Data Retention - Questionnaire to Service Providers

Fields marked with * are mandatory.

Background on the initiative

Technological developments and the digitalisation of our societies have led to significant changes in citizens' daily lives and to new challenges for law enforcement and judicial authorities in ensuring a high level of security, at both national and EU level. In today's digital age, almost every criminal investigation has a digital component, with more than 85% of investigations requiring access to digital evidence. Where, in the past, the primary form of evidence collected was physical evidence, nowadays a huge amount of potential evidence is stored by communication providers in the form of **metadata,** also called **non-content data** (such as users' and subscriber information, the source and destination of a message, the location of the device, date, time, duration, size, or another type of interaction that does not include the content of the communications).

To effectively fight and prosecute crimes, the police and judicial authorities may need access to certain of these metadata, as these could be decisive in identifying or locating suspects and/or accused persons, victims, in exculpating suspects and in general in shedding light in general on the commission of an offence. Without specific legal requirements to retain any such data, providers of electronic communications can store such meta data only to the extent the data is necessary for business purposes. In addition, as storage is only justified for as long as needed for business purposes, data requested for the purpose of criminal investigations may no longer be available when needed.

For the purpose of this initiative, data retention refers to the preservation by service providers of certain metadata processed in the context of the communication services that they provide, for a given period of time, to enable access under appropriate safeguards by competent authorities in the case of criminal investigations and to ensure criminal justice ("data retention for law enforcement purposes").

Since 2014, following the decision of the Court of Justice of the European Union to invalidate the EU Data Retention Directive on the grounds of a serious interference with fundamental rights and a lack of specific access safeguards, the EU law does not provide any more for obligations on service providers to retain data for law enforcement purposes.

While these obligations exist in many EU Member States, there are substantial discrepancies among the EU Member States having in place such legislations. As a result, the police and prosecutors face obstacles in conducting their work, as often the necessary data is not or no longer available when the investigation is conducted.

Technological developments also pose new challenges, as end users increasingly substitute traditional communication via voice telephony, text messages (SMS) and electronic mail conveyance services with functionally equivalent services offered in the form of applications running over internet access services

(such as Voice over IP - VoIP, instant messaging services and web-based email services). While these services fall under the scope of EU Electronic Communication Code, these are frequently not covered by national data retention legislations. As a result, metadata pertaining to communications taking place over the internet are particularly difficult to retrieve.

The lack of harmonised measures for the retention of metadata also impacts communication service providers. In the current situation, they might be subject to legal requirements for retention of metadata that differ depending on the Member State where they offer their services, or they have to adapt to frequent changes in national legislations that result from judgements at national and/or EU level. These factors make them face higher costs and obstacles in offering their services across the EU.

The above was of focal importance in the High-Level Group on Access to Data, where experts recommended the adoption of an EU framework on the retention of data for law enforcement purposes, covering also access safeguards. The Political Guidelines of the Commission and Commissioner Brunner's Mission letter and EU Member States (1) (2) recently underscored the need for measures to ensure lawful and effective access to data for law enforcement purposes. In the Communication ProtectEU: a European Internal Security Strategy, the Commission committed to present in 2025 a Roadmap setting out the way forward on lawful and effective access to data for law enforcement and to prioritise an assessment of the impact of data retention rules at EU level.

In the perspective of ensuring the availability of communication metadata for criminal investigations and prosecutions while respecting the EU standards of protection of fundamental rights and the integrity of the EU internal market, the Commission will assess the scope for action at EU level, while respecting the principle of subsidiarity. The present public consultation is intended to feed this assessment - without, however, either prejudging any action by the European Union or prejudging the legal feasibility of an EU action with regards to the limits of the Union's competence.

Terminology

For the purposes of this survey:

Data retention refers to the preservation by service providers of certain types of non-content data (subscriber data, IP, traffic data, location data) processed in the context of the communication services that they provide, for a given period, to enable access under appropriate safeguards by criminal justice authorities for the purpose of investigation and prosecution of crime.

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) or another type of interaction that does not include the content of the communications.

