic communication service provider refuses to submit non-content data because of the procedural requirements
- Electronic communication service provider does not retain these kind of non-content data
- Electronic communication service provider had non-content data, but they are no longer retained
- Electronic communication service provider is only able to provide parts of non-content data sets and/or non-content data requested
- Non-content data are obtained but are not readable due to technical obstacles (e.g. non-content data are encrypted)
- Non-content data provided have different technological and/or security standards
- Other

If other, please specify the reason(s) in the box below.

38. How long does it take for your organisation on average to obtain non-content data requested?*

- Less than a day
- Less than a week
- Less than a month
- Less than three months
- Over three months
- Other

If other, please specify the average timeframe within which you obtain non-content data in the box below.

39. How could the current procedure of requesting and accessing non-content data be improved?

40. What other alternatives to requesting non-content data are available? *

- Data preservation/quick freeze
- Non-digital evidentiary alternatives
- Other

If other, please specify such alternative solution(s) in the box below.

41. Please explain in the box below which of the alternative solution(s) is the most relevant in the absence of data retention rules and why.

Procedure for accessing non-content data in case of cross-border cases

42. On average, how often did you request access to non-content data from a cross-border electronic communication service provider in the course of a criminal

investigation/prosecution in the last two (2) years (2018 and 2019). If data for 2019 are not yet available, please provide data for the years 2017 and 2018.* (Please provide either exact figures, if available, or percentage ranges).

Reference period (Please indicate the year(s) or period(s) the data refer to)	Number of requests to ESPs in other Member States (Please provide numeric information)	Share of requests to ESPs in other Member States against the total number of requests (Please provide numeric information)	Comments
2017			
2018			
2019			
Any other shorter period(s) (e.g. quarter, semester, month)			

43. Which legal procedures do you use and to what kind of legal instruments do you resort to in order to obtain non-content data from electronic communication service providers in other Member States? Please select all answers, which apply.*¹⁴⁶

- Judicial cooperation channels (MLA, EIO)
- Bilateral agreement
- Police cooperation channels (Interpol, Europol)
- CoE (Budapest) Convention on Cybercrime contact point
- Other

If other, please specify your answers in the box below.

44. What are the main challenges in accessing non-content data in case of cross-border criminal cases from electronic communication service providers from other Member States? Please select up to three (3) answers, which in your opinion are the most relevant.*

- Lack of harmonized rules
- Lack of knowledge of other Member States' national legal framework
- Lack of knowledge of other Member States' practices on access to non-content data
- Language issues
- Unable to identify whom to contact
- Bad response rates
- Lengthy procedures
- Different technological and/or security standards
- Costs
- Other

Please elaborate on your answers in the box below.

Technological challenges

¹⁴⁶ Selection of these options would need to be verified during the desk research and expert consultation.

Challenges related to end-to-end encryption

Certain 'Over-the-Top' service providers, such as WhatsApp or Telegram, subject all messages, phone calls, videos and any other form of information exchanged on their platforms to end-to-end encryption. This means that the communication is encrypted directly by the sender's device and can only be decrypted by the receiver's device. The electronic communication service providers involved in the transmission of the communication do not possess the cryptographic keys necessary to decrypt the communication. Although only the content of the communication is encrypted, this section seeks to understand whether additional challenges arise for law enforcement authorities when accessing the non-content data generated by these new types of communications subject to end-to-end encryption (e.g. uncertainties as to whom to address non-content data access requests, partial encryption of the non-content data, etc.).

45. What is the procedure to request access to non-content data generated by communications subject to end-to-end encryption?*

- Requests can be sent to the ESPs
- Requests need to be sent to OTT service providers
- Requests need to be sent to OTT service providers and ESPs
- Other

If other, please specify your answers in the box below.

--

46. Is the number of requests for accessing encrypted non-content data increasing in the last couple of years?*

- No
- Yes, to a limited extent
- Yes, to some extent
- Yes, to a large extent
- Yes, to a very large extent

47. What type of impact does the end-to-end encryption of data have on the access to non-content data? You can select up to three (3) answers, which in your opinion are the most relevant.*

- Non-content data are unreadable
- Only a reduced amount of non-content data is available
- Prolongation of the investigation/prosecutions proceedings
- The need to onboard expert IT knowledge and skills
- Increased costs of the investigation/prosecutions proceedings
- Need to involve additional actors (e.g. OTT service providers) for requesting and accessing non-content data
- Access to non-content data is more important due to end-to-end encryption of content data
- Other

If other, please specify any other impact(s) in the box below.

--

New technological challenges

48. What are the biggest technological challenges in accessing non-content data in the investigation and/or prosecution of criminal cases?* (can ask to select e.g. up to three, or to rank the options by level of importance).

