



OPEN DIALOGUE

SUBMISSION ON THE RETENTION OF DATA BY SERVICE PROVIDERS FOR USE IN EU CRIMINAL PROCEEDINGS



12 SEPTEMBER 2025

The submission has been prepared by the Open Dialogue Foundation on behalf of the Building True Change Coalition (BTC Coalition).¹ The Building True Change Coalition (BTC Coalition) composed of human rights defenders, political activists, Bitcoin entrepreneurs, and industry experts and coordinated by the Open Dialogue Foundation.

The BTC Coalition aims to: (1) combat the abuse of Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) within the wider range of transnational repression mechanisms; (2) promote protection of the digital privacy and financial inclusion in non-democratic and developing countries; (3) promote Bitcoin and stablecoins as tools to support human rights efforts and provide humanitarian aid worldwide; and (4) educate on the role of Bitcoin mining as an instrument to facilitate the adoption of renewable energy sources.

The Open Dialogue Foundation (ODF) was established in Poland in 2009 on the initiative of Ukrainian student and civic activist Lyudmyla Kozlovska (who currently serves as President of the Foundation). Since its founding, statutory objectives of the Foundation include the protection of human rights, democracy and the rule of law in the post-Soviet area. ODF pursues its goals through the organisation of observation missions, monitoring especially individual human rights' violation cases. It also advocates for international legislation better serving human rights, such as the Magnitsky Act or the adding of conditionality clauses to EU & international financial assistance programmes directed at non-democratic states and hybrid regimes.

Our core mission centers on defending individuals facing human rights violations, particularly political prisoners and refugees, while working to prevent the abuse of international systems such as INTERPOL and the Schengen Information System by authoritarian regimes. ODF is known for its support for Ukraine during the Maidan revolution, its humanitarian response to Russian aggression in 2014 and 2022, as well as vocal advocacy campaigns to protect political prisoners in the post-Soviet area and impose G7 sanctions against Russia and its allies.

A central component involves combating transnational repression and SLAPP tactics—the practice whereby authoritarian governments extend their reach beyond national borders to silence, intimidate, or harm dissidents, journalists, human rights defenders, and their supporters and family members living abroad. We actively work to expose and counter transnational financial repression, based on the misuse of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) frameworks, cybersecurity laws which are increasingly weaponized by repressive regimes to freeze assets and criminalize legitimate civil society activities. Our mission extends to protecting the privacy and safety of donors through advocacy for privacy-preserving payment mechanisms such as Bitcoin and secure communication tools essential for human rights work, while advocating for legislative reforms that prevent transnational financial repression.

Prepared by **Lyudmyla Kozlovska** and **Julia Kisielinska**

Annex 1 “The principles of data retention under CJEU judgements” prepared for Open Dialogue Foundation by:
Gracjan Pietras, attorney-at-law
Marcin Liszka, attorney-at-law

Website: <https://odfoundation.eu/>

e-mail: odfoundation@odfoundation.eu X: [@ODFoundation](https://twitter.com/ODFoundation)

¹ <https://en.odfoundation.eu/projects-and-campaigns/combating-financial-exclusion-and-work-of-btc-coalition/>

Objective

This report provides an analysis of the European Commission's consultation on data retention by service providers for criminal proceedings. It examines the compatibility of proposed approaches with the Charter of Fundamental Rights and the jurisprudence of the Court of Justice of the European Union (CJEU), which has consistently prohibited indiscriminate or blanket retention of metadata. The aim is to assess whether the consultation's framing adequately respects these legal limits and to propose lawful, proportionate alternatives such as targeted and time-limited "quick-freeze" orders with judicial authorisation.

The European Union plays a pivotal role in setting global standards on privacy and digital rights. However, the framing of the current consultation reflects a restrictive and one-sided approach: many questions presuppose that new obligations for services providers are necessary, while downplaying evidence that law enforcement already operates in a "golden age of surveillance" with unprecedented access to commercial data. If unchecked, such measures risk eroding fundamental freedoms, enabling cross-border repression, and exposing citizens to greater cybersecurity threats by stockpiling sensitive personal data.

