Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement

Adopted on 4 November 2024

The European Data Protection Board has adopted the following statement:

In June 2023 the High-Level Group on Access to Data for Effective Law Enforcement ('HLG') was launched by the Presidency of the Council and the European Commission to explore "*challenges that law enforcement practitioners in the Union face in their daily work in connection to access to data"* and to *"identif[y] potential solutions and recommendations to overcome them, with the aim of ensuring the availability of effective law enforcement tools to fight crime and enhance public security in the digital age*".[1] The HLG has focused on three use-cases: access to data at rest in a user's device, access to data at rest in a service provider's system and real time access to communication data, each of which has been discussed in a dedicated working group [2].

One year later the HLG identified 42 'Recommendations' for the further development of Union policies and legislation, structured as "Capacity Building measures", "Cooperation with Industry and Standardisation" and "Legislative measures".

Although the recommendations are yet to "*be operationalised and will undergo an assessment of legal, technical and financial feasibility […], in a second phase, with a view to providing a concluding report in autumn 2024*"[3], the EDPB wishes to contribute to the discussion of the report by sharing preliminary, non-exhaustive concerns, as some of the recommendations appear to imply significant interferences with the right to data protection and the respect for private and family life.

[1] See p. 3 of the Recommendations.
[2] See p. 5 of the Recommendations.
[3] See p. 5 of the Recommendations.

1 GENERAL REMARKS

One of the consequences of the rapid digitalisation of almost all aspects of our life is the ongoing debate about the access to electronic data for law enforcement and criminal justice purposes. In this context, data protection experts have repeatedly warned against granting law enforcement excessive capacities that in some cases may amount to mass surveillance and cause serious interference with fundamental rights. This concerns in particular the recommendations addressing data retention (see Section 2) and data security and encryption (see Section 3). At the same time, the EDPB recognizes the need to strike the necessary balance between the rights and interests at issue, in order, among others, to avoid actual impunity of perpetrators of certain criminal offences, especially those committed online, as the Court of Justice has recently pointed out[4].

In that regard, the EDPB welcomes that the Recommendations reaffirm that any proposed measure should be "in full compliance with data protection and privacy rules[5]" and recalls that access to data should only be granted in the context of criminal investigations, on a case-by-case basis, and should in principle be subject to judicial authorisation[6].

The EDPB is however concerned by the fact that the Recommendations are not complemented and supported by objective evidence, including, where relevant, statistics. Evidence is of particular importance given that, for example, an analysis by the European Parliament's Research Service shows no measurable effect of data retention on crime rates or crime clearance rates in EU Member States with such regimes in place.[7] The lack of measurable data makes it difficult to assess the necessity and proportionality of certain proposed measures, as provided for by Article 52(1) of the Charter of Fundamental Rights of the EU as well as their effectiveness in practice.

2 DATA RETENTION

The EDPB is aware that, throughout the years, data retention has been the subject of numerous debates within the European Union. These discussions clearly show the complexity of the subject and the difficulty in finding the right balance between the need to protect individuals against modern forms of electronic surveillance on the one hand, and on the other hand, the necessity to use technology in criminal investigations.

The EDPB, therefore, positively notes the intention expressed in the Recommendations to establish a harmonised EU regime on data retention[8], thus creating a level playing field and legal certainty in the interest of all stakeholders, in full compliance with the CJEU jurisprudence.

---

[4] See Judgment of the Court of Justice of 30 April 2024, La Quadrature du Net and Others, Case C-470/21, ECLI:EU:C:2024:370, paragraphs 116 and 117 and of 4 October 2024, Bezirkshauptmannschaft Landeck, C-548/21, ECLI:EU:C:2024:830, paragraph 97.

[5] See recommendation 27 point (vi).

[6] See p. 2 of the Recommendations.

[7] European Parliamentary Research Service (EPRS), General data retention / effects on crime, available here: https://www.patrick-breyer.de/wp-content/uploads/2020/10/EPRS_103906-_General_data_retention___effects_on_crime_FINAL.docx .