- Big Data
- Blockchain technology

- End-to-end encryption of (non-)content data
- Introduction of 5G
- Introduction of the Internet of Things (IoT)
- Dynamic IP addresses and the use of CGN-NAT

Please explain your answer(s) based on your experience in the box below.

49. In your opinion, what is the likely impact of new technological trends (such as 5G and IoT) in access to non-content data? Please select up to three answers, which in your opinion are the most relevant.*

- No main impact
- Restrains access to non-content data (only certain types of non-content data can be accessed)
- It takes longer to access non-content data
- Non-content data are unreadable (data can be accessed but are unreadable due to encryption etc.)
- High costs of obtaining non-content data
- Shortage of human resources to process the information
- Lack of expert knowledge and skills for data analysis
- Incapability of obtaining such non-content data (e.g. technical obstacles to access data)
- Other

50. What are the measures (if any) which are envisaged to ensure access to non-content data in the context of such technological challenges? Please briefly elaborate in the box below.

Main issues/obstacles of the current system to access non-content data

While the study does not aim to assess the functioning of the current system for retention of and access to non-content data in the Member States, it is important to understand the opinions of its users. Below you will find a set of statements about the functioning of the procedure of requesting and accessing non-content data from electronic communication service providers based in your country or cross-border. Please state to what extent you agree with those statements, on a scale from 1 (fully disagree) to 5 (fully agree).

51. *National system of accessing non-content data*

	1 (fully disagree)	2 (disagree)	3 (Not agree nor disagree)	4 (agree)	5 (fully agree)
The procedure for requesting and accessing non-content data from the electronic communication service providers based in my country is suitable					
The procedure for requesting and accessing non-content data from the electronic communication service providers based in my country works in practice.					
The procedure for requesting and accessing non-content data from the					

electronic communication service providers based in my country provides quick access to the information needed					
The procedure for requesting and accessing non-content data from the electronic communication service providers based in my country provides legal certainty					

52. Cross-border access to non-content data – Within the EU

	1 (fully disagree)	2 (disagree)	3 (Not agree nor disagree)	4 (agree)	5 (fully agree)
The procedure for requesting and accessing non-content data from the electronic communication service providers based in other Member States is suitable					
Current practices for obtaining non-content data from the electronic communication service providers based in another Member State to investigate/prosecute serious cross-border crime works in practice					
The procedure for requesting and accessing non-content data from the electronic communication service providers based in another Member State provides quick access to the information needed					
The procedure for requesting and accessing non-content data from the electronic communication service providers based in another Member State provides legal certainty					

ANNEX VII: SURVEY QUESTIONNAIRE TO ELETRONIC COMMUNICATION SERVICE PROVIDERS (ESPS)

Profiling questions

1. In which country are you based?* *(Multiple answers, in case of cross-border ESPs, are possible.)*

- Austria
- Estonia
- France
- Germany
- Ireland
- Italy
- Poland
- Portugal
- Slovenia
- Spain
- Other (EU and/or third country)

If other, please specify the territorial scope of your company's activities.

2. Please provide the name of your company and your position within the company in the box below.*

Company name:

Your position:

3. What is the territorial scope of your company's activities?* ¹⁴⁷

- National
- Two or more EU Member States
- EU wide
- Worldwide
- Other

If other, please specify your company's territorial scope of activities.

4. If your company provides services in several countries, please briefly explain your company's structure or your group structure.*

5. What is your company's business model?*

- B2C
- B2B
- Both
- Other

If any other business model, please elaborate on your company's business model in the box below.

¹⁴⁷ If some of the information would be gathered in the course of the mapping exercise, we would refrain from asking additional questions like this one.

6. Which types of electronic communication services does your organisation provide? Please select as many services as relevant.*

- Fixed line
- Mobile services
- Cable services
- Satellite services
- Internet communication services
- Voiceover IP communication services
- Other

If any other type of services, please specify such services in the box below.

--

7. Are any of these electronic communication services provided through the resources (i.e. network) of another electronic communication service provider?*

- Yes
- No

If yes to Question 7

8. Who controls the data retention and processes the access requests to non-content data for law enforcement purposes linked to these services?

- Data retention and access requests are processed internally
- Data retention and access requests are processed in part by the other electronic communication service provider
- Data retention and access requests are processed entirely by the other electronic communication service provider
- Other

If other, please specify in the box below.