In preparing this report, the authors considered both legal and practical dimensions: the constitutional limits established by the CJEU, the persistent non-compliance of Member States with those limits, and the risk to civil society such as journalists, human rights defenders, and lawyers. The Open Dialogue Foundation highlights the need for a re-assessment of the EU's regulatory stance, ensuring that any initiative on data retention: prioritises compliance with CJEU rulings, protects fundamental rights and democratic participation, and safeguards against misuse of personal data in politically motivated or transnational repression cases.

The overall objective of this submission is therefore to offer constructive, legally sound responses to the Commission's consultation, while exposing the structural biases in the questionnaire and presenting concrete alternatives that enhance both security and rights protection.

Table of Contents:

Executive Summary	5
1. Context and Principles of Data Retention in the EU.....	6
a. Legal Background: EU Data Retention Directive and CJEU Case Law	6
b. Key Principles: Necessity, Proportionality, Targeted Retention, and Global Impact	6
c. Current Challenges: Member State Non-Compliance	7
d. “Targeted” Retention in Name Only: Chat Control and Mass Scanning	7
e. AML/CFT, Cybersecurity, and Transnational Financial Repression.....	8
2. Analysis of Consultation Questions and Responses	9
a. Availability of Tools and Evidence	9
b. Harmonisation of Rules	10
c. Metadata Retention Proposals.....	11
d. Fundamental Rights and Risks.....	12
e. Proportional Alternatives and Safeguards	13
3. Why the Consultation Structure is Problematic.....	14
a. Leading and Biased Questions.....	14
b. Limited Scope for Civil Society Input	14
c. Limited Space for Nuance.....	14
Annex 1. The principles of data retention under CJEU judgements.....	15

Executive Summary

This submission responds to the European Commission's consultation on data retention by service providers for criminal proceedings.

The Open Dialogue Foundation (ODF) recognises the importance of effective tools for criminal investigations but strongly emphasises that blanket or indiscriminate data retention is unlawful, disproportionate, and ineffective, as repeatedly confirmed by the Court of Justice of the EU (CJEU).

The central problem is not the absence of harmonised EU rules, but the persistent non-compliance of Member States with existing CJEU jurisprudence. Many national regimes continue to impose excessive or indiscriminate retention obligations, in direct violation of EU law. A new EU initiative should focus first on enforcement of existing limits, not on expanding obligations. In this submission, we highlight specific examples to illustrate how current national laws openly disregard CJEU rulings.

The Commission's consultation is also objectivity-wise problematic. Many of its questions are framed in a leading way, presupposing that more data retention is necessary while ignoring evidence to the contrary. This compromises the consultation process by excluding critical perspectives from civil society, industry, and customer representatives. For example, Question 3 assumes that law enforcement lacks sufficient tools, despite evidence that authorities already operate in a "golden age of surveillance," and Question 8 suggests that the absence of harmonised EU rules is itself a challenge, disregarding the fact that the real problem is Member State non-compliance with CJEU rulings. In this report, we present further examples of such biased framing and explain why they undermine the legitimacy of the consultation process.

Therefore, the main conclusions include:

1. **Indiscriminate retention is unlawful and counterproductive.** Blanket data retention not only violates CJEU case law but is also ineffective and dangerous. In practice, it fuels abuse of AML/CFT and cybersecurity frameworks, enabling arbitrary restrictions, account closures, and reputational harm.
2. **The problem is not a lack of data but unchecked access and weak remedies.** Law enforcement already has unprecedented access to financial transaction records (SWIFT, SEPA, KYC/AML databases), telecommunications metadata (retained by operators), air passenger data (PNR), and vast pools of commercially collected digital footprints. The gap lies not in evidence availability but in insufficient safeguards and the absence of independent remedies when this access is misused—creating fertile ground for the weaponisation of surveillance powers.
3. **Unchecked data practices create systemic risks and require legislative safeguards.** Indiscriminate retention and overbroad powers not only harm individuals through financial exclusion and reputational damage, but also generate national security vulnerabilities by eroding trust in the financial system and democratic institutions. The EU should therefore require that any targeted access to retained data be:
 - Subject to prior judicial authorisation for necessity and proportionality;
 - Strictly time-limited and narrowly scoped to the investigative purpose;
 - Coupled with ex post notification and redress rights for affected persons;
 - Enforceable through independent oversight bodies with sanctioning powers.