The **categorisation of non-content data** in this survey is based on the data categorisation outlined in Regulation - 2023/1543 (E-evidence Regulation)

Service provider means any natural or legal person that provides one or more of the following categories of services, with the exception of financial services as referred to in Article 2(2), point (b), of Directive 2006

/123/EC of the European Parliament and of the Council:

- electronic communications services as defined in Article 2, point (4), of Directive (EU) 2018/1972;
- internet domain name and IP numbering services, such as IP address assignment, domain name registry, domain name registrar and domain name-related privacy and proxy services;
- other information society services as referred to in Article 1(1), point (b), of Directive (EU) 2015/1535 that:
    - enable their users to communicate with each other; or
    - make it possible to store or otherwise process data on behalf of the users to whom the service is provided, provided that the storage of data is a defining component of the service provided to the user;

Requests for data refer to requests for access to retained data by criminal justice authorities regardless of the channel (i.e. formal cooperation between these authorities or direct cooperation with service providers).

Instructions

You will be asked to reply to a series of questions about the practice in your company/organisation.
Please note that at the end of the questionnaire, you will also able to upload any other document complementing your contribution to this questionnaire.
Thank you in advance for your time in filling this questionnaire!

Privacy Statement

Privacy Statement for Targeted consultation activities organised by the European Commission as part of the impact assessment on retention of data by service providers for criminal proceedings

PROTECTION OF YOUR PERSONAL DATA
Processing operation: Targeted consultation activities (including surveys, interviews and focus groups) for the impact assessment on retention of data by service providers for criminal proceedings
Controller: European Commission, Directorate-General for Migration & Home Affairs, Unit D4
Record reference: DPR-EC-01011

Table of Contents

Introduction
The European Commission (hereafter ‘the Commission’) is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).
This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.
The information in relation to the processing of personal data linked to targeted consultation activities organised by the services of the Commission (Directorate-General for Migration & Home Affairs (hereafter ‘DG HOME’), Unit D4) is presented below.

Why and how do we process your personal data?
Purpose of the processing operation: The Commission collects and uses your personal information within the framework of targeted consultation activities to obtain your views on a specific initiative, policy or intervention.
The targeted consultation activities will support the Commission by providing the necessary evidence to prepare a Staff Working Document on the Impact assessment on retention of data by service providers for criminal proceedings.
You are being contacted by the service of the Commission since it has concluded that your views are relevant and necessary to inform the specific initiative, policy or intervention concerned by the targeted consultation.
The contact details of the prospective respondent that have not been in the possession of the controller /processor and have been solely collected for this targeted consultation activity. The contact details of the prospective respondent that are already in the possession of/processed by the controller/processor and their further processing for the targeted consultation activity is lawful.
Impact Assessment tasks may include:
Holding interviews; Conducting surveys; Organising and executing focus groups; Organizing workshops or experts’ meetings
The targeted consultation will be performed through interviews, surveys, and focus groups. Please note that the interviews will be recorded only with your explicit consent.
Interviews will typically be done online, via phone and/or email exchanges and may require follow-up questions and clarifications. Surveys may be distributed via a specific platform (e.g., EUSurvey) or via email.
For reasons of transparency and openness your views will, in principle, be published on a Europa website, in the form of a summary report.
To avoid misuse, anonymous contributions to the Commission may not be accepted, regardless whether you consent to the publication of your identity together with your contribution.
It is your responsibility if you opt for confidentiality of your personal data to avoid any reference in your submission or contribution itself that would reveal your identity.
The consultation activity may use the Commission's online questionnaire tool EUSurvey that requires you to login via your ‘EU Login’ or ‘social media account’. ‘EU Login’ requires certain personal data such as the name, surname and e-mail address of the registrant. For further information, please refer to the privacy statements of ‘EU Login’ and ‘EU Survey’ as well as the processing operations ‘Identity & Access

Management Service (IAMS)' (reference number in the public DPO register: DPR-EC-03187) and 'EUSurvey' (reference number: DPR-EC-01488). Should you choose to log in through your social media account, please refer to the pertinent social media platform's privacy statement.

Your contribution to the targeted consultations may be stored in the Commission's document management system (for further information on the Commission's document management system please refer to the processing operation 'Management and (short- and medium-term) preservation of Commission documents`, reference number: DPR-EC-00536).
The personal data processed may be reused for the purpose of procedures before the EU Courts, national courts, the European Ombudsman or the European Court of Auditor.
Your personal data will not be used for an automated decision-making including profiling.

On what legal ground(s) do we process your personal data
We process your personal data, because:
(a) processing is necessary for the performance of a task carried out in the public interest;
(c) it is based on your consent, for one or more specified purposes to be contacted by the Commission for the present consultation (in case the respondent had previously consented to be contacted by the Commission for such type of consultation).

