Meeting with civil society

on experiences and challenges of data retention

6 June 2019, Brussels

European Commission - DG HOME

As part of a fact-finding exercise, the Commission is engaging with a wide range of stakeholders from the public and private sectors, including civil society, with operational, legal and technical expertise on data retention of non-content communication data. The aim is to fill knowledge gaps and gather information about the various aspects of data retention, from both a national and cross-border perspective.

The objective of the meeting is to get a better understanding about the impact of access to communications metadata (traffic, location, IP and subscriber data) by the law enforcement authorities in criminal investigations and prosecutions. The meeting will focus on the technical and operational possibilities and constraints and the appropriate safeguards in light of the requirements on both the retention and the access conditions set by the Court of Justice in its case law.

The aim of this non-paper it to provide a general framework for discussion during the meeting. This paper is not intended to be comprehensive; participants are encouraged to raise other relevant issues during the meeting. Written answers to these questions are not expected for the meeting. Participants are, however, invited to supplement their views and responses by quantitative or statistical data as much as possible.

1. What is the function and impact on individuals (both the users of communication services and the victims of crime) and/or society of data retention frameworks?

- Are there any analyses on the implications for individuals and/or society of the existing or planned national data protection regimes?

- Are there any existing analyses about the impact on the behaviour of persons concerned by retention of their communications data?

- Is there any available empirical information about actual abuse or misuse of data retained? Are you aware about any relevant court cases at the national level on this issue?

- Are there any analyses regarding the investigative or judicial outcome of using the data? Are there any evaluations, reports, statistics or studies on the subject available?

- Is it be possible to quantify and evaluate the *volumes* of data that are retained in different Member States?

- Is it possible to quantify and evaluate the amount of data requested and/or accessed by law enforcement authorities in different Member States in accordance with their data retention legislation?

- Is it possible to identify the data categories retained by the telecom operators for their business purposes (independently of data retention obligations)?

- What are the cross-border implications of data retention laws? Would an EU-wide data retention regime bring any added value? If so, what should it regulate?

2. How to design a data retention regime compatible with fundamental rights?

- Targeted retention: What are the risks for fundamental rights of such regimes, in particular regarding discrimination? How should the targeting criteria (i.e. predefined persons or geographical areas) be designed?

- Conversely, how should/could the retention of data of certain persons subject to professional privilege or confidentiality (doctors, lawyers, social workers, journalists, parliamentarians…) be excluded?

- What is the impact on the fundamental rights of the retention of specific categories of data, in light of evolutions in technology and criminal behaviour (i.e. internet telephony, end-to-end encryption, 5G)? How can this be minimised?

- How does the length of the retention period influence the interference with fundamental rights?

- Which authorities should be authorised to access these data to minimise the impact on fundamental rights?

- For what purposes should access be granted? In particular, in relation to what types of crimes should it be possible to access and use stored telecommunications data?

- What safeguards should be in place to ensure that data is stored and used only where it is strictly necessary and for predefined purposes? How should the risks of personal data and privacy breaches be minimised throughout the process of storage and handover by providers and use by authorities? *We would like to discuss here in particular ex-ante authorisation procedures, notifications to data subjects, data subject rights, remedies and ex-post supervision.*

- Are there any alternatives to data retention that could be equally effective in fighting crime and be more respectful of fundamental rights?