These provisions would ensure effective investigation capacity while embedding privacy, due process, and institutional accountability at the heart of EU law.

1. Context and Principles of Data Retention in the EU

a. Legal Background: EU Data Retention Directive and CJEU Case Law

The European Union has established some of the world's most stringent legal standards on data retention, rooted in the Charter of Fundamental Rights and shaped by a robust body of case law from the Court of Justice of the EU (CJEU). In its landmark judgments, the Court has consistently affirmed that “a general and indiscriminate retention of traffic and location data is not permissible.”²

The *Tele2 Sverige* judgment reiterated:

*“Directive 2006/24 entailed a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.”*³

This position is reinforced in *La Quadrature du Net*:

*“Legislation that provides for the retention of traffic and location data must lay down clear and precise rules, indicating in what circumstances and under which conditions a measure providing for the processing of such data may, in practice, be adopted.”*⁴

b. Key Principles: Necessity, Proportionality, Targeted Retention, and Global Impact

The idea of blanket retention had its roots in the EU itself, which was the first jurisdiction to formally propose and implement such requirements for all electronic communications providers via the 2006 Data Retention Directive (Directive 2006/24/EC). However, in *Digital Rights Ireland* (2014), the CJEU invalidated the Directive, holding that “by requiring the retention of all traffic data concerning all means of electronic communication, affecting all persons using electronic communications services, the Directive exceeds the limits imposed by compliance with the principle of proportionality.”⁵

These rulings established the legal baseline that **only targeted, necessary, and proportionate retention may, in exceptional cases, be permitted—and always subject to judicial authorisation, temporal limits, and redress rights**. The CJEU highlighted the need for remedies and oversight:

*“... legislation must lay down clear and precise rules to govern the scope and application of the measure in question and impose minimum safeguards so that the persons whose data have been retained have sufficient guarantees that their data are effectively protected against the risk of abuse and against any unlawful access and use of that data.”*⁶

Because the EU is both a major digital market and a leader in privacy law, its frameworks on data transfers—such as “adequacy” findings—make compliance with these standards mandatory for third countries seeking access to EU data.⁷ This has shaped international standards, as partners seeking cooperation on AML/CFT, counterterrorism, and cybersecurity must demonstrate rights protections equivalent to those mandated by the CJEU.⁸

² CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, para 56; C-203/15 & C-698/15, *Tele2 Sverige*, para 112

³ *Tele2 Sverige*, para 100

⁴ C-511/18, *La Quadrature du Net*, para 132

⁵ *Digital Rights Ireland*, para 65–69

⁶ *Tele2 Sverige*, para 117

⁷ see: Art. 45 GDPR

⁸ The CJEU judgment in the Schrems II case (Page 2)

However, evasion of the "essentially equivalent" rights protections remains possible in practice by authoritarian regimes, especially outside formal adequacy channels, but legally the standard is strict. There are also new threats posed by international instruments like the U.N. Convention on Cybercrime (Ad Hoc Committee on Cybercrime, 2024 draft) which establish obligations for cross-border data sharing but lack commensurate procedural safeguards. Human rights experts warn:

*"The absence of robust judicial oversight and remedial measures in such international frameworks opens the door for authoritarian governments to misuse access to financial, telecommunications and other sensitive data, enabling the transnational weaponisation of legal instruments."*⁹

These dynamics—EU leadership, international convergence, and emerging risks—underscore the conclusion of the CJEU in *Tele2 Sverige*:

*"A legislative measure that does not provide for such safeguards cannot be regarded as meeting the requirement of being strictly necessary within a democratic society."*¹⁰

c. Current Challenges: Member State Non-Compliance

Despite clear CJEU case law, according to the European Digital Right network and *Verfassungsblog.de*, many EU Member States continue to implement retention regimes that do not comply, including:

- **France:** Maintains broad retention.
- **Germany:** Suspended but unrepealed law and ongoing litigation.
- **Belgium, Poland, Italy, Spain, Hungary, Romania, Lithuania, Ireland:** All retain or attempt to reinstitute population-wide schemes or provide for excessive law enforcement access, often in open contradiction to CJEU principles and/or subject to ongoing litigation.^{11, 12, 13, 14}

d. "Targeted" Retention in Name Only: Chat Control and Mass Scanning

Numerous civil society organizations, academic institutions, cybersecurity experts, and technology developers have warned that the EU's proposed Regulation to Prevent and Combat Child Sexual Abuse ("Chat Control") presents serious dangers for privacy, digital security, and democratic freedoms.^{15, 16} If adopted in its current form, the regulation would enable the mass scanning of all private communications—including those protected by end-to-end encryption—effectively subjecting the entire population to blanket surveillance.

⁹ See: Joint Civil Society Statement on the Draft UN Cybercrime Convention, 2024

¹⁰ para 117

¹¹ European Digital Rights (EDRI), *Europe's Data Retention Saga and Its Risks for Digital Rights* (EDRI, 2023), available at: <https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/>

¹² Helsinki Foundation for Human Rights (HFHR), *European Court of Human Rights: Secret Surveillance in Poland Violates Citizens' Privacy Rights* (HFHR, 2023), available at: <https://hfhr.pl/en/news/european-court-of-human-rights-secret-surveillance-in-poland-violates-citizens-privacy-rights>

¹³ *Verfassungsblog*, *The Long and Winding Road: EU Data Retention Jurisprudence and Member State Resistance* (*Verfassungsblog*, 2023), available at: <https://verfassungsblog.de/the-long-and-winding-road/>

¹⁴ NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *CJEU Declares General Data Retention Unlawful in Tele2 Sverige* (CCDCOE, 2017), available at: <https://ccdcoe.org/incyber-articles/cjEU-declares-general-data-retention-unlawful-in-tele2-sverige/>

¹⁵ Patrick Breyer MEP, *Chat Control: Why EU Mass Scanning Plans Violate Fundamental Rights* (Patrick Breyer, 2024), available at: <https://www.patrick-breyer.de/en/posts/chat-control/>

¹⁶ Coalition of Scientists, *Open Letter on the EU's Proposed CSA Regulation ("Chat Control")* (September 2025), available at: <https://csa-scientist-open-letter.org/Sep2025>

On September 10, 2025 German Federal Ministry of Justice representatives recently stated:

“The regulation provisions [of Chat Control] are indeed very serious intrusions into privacy... There are narrow limits that had already become clear in the ECJ's rulings on data retention, and there is a need for regulation that is legally sound.”¹⁷

e. AML/CFT, Cybersecurity, and Transnational Financial Repression

Requirements to retain and monitor personal data now extend far beyond classic communications metadata. Today, AML/CFT and cybersecurity mandates force banks, payment operators, telecoms, and travel carriers to systematically collect and analyze financial transfers (SWIFT, SEPA), customer profiles and KYC databases, telecommunications logs, and even detailed travel records through Passenger Name Record (PNR) systems.

While these practices are promoted as tools to fight money laundering, terrorism, and cyber threats, real-world evidence—across the EU and globally—shows that such frameworks are frequently abused. They are weaponized by the authoritarian states and their proxies alike for arbitrary financial account closures, blacklisting leading to financial exclusion, and reputational attacks.

This practice exemplifies what the Open Dialogue Foundation (ODF) terms **“transnational financial repression”**: a systematic strategy whereby authoritarian regimes and their proxies extend repressive measures beyond borders to target not only human rights defenders, journalists, and civil society organizations, but also their family members, associates, and anyone who provides them with financial support. Such tactics aim to stifle dissent, restrict access to resources, and still fear throughout entire transnational networks engaged in human rights work. Nearly always, affected individuals face opaque “risk” labels and are left without remedy or recourse. This amounts, in effect, to transnational financial repression, where dissenters can be excluded from the banking system or global mobility networks without fair process or oversight.