The Union law which is the basis for the processing based on Article 5(1)(a) of Regulation (EU) 2018/1725 is the Treaty of the European Union, and more specifically its Articles 1 and 11, Article 298 of the Treaty on the Functioning of the European Union, read in conjunction with Recital 22 of Regulation (EU) 2018/1725), as well as the Protocol 2 on the application of the principles of subsidiarity and proportionality.
Which personal data do we collect and further process?
In order to carry out this processing operation the following categories of personal data may be processed :

name and surname, profession, country of residence, e-mail address of the respondent,the name of a self-employed individual (natural persons) on whose behalf the respondent is contributing,.

Furthermore, you may spontaneously provide other, non-requested personal data in the context of your reply to the targeted consultation.

Please note that the Data Controller does not request nor expect that data subjects provide any special categories of data under Article 10(1) of Regulation 2018/1725 (that is "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation") related to themselves or to third persons in their contributions to the targeted consultation activity. Any spontaneous inclusion of these types of personal data is the responsibility of the data subject and by including any of these types of data the data subject is considered to provide his/her explicit consent to the processing, in accordance with Article 10(2)(a) of Regulation 2018/1725.

If you provide contact information for other potential interviewees, that information will be managed with the same level of care and confidentiality as your own personal data. Please ensure that you inform and get their permission before you share their contact information with us. The potential interviewees will only participate in this exercise if they explicitly consent to do so. If these potential interviewees decline to participate in the consultation, their personal data will be deleted immediately.

How long do we keep your personal data?
The Data Controller only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely for a maximum of five years after the closure of the file to which the present targeted consultation belongs. A file is closed at the latest once there has been a final outcome in relation to the initiative to which the targeted consultation contributed.
This administrative retention period of five years is based on the retention policy of European Commission documents and files (and the personal data contained in them), governed by the common Commission-level retention list for European Commission files SEC(2019)900. It is a regulatory document in the form of a retention schedule that establishes the retention periods for different types of European Commission files. That list has been notified to the European Data Protection Supervisor.
The administrative retention period is the period during which the Commission departments are required to keep a file depending on its usefulness for administrative purposes and the relevant statutory and legal obligations. This period begins to run from the time when the file is closed.
In accordance with the common Commission-level retention list, after the ‘administrative retention period’, files including (the outcome of) targeted consultations (and the personal data contained in them) can be transferred to the Historical Archives of the European Commission for historical purposes (for the processing operations concerning the Historical Archives, please see record of processing 'Management and long-term preservation of the European Commission's Archives’, registered under reference number DPR-EC-00837).
How do we protect and safeguard your personal data?
All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the Commission (or of its contractors (processors) if contractors are engaged to assist the controller). All processing operations are carried out pursuant to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the Commission.
In order to protect your personal data, the Commission has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.
The Commission’s processors (contractors) are bound by a specific contractual clause for any processing operations of your personal data on behalf of the Commission. The processors have to put in place appropriate technical and organisational measures to ensure the level of security, required by the Commission.
Who has access to your personal data and to whom is it disclosed?
Access to your personal data is provided to the Commission staff responsible for carrying out this processing operation and to authorised staff according to the “need to know” principle, in particular to follow-up on the targeted consultation. Such staff abide by statutory, and when required, additional confidentiality agreements.
Certain personal data may be made public on the Europa website, namely:
any personal data on which you consented to their publication; personal data spontaneously provided by you in your contribution (without it being required by the targeted consultation activity).
Please note that pursuant to Article 3(13) of Regulation (EU) 2018/1725 public authorities (e.g. Court of Auditors, EU Court of Justice) which may receive personal data in the framework of a particular inquiry in

accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
What are your rights and how can you exercise them?
You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access your personal data and to rectify them in case your personal data are inaccurate or incomplete. Under certain conditions, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing and the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a), on grounds relating to your particular situation.

Insofar you have consented to the certain processing of your personal data to the Data Controller for the present processing operation, you can withdraw your consent at any time by notifying the Data Controller. The withdrawal will not affect the lawfulness of the processing carried out before you have withdrawn the consent.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.
Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.
In accordance with Article 14(3) of Regulation (EU) 2018/1725, your request as a data subject will be handled within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. In such case you will be informed of the extension of the time limit, together with the reasons for the delay.
Contact information The Data Controller
If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller.
European Commission, Directorate-General for Migration & Home Affairs, Unit D4 , Security in the Digital Age, at home-data-retention@ec.europa.eu The Data Protection Officer (DPO) of the Commission
You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu)) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.
Where to find more detailed information?
The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: http://ec.europa.eu/dpo-register.
This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-01011.