--

9. What is the size of your organisation?*

- Micro (staff headcount < 10 or turnover ≤ € 2 million)
- Small (staff headcount < 50 or turnover ≤ € 10 million)
- Medium size (staff headcount < 250 or turnover ≤ € 50 million)
- Large (staff headcount > 250 or turnover ≥ € 50 million)

10. What is your organisation's market share of the electronic communication services? Please provide the estimation of your size **based on the number of your users/customers** for every specific Member State in which you conduct activities in the table below (Please only provide data for B2C activities).*

EU Member State(s) in which your organisation is active (Please only provide data for the following countries: AT, DE, EE, ES, FR, IE, IT, PL, PT, SI)	Number of users

Please provide the estimation of your size **based on an estimation of your market share** for every specific Member State in which you conduct activities in the table below (Please only provide data for B2C activities).*

EU Member State(s) in which your organisation is active (Please only provide data for the following countries: AT, DE, EE, ES, FR, IE, IT, PL, PT, SI)	Market share estimation				
	Below 10%	10-30%	30-50%	50-70%	Above 70%

Please provide your name and contact details that would enable us to contact you for a **potential** follow-up interview. *All data provided will remain confidential and be treated in conformity with the European Commission Privacy Statement.*

Name

Email

Telephone number

National practices of retaining electronic communications non-content data (metadata) by the electronic communication service providers

Information on the characteristics of non-content data retained by the electronic communication service providers

One of the purposes of this study is to understand which non-content data electronic communication service providers retain. We have identified four (4) sub-categories of non-content data: subscriber data, traffic data, localisation data and other non-content data. Could you please indicate in the following questions what type of information your organisation retains regarding each of these categories of non-content data.

11. What type of **subscriber** non-content data (service-associated information) does your organisation retain? (Please select all applicable answers.)*
 - Name
 - Physical address
 - Username
 - Email address
 - Telephone number
 - SIM number
 - Device identification numbers (e.g. IMEI number, MAC number)
 - IP address
 - Port number for dynamic IP addresses
 - Billing and payment information (e.g. client number)
 - All of the above
 - Other (please specify)

12. Please specify in the table below what are the **purposes** for which you retain above listed subscriber data (including but not limited to IP address, port number for dynamic IP addresses, device identification numbers)?*

Subscriber non-content data	Purpose of processing							Comments
	Business and/or commercial	(Direct) marketing	Invoicing	Taxation	Law enforcement	Network security	National security	
Name								
Physical address associated								
Username								
Email address								
Telephone number								
SIM number								
Device identification numbers (e.g. IMEI number, MAC number)								
IP address								
Port number for dynamic IP addresses								
Billing and payment information (e.g. client number)								
Other								

13. What type of **traffic** non-content data (communication-associated information) does your organisation retain? (Please select all applicable answers.)*

- Duration of the communication
- Date & time of the communication (incl. time zone)
- Data volume of the electronic communication
- Missed calls (incl. No of rings of missed calls)
- Start of the communication
- End of the communication
- Connection to the relevant service
- Disconnection from to relevant service
- Type of communication (e.g. voice, SMS, email, chat, forum, social media)
- Type of network technology (e.g. ADSL, Wi-Fi, VoIP, cable, 3 or 4G network)
- Other (please specify)

14. Please specify in the table below what are the **purposes** for which you retain above listed traffic data?*

Traffic non-content data	Purpose of processing							Comments
	Business and/or commercial	(Direct) marketing	Invoicing	Taxation	Law enforcement	Network security	National security	
Duration of the								

Traffic non-content data	Purpose of processing							Comments
	Business and/or commercial	(Direct) marketing	Invoicing	Taxation	Law enforcement	Network security	National security	
communication								
Date & time of the communication (incl. time zone)								
Data volume of the electronic communication								
Missed calls (incl. No of rings of missed calls)								
Start of the communication								
End of the communication								
Connection to the relevant service								
Disconnection from to relevant service								
Type of communication (e.g. voice, SMS, email, chat, forum, social media)								
Type of network technology (e.g. ADSL, Wi-Fi, VoIP, cable, 3 or 4 G network)								
Other								

15. What type of **location** non-content data does your organisation retain? (Please select all applicable answers)*
- Location of the equipment or line at the start of the communication (e.g. cell towers, Wi-Fi hotspots)
 - Location of the equipment or line at the end of the communication (e.g. cell towers, Wi-Fi hotspots)
 - Other (please specify)
16. Please specify in the table below what are the **purposes** for which you retain above listed location data?*

Non-content data	Purpose of processing							Comments
	Business and/or commercial	(Direct) marketing	Invoicing	Taxation	Law enforcement	Network security	National security	
Location of the equipment or line at the start of the communication (e.g. cell towers, Wi-Fi hotspots)								
Location of the equipment or line at the end of the communication (e.g. cell towers, Wi-Fi hotspots)								
Other								

17. What type of **other** non-content data does your organisation retain? (Please select all applicable answers)*

- Destination of the communication: identifiers of the account, device or relevant service to which the communication has been sent.
- Destination of the communication: identifiers of the account, device or relevant service to which the communication has been forwarded, routed or transferred.
- Destination of the communication: identifiers of the account, device or relevant service to which the communication has been attempted to be forwarded, routed or transferred.
- Other (please specify)

18. Please specify in the table below what are the **purposes** for which you retain above listed other types of non-content data?

