Background document

High-Level Group on Access to Data for Effective Law Enforcement

Working Group 2

Access to Data
at Rest in a Provider's System

6 September 2023

Introduction

The European Union constitutes an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States,[1] and endeavours to ensure a *high level of security* through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws.[2]

In recent years, the European Council, the Council[3], other EU institutions[4] and agencies have on several occasions discussed and formulated conclusions on various legal and policy aspects of access to electronic communications data, including metadata, and more generally, to electronic evidence. In its conclusions of 22–23 June 2017,[5] the European Council already called for "addressing the challenges posed by systems that allow terrorists to communicate in ways that competent agencies cannot access, including end-to-end encryption, while safeguarding the benefits these systems bring for the protection of privacy, data and communication" and highlighted that "effective access to electronic evidence is essential to combating serious crime and terrorism". The EU Strategy to tackle Organised Crime 2021–2025 also stresses the importance of access to electronic communications data to tackle organised crime, making "law enforcement and the judiciary fit for the digital age." [6] Access to data is also of key importance for all EMPACT priorities in the fight against serious and organised crime for 2022–2025.[7]

In today's digital age, almost every criminal investigation has a digital component, as growing number of crimes occur solely online while access to data for law enforcement is needed in relation to most, if not all crimes. At the same time, any objective of enhancing security in the digital age for the purposes of effective law enforcement, must be pursued in full compliance with fundamental rights, in full respect of the EU Charter for Fundamental

[1] *The Treaty on The Functioning of the European Union* (TFEU), Article 67, para 1.
[2] *Ibid.*, para 3.
[3] Doc. no. 8289/1/16, *Council conclusions on improving criminal justice in cyberspace.*
[4] OJ 2018/C 346/29, Eur*opean Parliament resolution of 3 October 2017 on the fight against cybercrime.*
[5] Doc. EUCO 8/17.
[6] *Communication from the Commission on the EU Strategy to tackle Organised Crime 2021–2025,* COM/2021/170 final of 14 April 2021.
[7] Doc.no. 8665/21.

Rights, and fundamental rights proscribed therein, as interpreted by the Court of Justice of the European Union.

In the March 2023 *Lisbon Declaration*,[8] the European Police Chiefs expressed their particular concern about the national and international impact of the lack of clarity regarding data retention at the EU level for traffic and location data that affect not only the accomplishment of their missions but the whole of the society, bringing into question the impact on citizens' rights, freedoms and guarantees and, consequently, on the democratic rule of law since some types of crimes can only be prevented and investigated if non-content data retention is allowed.

Taking stock

In view of the above, as the first step, the Working Group 2 will take stock of the current situation, namely by inviting law enforcement practitioners to present their success stories, but also their failures to overcome certain obstacles and challenges.

Accordingly, the members of the Working Group 2 are invited to contribute in written a typical case scenario for access to data at rest in a provider's system, as well as to indicate challenges and capacity gaps that law enforcement authorities face or will face in the foreseeable future regarding access to data at rest in a provider's system, in particularly those that have effect on effective law enforcement.

In their contributions, members are free to consult the questions below.
In their analysis, participants should take into account the recently adopted e-evidence package and focus on challenges and gaps that will not be addressed by the new rules.

The cases should be submitted by 28 August 2023 to the following e-mail: EC-HLG-GOING-DARK@ec.europa.eu with the subject: ***Cases Working Group 2.***

While submitting, please indicate whether you would be interested in presenting the submitted case and/or identified challenges at the Working Group 2 meeting on 6 September 2023.

[8] *Joint Declaration of the European Police Chiefs (Lisbon Declaration)*, March 2023; available at: Joint-Declaration-of-the-European-Police-Chiefs-Lisbon-Declaration.pdf (policiajudiciaria.pt).

Discussion questions

The presentations will be followed by a discussion based on the following questions:

Morning session

1. *In which types of cases, and at which point in time, law enforcement authorities must access data at rest in a provider's system, in order for those cases to be effectively prevented, detected and investigated? What is the practitioners' experience with their national data retention regimes?*
2. *In such cases, which categories of data appear to be absolutely necessary in order to effectively investigate and prosecute criminal offences? Which type of providers are of particular relevance in such cases?*
3. *For which types of cases law enforcement authorities do not need access to data at rest in a provider's system?*

Afternoon session

1. *Are there any technical and legal challenges or capacity gaps that law enforcement authorities face or will face in the foreseeable future regarding access to data at rest in a provider's system? If so, what are these challenges concretely?*
2. *What are the alternatives to access to data at rest in a provider's system?*
3. *Do the alternatives address the challenges identified above, and how intrusive are they?*
4. *Do any of these challenges identified influence bringing justice to the victims of crimes? If so, in what way concretely?*
5. *Do any of those challenges identified influence cross-border or international police and judicial cooperation? If so, in what way concretely?*
6. *Would you consider any of these challenges to be insurmountable for law enforcement authorities? If yes, why? And how big a role these challenges play overall in criminal investigations in general and in the overall accomplishment of EU LEAs missions?*