ODF itself has been subjected to such practices. Since 2018, leading European banks have closed ODF’s accounts without clear justification, citing only “vague” classifications linked to AML/CFT compliance. These closures directly obstructed ODF’s ability to support political prisoners, deliver humanitarian aid, and finance advocacy campaigns. Family members and associates of ODF leadership have also faced arbitrary restrictions and reputational attacks. In each case, no transparent procedure, appeal mechanism, or independent remedy was available, illustrating how financial institutions can be weaponized against civil society.¹⁸

ODF has documented dozens of such cases, highlighting how powerful states and complicit institutions use AML/CFT and cybersecurity justifications to punish critics and suppress civic activism, well beyond any “targeted” law enforcement rationale.^{19, 20, 21}

¹⁷ Deutscher Bundestag, *Bundestag Press Release: Data Retention and Privacy Debate* (Kurzmeldungen, 2023), available at: <https://www.bundestag.de/presse/hib/kurzmeldungen-1108356>

¹⁸ Open Dialogue Foundation, *Financial Exclusion of ODF and Its Leadership as a Case of Transnational Repression* (ODF Report, 2019), available at: <https://en.odfoundation.eu/a/financial-exclusion-as-transnational-repression>

¹⁹ Open Dialogue Foundation (ODF) & Building True Change Coalition, *Submission on the EU Proposal for a Regulation on the Prevention of Money Laundering or Terrorist Financing* (ODF, 2024), available at: <https://en.odfoundation.eu/a/725781/building-true-change-btc-coalition-submission-on-the-eu-proposal-for-a-regulation-on-the-prevention-of-money-laundering-or-terrorist-financing/>

²⁰ Open Dialogue Foundation, *SLAPP & Transnational Financial Repression across Belgium/EU and the United States: The Case Against Lyudmyla Kozlovska and the Open Dialogue Foundation* (ODF, 2025), available at:

²¹ Open Dialogue Foundation, *Transnational Repression Against Barlyk Mendygazyev* (ODF, 2024), available at: <https://en.odfoundation.eu/a/727011/transnational-repression-against-barlyk-mendygazyev/>

These risks are now amplified by growing international legal uncertainty. The draft U.N. Cybercrime Convention—promoted by China, Russia, Belarus, and North Korea explicitly to avoid human rights constraints—has the potential to make EU-collected data, including AML/CFT and travel records, accessible to regimes that use them not for justice, but for transnational repression. The proposed treaty dramatically weakens standards of judicial oversight and remedy.²² Civil society, including ODF, warns that such legal measures will give authoritarian regimes a back door—enabling cross-border surveillance and persecution cloaked as “international cooperation.”

Without rigorously enforced standards of necessity, proportionality, independent oversight, and genuine remedy, the very tools created to protect society can and do become vectors for systematic rights abuses. The EU and its member states risk undermining not only their own rule of law, but also their global reputation as champions of human rights and fundamental freedoms.

2. Analysis of Consultation Questions and Responses

This section provides a structured analysis of the European Commission’s consultation questions.

a. Availability of Tools and Evidence

The Commission frames the consultation on the assumption that criminal investigations in the EU are hampered by insufficient access to digital evidence. The premise is legally and factually flawed. The CJEU has repeatedly held that limitations on fundamental rights may only be justified where they are strictly necessary and proportionate to the legitimate aim pursued.²³ Although some officials warn about losing investigative capacity in the face of encryption and digital privacy tools, independent research reveals that **we have entered an era of unprecedented surveillance capabilities.** Law enforcement agencies, leveraging massive troves of personal information generated by smartphones, social media, financial transactions, collected travel data and everyday digital services, now enjoy a level of access to individuals’ private lives unmatched in previous generations.²⁴ This surveillance-rich environment fundamentally alters the balance between state investigatory powers and individual privacy rights.²⁵ This undermines the necessity argument for indiscriminate new retention measures.