Non-content data	Purpose of processing							Comments
	Business and/or commercial	(Direct) marketing	Invoicing	Taxation	Law enforcement	Network security	National security	
Destination of the communication: identifiers of the account, device or relevant service to which the communication has been sent								
Destination of the communication: identifiers of the account, device or relevant service to which the communication								

Non-content data	Purpose of processing							Comments
	Business and/or commercial	(Direct) marketing	Invoicing	Taxation	Law enforcement	Network security	National security	
has been forwarded, routed or transferred								
Destination of the communication: identifiers of the account, device or relevant service to which the communication has been attempted to be forwarded, routed or transferred								
Other								

19. What determines the length of the retention periods of non-content data?*

- Retention periods are determined by the type of non-content data retained
- Retention periods are determined by the purpose for which the non-content data are processed (commercial v. law enforcement)
- Retention periods are determined by both – type of non-content data retained and the purpose for which they are processed
- Other

If other, please explain in the box below what determined the retention periods.

Only appears if the answer to question 19 is 'by the type of non-content data' or by 'both'

20. Please indicate in the table below the retention period for **subscriber** (service-associated information) non-content data and whether the retention periods have been set by law or not.*¹⁴⁸

Non-content data	Retention period*	How is the retention period fixed?*				Comments
		By national law or administrative decision	By case-law	By the ESP itself	Other (please specify)	
Name						
Physical address associated						
Username						
Email address						
Telephone number						
SIM number						

¹⁴⁸ This table should appear if retention periods are set differently per type of non-content data.

Non-content data	Retention period*	How is the retention period fixed?*				Comments
		By national law or administrative decision	By case-law	By the ESP itself	Other (please specify)	
Device identification numbers (e.g. IMEI number, MAC number)						
IP address						
Port number for dynamic IP addresses						
Billing and payment information (e.g. client number)						
Other						

21. Please indicate in the table below the retention period for **traffic** non-content data and whether the retention periods have been set by law or not

Non-content data	Retention period*	How is the retention period fixed?*				Comments
		By national law or administrative decision	By case-law	By the ESP itself	Other (please specify)	
Duration of the communication						
Date & time of the communication (incl. time zone)						
Data volume of the electronic communication						
Missed calls (incl. No of rings of missed calls)						
Start of the communication						
End of the communication						
Connection to the relevant service						
Disconnection from to relevant service						
Type of communication (e.g. voice, SMS, email, chat, forum, social media)						
Type of network technology (e.g.						

Non-content data	Retention period*	How is the retention period fixed?*				Comments
		By national law or administrative decision	By case-law	By the ESP itself	Other (please specify)	
ADSL, Wi-Fi, VoIP, cable, 3 or 4 G network)						
Other						

22. Please indicate in the table below the retention period for **location** non-content data and whether the retention periods have been set by law or not.

Non-content data	Retention period*	How is the retention period fixed?*				Comments
		By national law or administrative decision	By case-law	By the ESP itself	Other (please specify)	
Location of the equipment or line at the start of the communication (e.g. cell towers, Wi-Fi hotspots)						
Location of the equipment or line at the end of the communication (e.g. cell towers, Wi-Fi hotspots)						
Other						

23. Please indicate in the table below the retention period for **other** non-content data and whether the retention periods have been set by law or not.

Non-content data	Retention period*	How is the retention period fixed?*				Comments
		By national law or administrative decision	By case-law	By the ESP itself	Other (please specify)	
Destination of the communication: identifiers of the account, device or relevant service to which the communication has been sent						
Destination of the communication: identifiers of the account, device or relevant service to which the communication has been forwarded, routed or transferred						
Destination of the communication:						

Non-content data	Retention period*	How is the retention period fixed?*				Comments
		By national law or administrative decision	By case-law	By the ESP itself	Other (please specify)	
identifiers of the account, device or relevant service to which the communication has been attempted to be forwarded, routed or transferred						
Other						

Only appears if the answer to question 19 is 'by the purpose for which they are processed' or 'by both'

24. Please indicate in the table below the retention period for each specific purpose for which the non-content data are processed and whether this retention period has been set by law or not.*¹⁴⁹

Purpose for which the non-content data is processed	Retention period*	How is the retention period fixed?*				Comments
		By national law or administrative decision	By case-law	By the ESP itself	Other (Please specify)	
General business / commercial						
(Direct) marketing						
Billing						
Invoicing						
Taxation						
Network security						
Law enforcement						
National security						
Other (Please specify)						

Information on the costs of retention of non-content data for law enforcement purposes

25. Does your company have the legal obligation to retain certain types of non-content data exclusively for law enforcement purposes? (Please consider only legislation currently in force)

*

- Yes
- No

¹⁴⁹ This table should appear if retention periods are set differently per type of non-content data.