General questions

* You are:

- Provider of electronic communications services (such as traditional voice telephony/voice communications services and text messages/SMS)
- Provider offering number-independent interpersonal communications services - such as voice over IP (VoIP), instant messaging and electronic mail services, etc
- Internet Service Provider
- Provider of services consisting wholly or mainly of the conveyance of signals, such as transmission services used for M2M communications and for broadcasting signals
- Provider of information society services that provide editorial control over content transmitted using electronic communication services (such as X or Facebook)
- Provider of cloud services
- Digital marketplace
- Provider of internet infrastructure services (such as IP addresses and domain name registries and registrars)
- Hosting service provider
- Other

If other, please specify:

200 character(s) maximum

* How big is your company (number of employees)?

- Less than 100
- Between 101 and 999
- Between 1000 and 4999
- Between 5000 and 249,999
- More than 250,000

* Your contribution

- can be published with your organisation's information (I consent the publication of all information in my contribution in whole or in part including the name of my organisation, and I declare that nothing within my response is unlawful or would infringe the rights of any third party in a manner that would prevent publication)
- can be published provided that your organisation remains anonymous (I consent to the publication of any information in my contribution in whole or in part (which may include quotes or opinions I express) provided that it is done anonymously. I declare that nothing within my response is unlawful or would infringe the rights of any third party in a manner that would prevent the publication.

Note that, whatever option chosen, your personal data (name etc.) will not be published. Your answers, excepting personal data, may be subject to a request for public access to documents under Regulation (EC) N°1049/2001.

Processing of non-content data in your company

Which of the following **subscribers' data** do you process (pick the options that apply to your organisation):

	Generate /handle	Generate /handle and store for your business purposes	Generate /handle and store due to legal obligations	Do not generate /handle
* Name	○	○	○	○
* Date of birth	○	○	○	○
* Postal or geographic address	○	○	○	○
* E-mail address	○	○	○	○
* Phone number or provided by the subscriber at the moment of initial registration or activation	○	○	○	○
* Date and time of initial registration	○	○	○	○
* Type of registration	○	○	○	○
* Copy of a contract	○	○	○	○
* Means of verification of identity at the moment of the registration	○	○	○	○
* Copies of documents provided by the subscriber (such as ID documents)	○	○	○	○
* Type of service (ADSL, WiFi, VoIP, cable, 3G, 4G)	○	○	○	○
* Duration of the service	○	○	○	○

* Phone number used by the subscriber at the moment of initial registration or activation				
* Associated device identification numbers (serial number, IMEI, MAC)				
* IP address at signup				
* SIM number used or provided by the subscriber at the moment of initial registration or activation				
* Billing and payment information (bank account, credit card number etc.) records				
* PUK codes				
* Other relevant information pertaining to the identity of the user/subscription holder (please specify under “other” below)				

If your company generates/handles other relevant information pertaining to the identity of the user /subscription holder, please specify:

Which of the following **traffic data related to outgoing communication** do you process (pick the options that apply to your organisation):

	Generate /handle	Generate /handle and store for your business purposes	Generate /handle and store due to legal obligations	Do not generate /handle
* (For mobile telephony services) phone number, IMSI, IMEI, Bearer /teleservice used (e.g. UMTS, GPRS)	○	○	○	○
* (For internet services) Source IP address, port number(s), browser, email header information, message ID	○	○	○	○
* (For hosting services) Logfiles, Tickets	○	○	○	○
* Call attempts (including number of rings of missed calls)	○	○	○	○
* Connection to the relevant service	○	○	○	○
* Disconnection from relevant service	○	○	○	○
* Duration of the communication /connection or access session	○	○	○	○
* Data volume of the electronic communication	○	○	○	○
* Type of communication (voice, SMS, email, chat, forum, social media)	○	○	○	○
* Type of the relevant service (ADSL, WiFi, VoIP, cable, 3G, 4G).	○	○	○	○

Which of the following **traffic data related to incoming communication** do you process (pick the options that apply to your organisation):

	Generate /handle	Generate /handle and store for your business purposes	Generate /handle and store due to legal obligations	Do not generate /handle
* Identifiers of the account, device or relevant service to which the communication has been sent	○	○	○	○
* Identifiers of the account, device or relevant service to which the communication has been forwarded, routed or transferred	○	○	○	○
* Identifiers of the account, device or relevant service to which the communication has been attempted to be forwarded, routed or transferred	○	○	○	○

Which of the following **location data** do you process (pick the options that apply to your organisation):

	Generate /handle	Generate /handle and store for your business purposes	Generate /handle and store due to legal obligations	Do not generate /handle
* Base station ID, including geographical information (X/Y) of the terminal equipment or line at the **start** of the communication (cell towers, wifi hotspots)	○	○	○	○
* Base station ID, including geographical information (X/Y) of the terminal equipment or line at the **end** of the communication (cell towers, wifi hotspots)	○	○	○	○

If your organisation processes any other non-content data not specified above, please describe:

What is the normal retention period at your company for business purposes for **subscribers' data**?