Case law confirms that blanket retention is neither lawful nor proportionate. In *Digital Rights Ireland* (2014) the Court invalidated the Data Retention Directive for imposing a “wide-ranging and particularly serious interference” with Articles 7 and 8 of the Charter.²⁶ In *Tele2/Watson* (2016), the Court prohibited general and indiscriminate retention, clarifying that only targeted, time-limited regimes linked to serious crime may be permissible.²⁷ Nevertheless, Member States continue to legislate in breach of these limits,

²² Epicenter.works, *Open Letter to the EU Commission and Member States on the Draft UN Cybercrime Convention* (Epicenter.works, 2024), available at: [https://epicenter.works/fileadmin/user_upload/Cybercrime - Open Letter to EU-Commission and Member States.pdf](https://epicenter.works/fileadmin/user_upload/Cybercrime_-_Open_Letter_to_EU-Commission_and_Member_States.pdf)

²³ Charter of Fundamental Rights of the European Union, Articles 7-8; CJEU, *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12, 2014)

²⁴ *Carpenter v. US*; Joh, 2020; UN Special Rapporteur, 2022

²⁵ EDRI, *Public Consultation on Retention of Data by Service Providers for Criminal Proceedings: Answering Guide for Civil Society* (12 Aug 2025)

²⁶ CJEU, *Digital Rights Ireland* (Joined Cases C-293/12 and C-59/12, 2014)

²⁷ CJEU, *Tele2 Sverige AB v. Post- och telestyrelsen and Watson* (Joined Cases C-203/15 and C-698/15, 2016)

introducing national schemes that effectively replicate the annulled Directive.²⁸ The resulting challenge is not lack of EU legislation but persistent non-compliance with binding CJEU rulings.

Further, the Commission has not substantiated the claim that broader data retention would improve criminal justice outcomes. Independent studies, including analysis by the European Parliamentary Research Service, have found no measurable correlation between data retention regimes and crime clearance rates.²⁹ Europol has itself acknowledged that the true obstacle lies in managing and analysing vast quantities of existing data, which already overwhelm investigative capacity.³⁰ Imposing additional blanket retention obligations would exacerbate this problem, increasing the volume of irrelevant material while diluting resources needed for targeted, serious-crime investigations.

Accordingly, any claim of necessity for broad or indiscriminate surveillance powers cannot withstand scrutiny. The only lawful and proportionate approach is to adopt targeted “quick-freeze” orders, subject to prior judicial authorisation and strictly limited to the investigation of serious crimes. Such measures must be accompanied by robust safeguards to protect professional privilege, journalistic sources, the work of human rights defenders and their donors, associates. This narrowly tailored model is not only consistent with established human rights principles but is also required to satisfy the Court of Justice of the European Union’s strict proportionality standard (see, e.g., CJEU, *Tele2 Sverige* and *Watson*). By embracing such safeguards, legislators can ensure that law enforcement retains effective investigative tools while safeguarding the general population against suspicionless or arbitrary intrusion into their private lives.

b. Harmonisation of Rules

The consultation suggests that the absence of harmonised EU rules on data retention creates operational challenges for law enforcement. This framing obscures the actual legal problem. The CJEU has already provided clear and binding limits: general and indiscriminate retention of traffic and location data is incompatible with Articles 7, 8, and 11 of the Charter of Fundamental Rights.³¹ Where divergences exist across Member States, they are not due to a lack of EU-level harmonisation but rather to the persistence of national laws that openly disregard CJEU rulings.³²

The jurisprudence is unequivocal. In *Tele2/Watson*, the Court ruled that only targeted regimes, strictly necessary for the fight against serious crime and subject to robust safeguard, can be justified.³³ Similarly, in *La Quadrature du Net*, the Court reiterated that indiscriminate retention of data for law enforcement purposes violates the Charter, with limited exceptions only for narrowly tailored national security measures³⁴. Despite this, several Member States have introduced or maintained regimes that mirror the annulled Directive’s indiscriminate model, exposing individuals across the EU to unlawful mass surveillance.³⁵

²⁸ Bilenas Vadapalas, *Legal Opinion on Data Retention* (7 Apr 2022)

²⁹ European Parliamentary Research Service (EPRS), *General Data Retention and Its Effects on Crime* (2020)

³⁰ Europol, *Common Challenges in Cybercrime Investigations* (2024)