If replied Yes to question 22

26. Has your business incurred any additional costs directly linked to the retention of non-content data for law enforcement purposes in the last few years (i.e. since the national legal framework has been put in place)?*
- No additional costs
 - Some additional costs
 - Substantial additional costs
 - Major additional costs

If additional costs in question 23

27. Please select the three most relevant reasons for these additional costs.*
- Costs of setting up new infrastructure and tools
 - Costs of IT equipment and system
 - Costs of internal controls and audit
 - Costs of staff
 - Other (please specify)

If in profiling question 5, answer is both (B2C and B2B),

Are the additional costs incurred similar for your B2B activities?*

- Yes
- No

If no, please explain how they differ.

28. On average, what are the annual costs associated with retention and access of non-content data for law enforcement purposes?

	Costs of retention	Costs of granting access	Overall annual costs
Initial costs of setting up new infrastructure and tools			
Costs of IT equipment and system			
Costs of internal controls and audit			
Costs of staff			
Other			

If there are other costs, please explain in the box below.

29. Do you receive reimbursement for these costs under the current legal national framework?*
- Yes, entirely
 - Yes, partially
 - No
 - Other

If needed, please explain your answer in the box below.

30. Who reimburses the costs of retention and access requests of non-content data for law enforcement purposes? Please explain in the box below.*

National practices of requesting access to electronic communications non-content data (metadata) by the law enforcement authorities

Frequency of requests to access non-content data by law enforcement authorities

31. How do you record requests to access such non-content data?*

- On a monthly basis
- On a quarterly basis
- On a yearly basis
- Other

If other, please explain such practice(s) in the box below.

32. Do you hold any statistics on the number of requests for non-content data by law enforcement authorities?*

- Yes
- No

If no, please explain why:

If yes to question 29

33. Do you publish any transparency or other types of reports on the number of requests to access non-content data or do you make data on the number of requests to access non-content data public?*

- Yes
- No

If yes to question 30

34. Please explain the basis of such a reporting obligation (e.g. mandatory by law, established practice) and how often do you publish such reports/information in the box below.*

35. Could you please provide the number of requests for non-content data in the last two (2) years (2018 and 2019) by the national law enforcement authorities, in the table below? If data for 2019 are not yet available, please provide data for the years 2017 and 2018.*

- Yes

Reference period* (Please indicate the year(s) or period(s) the data refer to)	Number of national LEAs requests* (Please provide numeric information)	Comments
2017		
2018		
2019		
Any other shorter period(s) (e.g. quarter, semester, month)		

- No

If no to question 32

36. What is the reason that you cannot provide any estimation on the numbers of requests for non-content data?

- We do not hold any statistics
- There is no legal obligation obliging us to record numbers of requests
- We are prohibited by law to record numbers of requests
- Other

Please explain your answer:

37. **On average**, which types of **subscriber** non-content data are most often requested by the law enforcement authorities. Please provide an estimation of the percentage of requests to access different types of subscriber non-content data during the course of one year (2018 or 2019).*

Subscriber non-content data	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
Name						
Physical address associated						
Username						
Email address						
Telephone number						
SIM number						
Device identification numbers (e.g. IMEI number, MAC number)						
IP address						
Port number for dynamic IP addresses						
Billing and payment information (e.g. client number)						
Other						

38. **On average**, which types of **traffic** non-content data are most often requested by the law enforcement authorities. Please provide an estimation of the percentage of requests to access different types of traffic non-content data during the course of one year (2018 or 2019).*

Traffic non-content data	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
Duration of the communication						
Date & time of the communication (incl. time zone)						
Data volume of the						

Traffic non-content data	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
electronic communication						
Missed calls (incl. No of rings of missed calls)						
Start of the communication						
End of the communication						
Connection to the relevant service						
Disconnection from to relevant service						
Type of communication (e.g. voice, SMS, email, chat, forum, social media)						
Type of network technology (e.g. ADSL, Wi-Fi, VoIP, cable, 3 or 4 G network)						
Other						

39. **On average**, which types of **location** non-content data are most often requested by the law enforcement authorities. Please provide an estimation of the percentage of requests to access different types of location non-content data during the course of one year (2018 or 2019).*