	Retention period (please specify duration, or insert N/A if your company does not generate/handle such data)
Name	
Date of birth	
Postal or geographic address	
E-mail address	
Phone number	
Date and time of initial registration	
Type of registration	
Copy of a contract	
Means of verification of identity at the moment of the registration	
Copies of documents provided by the subscriber (such as ID documents)	
Type of service (ADSL, WiFi, VoIP, cable, 3G, 4G)	
Duration of the service	
Phone number used by or provided by the subscriber at the moment of initial registration or activation	
Associated device identification numbers (serial number, IMEI, MAC)	
IP address at signup	
SIM number used or provided by the subscriber at the moment of initial registration or activation	
Billing and payment information (bank account, credit card number etc.) records	
PUK codes	

If your company generates/handles other relevant information pertaining to the identity of the user /subscription holder for business purposes, please specify both their nature and applicable retention period:

What is the normal retention period at your company for business purposes for **traffic data related to outgoing communication**?

	Retention period (please specify duration, or insert N/A if your company does not generate/handle such data)
(For mobile telephony services) phone number, IMSI, IMEI, Bearer/teleservice used (e.g. UMTS, GPRS)	
(For internet services) Source IP address, port number(s), browser, email header information, message ID	
(For hosting services) Logfiles, Tickets	
Call attempts (including number of rings of missed calls)	
Connection to the relevant service	
Disconnection from relevant service	
Duration of the communication/connection or access session	
Data volume of the electronic communication	
Type of communication (voice, SMS, email, chat, forum, social media)	
Type of the relevant service (ADSL, WiFi, VoIP, cable, 3G, 4G).	

What is the normal retention period at your company for business purposes for **traffic data related to incoming communication**?

	Retention period (please specify duration, or insert N/A if your company does not generate/handle such data)
(For mobile telephony services) phone number, IMSI, IMEI, Bearer/teleservice used (e.g. UMTS, GPRS)	
(For internet services) Source IP address, port number(s), browser, email header information, message ID	
(For hosting services) Logfiles, Tickets	
Call attempts (including number of rings of missed calls)	
Connection to the relevant service	
Disconnection from relevant service	
Duration of the communication/connection or access session	
Data volume of the electronic communication	
Type of communication (voice, SMS, email, chat, forum, social media)	
Type of the relevant service (ADSL, WiFi, VoIP, cable, 3G, 4G).	

What is the normal retention period at your company for business purposes for **location data**?

	Retention period (please specify duration, or insert N/A if your company does not generate/handle such data)
Base station ID, including geographical information (X/Y) of the terminal equipment or line at the **start** of the communication (cell towers, wifi hotspots)	
Base station ID, including geographical information (X/Y) of the terminal equipment or line at the **end** of the communication (cell towers, wifi hotspots)	

If your organisation processes any other non-content data not specified above, please describe and specify the applicable retention period for business purposes:

Does the table below reflect the way you categorise non-content data?

- Yes
- No

Data needed to identify a person (subscriber or user)	Data needed to identify a terminal equipment (means of communication)	Data needed to identify a location (origin and destination) of communication and/or device (terminal equipment)	Data needed to identify the time and/or the duration of the communication	Data needed to identify the network/service used

* If not, how do you categorise non-content data? Please explain and/or attach any relevant documents below

Please upload your file(s)

Legal requirements applicable to your company on data retention

* Do you operate in one or multiple Member States?
  - One
  - Multiple

* In this Member State, which of the following applies:
  - Data Retention legislation for law enforcement purposes is in place
  - Data Retention legislation for law enforcement purposes is not in place

* In those Member States in which you operate, which of the following applies:
  - None of them have data retention legislation in place
  - One or more has no data retention legislation, but the others do
  - All Member States where you operate have data retention rules, but they are different e.g. in terms of the data retained, retention periods, the providers concerned etc.
  - Data retention rules are applicable in all the Member States where you operate, with the same requirements

* If you operate in Member States with different requirements, please elaborate on the existing differences between the legal regimes (g. data categories, retention periods, providers concerned, targeted retention, etc.)