³¹ Charter of Fundamental Rights of the European Union, Arts. 7,8,11

³² EDRI, *Public Consultation on Retention of Data by Service Providers for Criminal Proceedings: Answering Guide for Civil Society* (12 Aug 2025)

³³ CJEU, *Tele2 Sverige AB v. Post -ch telestyrelsen and Watson* (Joined Cases C-203/15 and C-698/15)

³⁴ CJEU, *La Quadrature du Net and Others* (Joined Cases C-511/18, C-512/18, C-520/18, 2020)

³⁵ Bilenas Vadapalas, *Legal Opinion on Data Retention* (7 Apr 2022)

The “challenge” therefore lies not in legislative fragmentation but in systematic non-compliance with existing EU law. Harmonisation that entrenches or expands these unlawful practices would amount to codifying illegality at the Union level. A lawful initiative should instead prioritise:

- Rigorous infringement proceedings against Member States whose legislation remains incompatible with CJEU jurisprudence;
- Guidance to ensure that any targeted retention measures meet the tests of strict necessity and proportionality; and
- Special safeguards for journalists, lawyers, human rights defenders, their associates and donors; protection should expand on parliamentarians, whose communications are particularly sensitive and enjoy elevated protection under the Charter.

Without such enforcement, harmonisation risks legitimising what the Court has already struck down as unconstitutional. The Commission should focus its efforts on ensuring compliance with the Charter and CJEU case law, rather than using "harmonisation" as a vehicle for reintroducing blanket retention.

c. Metadata Retention Proposals

The consultation repeatedly asks whether service providers should be obliged to retain metadata for longer periods or in greater scope for law enforcement purposes. This framing presupposes that blanket data stockpiling is both lawful and necessary. In fact, the opposite is true.

The Court of Justice of the European Union (CJEU) has consistently struck down indiscriminate retention of traffic and location data as incompatible with the Charter of Fundamental Rights.³⁶ Metadata can reveal an individual’s movements, associations, political views, and professional relationships.³⁷ Taken together, even fragments of metadata generate highly detailed profiles of people’s private lives - sometimes more revealing than content data itself. As a result, the CJEU requires that retention measures must be targeted, strictly necessary, proportionate, and limited to combating serious crime.³⁸

Further extending retention obligations would create multiple risks:

- Fundamental rights violations, which would indiscriminate metadata stockpiling chills freedom of expression, association, and religion, and undermines legal privilege for journalists, lawyers, and parliamentarians.
- Cybersecurity vulnerabilities that centralise storage of vast metadata sets increases the attack surface for hackers and hostile state actors.
- Misuse and transnational repression, where retained data may be abused for political persecution, including cross-border surveillance of dissidents and NGOs.

The Commission’s suggestion that more data retention would improve criminal investigations is not evidence-based. Empirical studies have found no measurable correlation between indiscriminate retention and improved crime clearance rates.³⁹ Instead, proportionate tools such as quick-freeze orders, backed by judicial authorisation and serious-crime thresholds, can secure necessary data without subjecting entire populations to generalised suspicion.

³⁶ CJEU, *Tele2 Sverige AB v. Post -ch telestyrelsen and Watson* (Joined Cases C-203/15 and C-698/15)

³⁷ EDRI, *Answering Guide for Civil Society on the Public Consultation on Data Retention* (12 Aug 2025)

³⁸ CJEU, *La Quadrature du Net and Others* (Joined Cases C-511/18, C-512/18, C-520/18, 2020)

³⁹ European Parliamentary Research Service (EPRS), *General Data Retention and Its Effects on Crime* (2020)

Accordingly, any proposal to extend retention periods or categories of metadata would be both unlawful and counterproductive. A lawful EU initiative must focus instead on ensuring compliance with existing CJEU jurisprudence, enforcing targeted retention only under strict safeguards.

d. Fundamental Rights and Risks

Blanket or indiscriminate retention of metadata poses serious risks to the fundamental rights guaranteed under the Charter of Fundamental Rights of the EU, including the right to privacy (Article 7), data protection (Article 8), freedom of expression and association (Articles 11-12), and the right to an effective remedy (Article 47). The Court of Justice of the EU has repeatedly struck down indiscriminate regimes affirming that such measures are disproportionate and unlawful.⁴⁰

Metadata can reveal patterns of life no less sensitive than content itself.⁴¹ When retained en masse, it allows for detailed profiling of individual's movements, habits, and relationships, exposing entire populations to surveillance without suspicion. This fundamentally alters the relationship between citizens and the state, placing individuals under generalised suspicion.