Location non-content data	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
Location of the equipment or line at the start of the communication (e.g. cell towers, Wi-Fi hotspots)						
Location of the equipment or line at the end of the communication (e.g. cell towers, Wi-Fi hotspots)						
Other						

40. **On average**, which types of **other** non-content data are most often requested by the law enforcement authorities. Please provide an estimation of the percentage of requests to access different types of other non-content data during the course of one year (2018 or 2019).*

Other non-content data	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
Destination of the communication: identifiers of the account, device or relevant service to which the communication has been						

Other non-content data	0-20%	20%-40%	40%-60%	60%-80%	More than 80%	Comments/Notes
sent						
Destination of the communication: identifiers of the account, device or relevant service to which the communication has been forwarded, routed or transferred						
Destination of the communication: identifiers of the account, device or relevant service to which the communication has been attempted to be forwarded, routed or transferred						
Other						

Procedure for requesting access to non-content data by the law enforcement authorities within your country

41. Does the procedure for requesting access to non-content data provide for a usage of a Single Points of Contact (SPOCs)?*
 - Yes
 - No
42. Is the usage of the SPOC mandatory for the electronic communication service providers?
 - Yes
 - No

If no to question 39

43. On average, how frequently do you get a request for non-content data via the SPOCs?*
 - Always (in 100% of cases)
 - Almost always (in at least 80% of the cases)
 - Often (in at least 60% of cases)
 - Regularly (in at least 40% of cases)
 - Sometimes (in less than 40% of cases)
 - Rarely (in less than 20% of cases)
 - Never
44. How would you describe the relevance of the use of the SPOCs as a tool to grant access non-content data?*
 - Fully relevant
 - Partially relevant
 - Not at all relevant
 - Not able to respond

Please explain your answer based on your experience in the box below.

45. What are other practical arrangements/tools in place between the law enforcement authorities and the electronic communication service providers to access non-content data?*
- Pre-developed forms
 - Direct access
 - IT Platforms
 - Other

Please specify the manner in which such tool(s) are used in the box below.

46. What is the most frequent practice used by the law enforcement authorities to request non-content data?*
- Targeted requests - Linked to a specific user
 - Targeted requests - Linked to a specific device
 - Targeted requests - Linked to a specific time period
 - Large scale request – Linked to a larger number of people
 - Large scale request – Relating to a log cell
 - Large scale request – Relating to a geographical area
 - Other

If other, please specify such types of requests in the box below.

47. On average, what is the proportion between targeted and large-scale requests in the last two (2) years (2018 and 2019)? If data for 2019 are not yet available, please provide data for the years 2017 and 2018.*

Type of request	Percentage of requests in 2017	Percentage of requests in 2018	Percentage of requests in 2019	Any other given period
Targeted				
Large Scale				

48. How do you record the number of access requests? *
- Every access request made by the law enforcement authority counts as a separate request
 - Every access request made for a particular type of non-content data counts as a separate request
 - Every access request linked to a specific user counts as a separate request
 - Other

Please elaborate on your answer in the box below.

49. Is the procedure to respond to the requests for non-content data from law enforcement authorities automated?*
- Fully automated
 - Partially automated
 - Not at all automated

Please briefly elaborate on your answer in the box below.

50. Is the procedure to process request for non-content data carried out internally within your organisation or is this process outsourced?*
- Fully internal
 - Partially internal and partially outsourced

- Fully outsourced

Please briefly elaborate on your answer in the box below:

51. Does your organisation have a vetting system in place to perform a background check on whether the request for non-content data was submitted lawfully and from a credible source?*
- Yes
 - No

If yes, please briefly explain how the vetting system verifies that the request comes from a credible source in the box below.

If yes, please briefly explain how the vetting system verifies that the request was submitted lawfully in the box below.

If yes to question 48

52. Is such a vetting system (e.g. verification process) automated?*
- Fully automated
 - Partially automated
 - Not at all automated

Please briefly elaborate on your answer in the box below.

53. On average, what is the proportion of requests for non-content data which are refused? (A *refused request* is a request where you did not disclose any non-content data requested or where you disclosed only a limited amount of non-content data that did not suffice for the law enforcement authority to pursue the criminal case.)*
- Always (in 100% of cases)
 - Almost always (in at least 80% of the cases)
 - Often (in at least 60% of cases)
 - Regularly (in at least 40% of cases)
 - Sometimes (in less than 40% of cases)
 - Rarely (in less than 20% of cases)
 - Never

If needed, please explain your answer in the box below.