1500 character(s) maximum

* Please elaborate on the main challenges, if any, that you encounter as a result of the situation applicable to you:

1500 character(s) maximum

If you operate in Member States with different requirements, do you experience a conflict of laws? Please elaborate below if this is the case.

1500 character(s) maximum

* In 2014 the Court of Justice of the EU invalidated the legal instrument that regulated data retention at EU level.

Have you had to adapt your system since to align with new national requirements?

- Yes
- No
- Not applicable

* If yes, did you set up specific procedures to develop and implement the technical requirements?

- ( ) Yes
- ( ) No

* If yes, did you implement any of the following measures? (pick those that apply to you):

- [ ] You recruited extra staff
- [ ] You created separate storing systems
- [ ] You created a new access system
- [ ] You had to set up new technical communication channels
- [ ] Other

If other, please elaborate:

250 character(s) maximum

* Can you elaborate and/or quantify the implementation costs, if any?

250 character(s) maximum

* Can you elaborate/quantify on the recurrent costs, if any?

250 character(s) maximum

If the national legislation under which you are operating provides for retention requirements targeted to specific categories of persons or geographic areas, please elaborate on the technical aspects for the implementation of these requirements.

- For retention based on geographic criteria: cell coverage precision, user moving from one cell to another, roaming, etc

500 character(s) maximum

- For retention based on **categories of persons**: practical application to the communications of the users subject to the measure:

500 character(s) maximum

- Other criteria / other aspects you wish to raise:

500 character(s) maximum

If the national legislation under which you are operating foresees the exclusion of certain categories of persons subject to professional privilege or confidentiality (doctors, lawyers, social workers, journalists, parliamentarians…), please elaborate on the technical implementation of these requirements, and in particular the practical application to the communications of the users excluded by the measure:

500 character(s) maximum

If the national legislation(s) under which you are operating require you to retain data for longer periods than you would need for your business purposes:

- Can you specify how much longer the retention obligation is compared to your needs?

500 character(s) maximum

- Can you estimate the difference in terms of volume compared to your business needs?

500 character(s) maximum

- Can you estimate the marginal costs of retaining such data?

500 character(s) maximum

If the national legislation(s) under which you are operating require you to retain more data than those that you would need for your business purposes:

- Can you estimate the difference in terms of volume compared to your business needs?

500 character(s) maximum

- Can you estimate the marginal costs of retaining such data?

500 character(s) maximum

If you are operating in multiple Member States where national legislations provide for different retention obligations, how do you apply the different requirements (for example, in case of differences in retention periods, do you apply different retention periods depending on the origin of the data) ? Please elaborate, providing examples applicable to your case.

1500 character(s) maximum

* Do you keep separate databases for data retained for business and for law enforcement purposes?

- Yes
- No
- Not applicable

* If yes, does this stem from legal obligations or business choices?

250 character(s) maximum

If this affects costs, can you quantify them?

500 character(s) maximum

* Which security measures (e.g. encryption, anonymization, deletion, localisation or other measures to protect data against unauthorised access, misuse etc) do you apply to the different categories of data you generate and process? Please elaborate:

500 character(s) maximum

* Is there a difference in the level of security measures applied to data retained for business purposes and data retained for law enforcement purposes?

- Yes
- No
- Not applicable

* If yes, are such differences applied by mandatory requirements or based on business choices? Please elaborate:

500 character(s) maximum

Cooperation with Public Authorities

* Is your organisation part of voluntary cooperation mechanisms with public authorities (such as Memoranda of Understanding, participation to EU platforms such as SIRIUS, exchanges of best practices) for the purpose of facilitating access to data?

- ○ Yes
- ○ No
- ○ Not applicable

* If yes, please elaborate on such forms of cooperation:

500 character(s) maximum

* If no, please elaborate on the reasons:

500 character(s) maximum

* Does your company issue transparency reports on the practice of cooperation with public authorities in the context of access to data for criminal justice purposes?

- ○ Yes
- ○ No

* If no, please specify the reasons why:

- ☐ Reputational risks towards consumers (lack of trust)
- ☐ Lack of records
- ☐ Lack of resources
- ☐ Other

If other, please specify:

500 character(s) maximum

* Do you have specific procedures in place to receive and respond to requests for access to data from public authorities?