[8] See first sentence of recommendation 27.

However, the EDPB has specific concerns about the recommendation suggesting that the scope of a future EU harmonised regime on retention and access should cover 'present and future "data handlers" (i.e. service providers of any kind that could provide access to e-evidence)' [9].

At present, the scope of data retention regimes is generally confined to the provision of publicly available electronic communications services[10] in public communications networks. Recommendation 27 seems to align retention obligations with access to data possibilities provided by the new e-Evidence Regulation, which has a broad scope with regards to what should be considered as e-evidence for the purposes of production and preservation orders[11].

The EDPB would like to recall that the personal and material scope of any future EU legal framework on retention of and access to personal data is one of the key elements for the assessment of the necessity and proportionality of the proposed regime. In that regard, the CJEU has already stated that general and indiscriminate retention of all traffic data is, in principle, prohibited and can be justified solely on the basis of the protection of national security, if the Member State concerned is faced with a serious threat to national security that can be categorised as real and actual or foreseeable[12]. Against this background, the EDPB considers that a broad and general obligation to retain data in electronic form by all 'present and future "data handlers" (i.e. service providers of any kind that could provide access to any e-evidence)' would extend the personal and material scope of data retention beyond the guardrails established in the aforementioned case-law and would thus be highly problematic. Such recommendation could lead to an almost horizontal obligation for providers of information society services of any kind to retain electronic data and may cause a situation of widespread surveillance. It is difficult to imagine how such a legal regime would meet the requirements of necessity and proportionality of the Charter of Fundamental Rights of the EU and the CJEU jurisprudence.

With respect to the recommendation for the "establishment at the very least of an obligation for companies to retain data sufficient to ensure that any user can be clearly identified (e.g., IP address and port number)"[13], the EDPB acknowledges that the recent judgment of the CJEU in the Hadopi case[14] does indicate that, under certain circumstances, the general retention of IP addresses assigned to the source of an internet connection, as well as of data relating to the civil identity of users of means of electronic communication may be lawful. The Court has clarified that general and indiscriminate retention of IP addresses does not necessarily constitute a serious interference with fundamental rights and could be permissible under EU law for fight against any type of crime. However, this

[9] See recommendation 27 point (ii).

[10] Electronic communication services are defined in Directive (EU) 2018/1972 establishing the European Electronic Communications Code (EECC) and include also inter-personal communications services such as voice-over-IP, instant messaging and email services.

[11] E-Evidence Regulation applies not only to providers of electronic communications services but also to specific providers of information society services that do not qualify as electronic communications service providers but offer their users the ability to communicate with each other (e.g. online marketplaces providing consumers and businesses with the ability to communicate with each other, online gaming platforms, online gambling platforms, etc.), or offer their users services that can be used to store or otherwise process data on their behalf.

[12] See Judgment of the Court of Justice of 6 October 2020, La Quadrature du Net and Others, Joined Cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, paragraph 137.

[13] See point (v) of the recommendation 27.

[14] Judgment of the Court of Justice of 30 April 2024, La Quadrature du Net and Others, Case C-470/21, ECLI:EU:C:2024:370.

assessment by the Court is strictly limited to cases where it is genuinely ruled out that that retention could give rise to serious interferences with the private life of the person concerned due to the possibility of drawing precise conclusions about that person. Accordingly, any combination of those IP addresses with other retained data, which would allow precise conclusions to be drawn about the private life of the persons whose data are thus retained, must be genuinely ruled out[15].

The EDPB would like to emphasise that the Court's reasoning, justifying the retention of IP addresses in a general and indiscriminate way can in no way be automatically extended to other (more sensitive) traffic and location data, which could easily enable a more detailed profile of the user to be produced.

3 DATA SECURITY AND ENCRYPTION

In its Recommendations, the HLG makes several mentions of encryption as a "challenge" with regard to the need to allow for lawful access to be put in place. This topic is addressed by several specific recommendations, covering the use cases of the interception of communication[16], access to data on devices[17] and in the context of the provision of services[18].