54. What are the most frequent reasons for NOT being able to answer (entirely or in part) to the request for non-content data from law enforcement authorities? Please select maximum three (3) reasons, which in your experience are the most frequent.*
- Electronic communication service provider is not the right addressee
 - Electronic communication service provider refuses to submit non-content data because of the procedural requirements
 - Electronic communication service provider does not retain these kind of non-content data
 - Electronic communication service provider had the non-content data, but they are no longer retained
 - Electronic communication service provider is only able to provide parts of non-content data sets and/or non-content data requested

- Non-content data are obtained but are not readable due to technical obstacles (e.g. non-content data are encrypted)
- Non-content data provided have different technological and/or security standards
- Other

If needed, please specify the reason(s) in the box below.

55. How long does it take for your company on average to disclose the non-content data that were requested?*

- Less than a day
- Less than a week
- Less than a month
- Less than three months
- Over three months
- Other

If other, please specify, on average, the timeframe for disclosing non-content data in the box below.

56. How could the current procedure of requesting and accessing non-content data be improved?

Procedure for responding to requests from law enforcement authorities in other Member States

57. Could you please provide the number of requests to access non-content data in the last two (2) years (2018 and 2019) by the law enforcement authorities from other Member States, in the table below. If data for 2019 are not yet available, please provide data for the years 2017 and 2018.* (Please provide figures and/or shares, depending on availability.)

- Yes

Reference period (Please indicate the year(s) or period(s) the data refer to)	Number of requests from LEAs in other MSs (Please provide numeric information)	Share of requests from LEAs in other MSs (Please provide numeric information)	Comments
2017			
2018			
2019			
Any other shorter period(s) (e.g. quarter, semester, month)			

- No

If no to question 54

58. What is the reason that you cannot provide any estimation on the numbers of requests to access non-content data by the law enforcement authorities from other Member States?
- We do not hold any statistics
 - There is no legal obligation obliging us to record numbers of requests
 - We are prohibited by law to record numbers of requests

- Other

Please explain your answer:

59. Which legal procedures do law enforcement authorities from other Member States use and what kind of legal instruments do they resort to in order to request access to non-content data? Please select up to three (3) answers, which in your opinion are the most relevant.*¹⁵⁰
- Judicial cooperation channels (MLA, EIO)
 - Bilateral agreement
 - Police cooperation channels (Interpol, Europol)
 - CoE (Budapest) Convention on Cybercrime contact point
 - Other

If other, please specify your answers in the box below.

60. What are the main challenges in responding to requests for non-content data from law enforcement authorities from other Member States? Please select up to three (3) answers, which in your opinion are the most relevant.*
- Lack of harmonized rules
 - Lack of knowledge of other Member States' national legal framework
 - Lack of knowledge of other Member States' practices on request to access non-content data
 - Language issue
 - Unable to identify if the law enforcement authority is authorized to request such non-content data
 - Lengthy procedures
 - Different technological and/or security standards
 - Costs
 - Other

Please elaborate on your answers in the box below.

Technological challenges in retaining and accessing non-content data

Technological challenges concerning security requirements

61. What kind of security requirements does your organisation need to adhere to when it comes to retention of non-content data for law enforcement purposes?* (*Multiple answers are possible.*)
- Localisation requirements with respect to the territory in which non-content data should be retained
 - Rules on separate storage of certain dataset of non-content data
 - Encryption of non-content data
 - Access controls
 - Pseudonymisation of non-content data
 - Other

Please briefly elaborate on your answer(s) in the box below.

¹⁵⁰ Selection of these options would need to be verified during the desk research and expert consultation.

62. Are the security requirements that your organisation needs to adhere to for law enforcement purposes more or less stringent than those in place for business purposes?*

- More stringent
- Same
- Less stringent

In case the security requirements are different, please explain what the main differences are?

Challenges related to Over-the-Top communication platforms and end-to-end encryption

63. What is your organisation's role in the treatment of requests for non-content data from communications that occur via an Over-the-Top (OTT) platform (e.g. WhatsApp, Telegram)?*

- No role, requests are processed by OTT service providers only
- Limited role (e.g. processed until data reach a network node), requests are forwarded to OTT service providers for completion
- Major role
- Other

If other, please specify any other impact(s) in the box below

If limited role, major role or other

Please elaborate on your role in treating requests for non-content data from OTT communications and whether this has an impact on your organisation.

64. What is the proportion of non-content data transmitted through your network that stems from communications that occur via an Over-the-Top (OTT) platform (e.g. WhatsApp, Telegram)?*

- All (100% of all non-content data)
- Almost all (at least 80% of non-content data)
- Most (at least 60% of non-content data)
- Some (at least 40% of non-content data)
- A limited part (less than 40% of non-content data)
- A very limited part (less than 20% of non-content data)
- None

The study also seeks to understand the impact, if any, of end-to-end encryption on non-content data. To that end, please consider the following scenario:

A communication occurs via a traditional communication channel, for example, an SMS is sent via a telecommunication operator. The exact same communication occurs via an over-the-top (OTT) platform, for example the same message is sent via WhatsApp.