- ○ Yes

- ○ No
- ○ Not applicable

* If yes, please elaborate on such practices:

500 character(s) maximum

* Do you have a department, legal entity or a point of contact in your organisation dedicated to the cooperation with public authorities?

- ○ Yes
- ○ No

* If not, please elaborate on the reasons:

500 character(s) maximum

* Do you have procedures in place to verify the authenticity of the requests of public authorities?

- ○ Yes
- ○ No
- ○ Not applicable

* If yes, can you elaborate on your practices?

500 character(s) maximum

* In case your business rejected or complied only partially with requests for access to non-content data, what were the reasons?

- ☐ The request did not fulfil the legal requirements
- ☐ The request was not put forward via the company's forms or standards
- ☐ It was not possible to execute the request because the data sought was not available anymore
- ☐ You considered that you were not bound by the request
- ☐ It was not possible to execute the request because the data category sought is not retained
- ☐ Others

☐ Not applicable

* If others, please specify:

250 character(s) maximum

* Can you quantify the above cases?

250 character(s) maximum

Access to non-content data

* Has your company ever been requested by a prosecutor, judge, independent administrative authority or law enforcement to access non-content data for the purpose of a criminal investigation?

○ Yes
○ No

* If yes, how many such requests have you received in the last 12 months?

100 character(s) maximum

* Please elaborate, for the last 12 months:

- The main purposes / types of crimes for which the requests were made:

500 character(s) maximum

*

- The percentage which were emergency disclosure requests:

100 character(s) maximum

*

- The percentage of requests pertaining to missing persons:

100 character(s) maximum

*

- The percentage of requests targeted to a specific person/s, versus 'bulk requests' (e.g. all data of all persons at one location within a certain radius of a crime scene or range of a cell phone tower):

100 character(s) maximum

*

- The average "age" of the requested data (how old the data was at the time of the initial request):

100 character(s) maximum

Over the last 12 months, please specify which types of **subscribers' data** have been requested by public authorities for the purposes of law enforcement purposes. If possible, please specify to what percentage these amount to out of the total of all requests received:

Name	* Yes Yes No No	Percentage: *Only values between 0 and 100 are allowed* %
Date of birth	* Yes No	Percentage: *Only values between 0 and 100 are allowed* %
Postal or geographic address	* Yes No	Percentage: *Only values between 0 and 100 are allowed* %
E-mail address	* Yes No	Percentage: *Only values of at most 100 are allowed* %
		Percentage:

Phone number	* Yes No	*Only values of at most 100 are allowed* %
Date and time of initial registration	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Type of registration	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Copy of a contract	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Means of verification of identity at the moment of the registration	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Copies of documents provided by the subscriber (such as ID documents)	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Type of service (ADSL, WiFi, VoIP, cable, 3G, 4G)	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Duration of the service	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Phone number used by or provided by the	*	Percentage: *Only values of at most 100 are allowed*

subscriber at the moment of initial registration or activation	Yes No	%
Associated device identification numbers (serial number, IMEI, MAC)	* Yes No	Percentage: *Only values of at most 100 are allowed* %
IP address at signup	* Yes No	Percentage: *Only values of at most 100 are allowed* %
SIM number used or provided by the subscriber at the moment of initial registration or activation	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Billing and payment information (bank account, credit card number etc.) records	* Yes No	Percentage: *Only values of at most 100 are allowed* %
PUK codes	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Other relevant information pertaining to the identity of the user/subscription holder (please specify under “other” below)	* Yes No	Percentage: *Only values of at most 100 are allowed* %

If others, please specify:

250 character(s) maximum

Over the last 12 months, please specify which types of **traffic data related to outgoing communication** h ave been requested by public authorities for the purposes of law enforcement purposes. If possible, please specify to what percentage these amount to out of the total of all requests received:

(For mobile telephony services) phone number IMSI IMEI Bearer/teleservice used (e.g. UMTS, GPRS)	* ○ Yes ○ No	Percentage: *Only values between 0 and 100 are allowed* %
(For internet services) Source IP address, port number(s), browser, email header information message ID	* ○ Yes ○ No	Percentage: *Only values between 0 and 100 are allowed* %
(For hosting services) Logfiles Tickets	* ○ Yes ○ No	Percentage: *Only values between 0 and 100 are allowed* %
Call attempts (including number of rings of missed calls)	* ○ Yes ○ No	Percentage: *Only values of at most 100 are allowed* %
Connection to the relevant service	* ○ Yes ○ No	Percentage: *Only values of at most 100 are allowed* %
Disconnection from relevant service	* ○ Yes ○ No	Percentage: *Only values of at most 100 are allowed* %
Duration of the communication/connection or access session	* ○ Yes ○ No	Percentage: *Only values of at most 100 are allowed* %
Data volume of the electronic communication	* ○ Yes	Percentage: *Only values of at most 100 are allowed*