While the EDPB understands the importance for law enforcement authorities to have technical possibilities for otherwise lawful access to certain data, the EDPB stresses again[19] that encryption is essential for ensuring the security and confidentiality of personal data and electronic communications, as it provides strong technical safeguards against access to that information by anyone other than the user and the recipients chosen by him, including by the provider. In particular, in the context of interpersonal communications, genuine end-to-end encryption ('E2EE') covering the terminal devices and the data therein, with the decryption keys held solely by the users is a crucial tool for ensuring the confidentiality of electronic communications. Preventing the use of encryption or weakening the effectivity of the protection it provides, would have a severe impact on the respect for private life and confidentiality of users, on their freedom of expression as well as on innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide.

It is crucial to note that the weakening of the protection provided by encryption may be the result of different technical measures that are not limited to the introduction of a "backdoor" within the encryption process itself. In order to fully assess the effective weakening resulting from the possible measures, it is necessary to not only ascertain how the encryption process is impacted, but also if any of the measures introduced renders the guarantees provided by encryption moot or significantly weaken them. The impact on confidentiality and integrity of the whole communication, including but not restricted to the communication channel and the involved devices, must be fully assessed. For example, the introduction of a client-side process allowing remote access to data before it is encrypted or after it is decrypted at the recipient – although not weakening the encryption algorithm on

[15] Idem, paragraph 83.
[16] See recommendations 22 and 23.
[17] See recommendation 26.
[18] See recommendation 27(3)
[19] EDPB-EDPS Joint Opinion 4/2022 and EPDB Statement 1/2024.

a technical level – would likely lead to substantial, untargeted access and processing of unencrypted content on end user's devices and undermine the security and confidentiality of their communications.

In addition, the EDPB would like to underline the fact that, in order to respond to lawful interception or access orders, the providers might face the technical necessity to apply measures weakening encryption indiscriminately to all users to be able to respond to that order, even in cases where the initial interception or access order was limited to a specific individual or a specific group of individuals. Such indiscriminate weakening of encryption – whether achieved via measures required from providers or via weakening technical encryption standards – might lead to a high risk of violations of the fundamental rights of EU individuals, in particular in the context of electronic communications. To that regard, the EDPB would like to recall the case of PODCHASOV v. RUSSIA[20], where the ECtHR found that an "obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued".

Finally, the EDPB notes that the HLG did consider these issues and systematically added statements saying that their Recommendations should not undermine or weaken encryption and the security of devices and communications. The EDPB would like to urge caution against the temptation to set up contradictory demands for providers (to both allow for interception of specific communications and not indiscriminately weaken encryption) and "*oblige [] them to find the mean*" to comply. Such obligations would lead to strong uncertainty for the providers, possible incoherent enforcement, and as a consequence would work against the objective of finding the right balance with the protection of the user's fundamental rights. The EDPB would thus advise to determine and assess the types of measures to be put in place by providers, which should be the basis on which to assess whether they effectively undermine or weaken encryption and the security of personal data and communications in general. More generally, it is crucial to back any recommendation that entails the use of a technical solution with an assessment of the practical feasibility and compliance of said solution with data protection and privacy by design and by default obligations. As a principle, any technical requirement on providers which has the potential to impact the fundamental rights and freedoms of individuals should be laid down by law which respects the essence of the fundamental rights and freedoms and is deemed necessary and proportionate in a democratic society.

4 CONCLUSION

While the EDPD supports the aim of effective law enforcement, doubts remain whether all measures suggested by the HLG would be compliant with the Charter of Fundamental Rights of the EU, especially the right to data protection and the respect for private and family life, given their potential serious intrusiveness.

The EDPB therefore calls for the Commission and the Member States to undertake the assessment of the legal feasibility with due diligence and in full compliance with the data protection and privacy rules.

For the European Data Protection Board

[20] ECtHR judgment of 13 February 2024, 33696/19, § 79.

The Chair

(Anu Talus)