65. What changes in terms of the amount of non-content data available for the WhatsApp message compared to the traditional SMS? *

- More non-content data is available for the WhatsApp message
- Less non-content data is available for the WhatsApp message
- The same amount of non-content data is available for both communications
- Other (please specify)

Please explain your answer(s) in the box below.

66. In the example provided above, would the type of non-content data available for the two communications (WhatsApp message vs. traditional SMS) be different? If yes, please explain how it differs?

67. Does the end-to-end encryption of content data impact your ability to provide access to non-content data by law enforcement authorities?*
- No
 - Yes, to a limited extent
 - Yes, to some extent
 - Yes, to a large extent
 - Yes, to a very large extent

68. If yes, what type of impact does the end-to-end encryption of content data have on the access to non-content data? You can select up to three answers, which in your opinion are the most relevant.* *(Possible to ask respondents to select most relevant options, e.g. up to 3, or to rank the options provided by relevance)*

- LEAs cannot access such non-content data
- Only a reduced amount of non-content data is available to LEAs
- Prolongation of the access request procedure
- The need to onboard expert IT knowledge and skills on the side of the electronic communication service providers
- The need to onboard expert IT knowledge and skills on the side of the LEAs
- Increased costs of answering to the request to access non-content data
- Need to involve additional actors (e.g. OTT service providers) for requesting and accessing non-content data
- Access to non-content data is becoming more important due to end-to-end encryption of content data
- Other

If other, please specify any other impact(s) in the box below.

New technological challenges

69. What are the biggest technological challenges in your ability to retain and provide access to non-content data by the law enforcement authorities?* *(Possible to ask respondents to select most relevant options, e.g. up to 3, or to rank the options provided by relevance)*

- Big Data – Artificial Intelligence
- Blockchain technology
- Introduction of 5G
- Introduction of the Internet of Things (IoT)
- Dynamic IP addresses and the use of CGN-NAT

Please explain your answer(s) based on your experience in the box below.

70. In your opinion, what is the likely impact of new technological trends (such as 5G or IoT) on access to non-content data? Please select up to three answers, which in your opinion are the most relevant.*

- No main impact
- Restrained access to non-content data (only certain types of non-content data can be accessed)
- It takes longer to access non-content data
- Non-content data are unreadable (data can be accessed but are unreadable due to encryption etc.)
- High costs of obtaining non-content data
- Shortage of human resources to process the information

- Lack of expert knowledge and skills for data analysis
- Incapability of obtaining such non-content data (e.g. technical obstacles to access data)
- Other

If other, please specify any other impact(s) in the box below.

71. What are the measures (if any) which are envisaged to ensure retention and access to non-content data in the context of such technological challenges? Please briefly elaborate in the box below.*

Main issues/obstacles of the current system to access non-content data

While the study does not aim to assess the functioning of the current system for retention of and access to non-content data in the Member States, it is important to understand the opinions of its users. Below you will find a set of statements about the functioning of the procedure of retaining and requesting non-content data by law enforcement authorities based in your country or cross-border. Please state to what extent you agree with those statements, on a scale from 1 (fully disagree) to 5 (fully agree).

72. *National systems for replying to requests of non-content data from law enforcement authorities in the same Member State*

	1 (fully disagree)	2 (disagree)	3 (Not agree nor disagree)	4 (agree)	5 (fully agree)
The procedure for replying to requests for non-content data from law enforcement authorities in my country is suitable.					
The procedure for replying to requests for non-content data from law enforcement authorities in my country works in practice.					
The procedure for replying to requests for non-content data from law enforcement authorities in my country works in practice.					
The procedure for replying to requests for non-content data from law enforcement authorities in my country provides quick access to the information needed.					
The procedure for replying to requests for non-content data from law enforcement authorities in my country provides legal certainty.					

73. *National system for replying to requests of non-content data from law enforcement authorities in other Member States*

	1 (fully disagree)	2 (disagree)	3 (Not agree nor disagree)	4 (agree)	5 (fully agree)
The procedure for replying to requests for non-content data from law enforcement authorities based in other Member States is suitable.					
Current practices for replying to requests for non-content data from law enforcement authorities from other Member States to investigate/prosecute serious cross-border crime works in practice.					
The procedure for replying to requests for non-content data from law enforcement authorities based in other Member States provides quick access to the information needed.					
The procedure for replying to requests for non-content data from law enforcement authorities based in other Member States provides legal certainty.					