	No	%
Type of communication (voice, SMS, email, chat, forum, social media)	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Type of the relevant service (ADSL, WiFi, VoIP, cable, 3G, 4G).	* Yes No	Percentage: *Only values of at most 100 are allowed* %
Type of service (ADSL, WiFi, VoIP, cable, 3G, 4G)	* Yes No	Percentage: *Only values of at most 100 are allowed* %

Over the last 12 months, please specify which types of **traffic data related to incoming communication** h ave been requested by public authorities for the purposes of law enforcement purposes. If possible, please specify to what percentage these amount to out of the total of all requests received:

Identifiers of the account, device or relevant service to which the communication has been sent	* Yes No	Percentage: *Only values between 0 and 100 are allowed* %
Identifiers of the account, device or relevant service to which the communication has been forwarded, routed or transferred	* Yes No	Percentage: *Only values between 0 and 100 are allowed* %
Identifiers of the account, device or relevant service to which the communication has been attempted to be forwarded, routed or transferred	* Yes No	Percentage: *Only values between 0 and 100 are allowed* %

Over the last 12 months, please specify which types of **location data** have been requested by public authorities for the purposes of law enforcement purposes. If possible, please specify to what percentage these amount to out of the total of all requests received:

		Percentage:

Base station ID, including geographical information (X/Y) of the terminal equipment or line at the start of the communication (cell towers, wifi hotspots)	* Yes No	*Only values between 0 and 100 are allowed* %
Base station ID, including geographical information (X/Y) of the terminal equipment or line at the end of the communication (cell towers, wifi hotspots)	* Yes No	Percentage: *Only values between 0 and 100 are allowed* %

Over the last 12 months, please specify if there were **other types of non-content data** requested by public authorities for the purposes of law enforcement purposes. If possible, please specify to what percentage these amount to out of the total of all requests received:

Other types of non-content data	* Yes No	Percentage: *100 character(s) maximum*

If others, please specify:

250 character(s) maximum

* Do any law enforcement authorities have direct access to data retained by your company for law enforcement purposes?

- Yes
- No
- Don't know

* Do you receive requests for data older than your mandatory retention period?

- Yes
- No

If yes, can you quantify the percentage compared to the overall amount of requests?

Costs

If you incur costs when you store data for longer periods due to the duration of the retention do you (select one):

- bear them

- receive a forfeit compensation
- charge per request received
- N/A

Can you estimate the marginal costs of retaining such data for longer periods?

250 character(s) maximum

If you incur costs when you provide access to public authorities (select one):

- bear them
- receive a forfeit compensation
- charge per request received
- N/A

* Can you estimate the cost of providing non content data following a request by public authorities?

250 character(s) maximum

Future measures

* Do you expect that the harmonisation of the practices of data retention for criminal justice purposes by a legislative measure at EU level could lead to a reduction of your current compliance costs for your operations across the EU?

- Yes
- No

* Can you quantify the expected reduction of costs, if any?

250 character(s) maximum

* Do you expect additional costs resulting from a harmonisation of the practices of data retention for law enforcement purposes by a legislative measure at EU level?

- Yes
- No

If yes, please indicate where you would expect these additional costs to stem from:

- You will need to recruit extra staff
-

You will need to create separate storing systems

- [ ] You will need to create a new access system
- [ ] You will need to set up new technical communication channels
- [ ] Other

If others, please specify:

150 character(s) maximum

Can you quantify the expected implementation costs, if any?

250 character(s) maximum

Can you quantify the expected recurrent costs, if any?

250 character(s) maximum

* Do you expect that the harmonisation of the practices of data retention for criminal justice purposes by a legislative measure at EU level could lead to more legal certainty with regard to the obligations and safeguards on data retention? Please elaborate your answer:

1500 character(s) maximum

* Looking at future technologies, can you elaborate on the evolution that you see in the business model of your organisation regarding data processing of 'identification/subscription' and traffic and location data?

1500 character(s) maximum

Do you have any other issue that you wish to raise in the context of this consultation? Please elaborate.

You may attach contributions or other relevant documents below

1500 character(s) maximum

Please upload your file(s)

Free Text Question