The chilling effect of mass surveillance undermines free speech and democratic participation. When communications data around political gatherings, religious institutions, or journalistic activities are retained, it deters individuals from exercising their rights. Targeting "sensitive locations" would disproportionately impact civil society, minorities, and opposition groups.

Indiscriminate retention threatens the confidentiality of lawyers, journalists, and Members of Parliament.⁴² Attorney-client privilege, journalistic source protection, and parliamentary independence are cornerstones of the rule of law and democratic governance. Any retention framework must categorically exempt such communications or at minimum apply a higher threshold with independent judicial oversight.

Stockpiling vast amounts of metadata also creates systemic cybersecurity vulnerabilities. Data retention obligations expand the attack surface for hackers, criminals, and hostile state actors. Past breaches in the telecom sector demonstrate how poorly secured data expose millions of users.⁴³ Moreover, retained data risks being repurposed for other objectives, including politically motivated surveillance and transnational financial repression.⁴⁴

The experience of the Open Dialogue Foundation illustrates this risk in practice: in 2022, a collective criminal complaint was filed in Belgium by a group of officers from the anti-terrorism unit of Kazakhstan's National Security Committee (KNB) and their minor children against Lyudmyla Kozlovska and the Open Dialogue Foundation. The claimants accused the ODF and its president of "harassment, defamation, and cyberbullying of minor children". They demanded the removal from social media of publications which are, in fact, eyewitness testimonies and materials documenting the involvement of secret service officers in political repression, torture, and killings in Kazakhstan. Eventually, the Belgian court dismissed all claims brought under the collective complaint, ruling that Belgium had no jurisdiction over the alleged crimes. It is important to note that the Kazakhstani officers of special services attempted to use the collective complaint to obtain a wide range of data against Lyudmyla Kozlovska and the Open Dialogue Foundation

⁴⁰ CJEU, *Digital Rights Ireland* (C-293/12, C-594/12, 2014); *Tele2/Watson* (C-203/15, C-698//15, 2016); *La Quadrature du Net* (Joined Cases C-511/18, C-512/18, C-520/18, 2020)

⁴¹ EDRI, *Answering Guide for Civil Society on the Public Consultation on Data Retention* (12 Aug 2025)

⁴² Patrick Breyer MEP, *Stop the Return of Indiscriminate and General Communications Data Retention* (2022)

⁴³ European Data Protection Board, *Hellenic DPA fines imposed on telecom operators due to personal data breach* (2022)

⁴⁴ ODF, *SLAPP & Transnational Repression Case* (2024)

(information on movements/travel data, such as stays at airports and hotels, as well as data from internet providers and cloud services concerning internal communications, even metadata from advocacy videos and financial transactions within the European Union and the United States). The Belgian investigating judge explicitly noted “the use of Belgian justice to gather as much personal and private data about Kozlovska as possible for purposes other than simply uncovering the truth in this case”. It is noteworthy that the criminal complaint was filed with the participation of Claude Monique, former intelligence officer of France and current head of the private intelligence and lobbying company European Strategic Intelligence and Security Centre (ESISC). In 2017–18, ESISC and Claude Monique were the targets of an investigation by an independent investigative body into allegations of corruption within PACE in connection with possible lobbying of Azerbaijan's interests (so-called “caviar diplomacy”).⁴⁵

In conclusion, the fundamental rights costs of blanket retention are far too high, while evidence shows no clear benefit in crime clearance rates. Proportionate alternatives such as targeted, time-limited quick-freeze orders with judicial oversight provide a lawful way to reconcile security needs with the EU's constitutional framework.

e. Proportional Alternatives and Safeguards

The CJEU has made clear that indiscriminate or blanket retention cannot be justified under the Charter of Fundamental Rights. However, this does not mean that effective tools for criminal investigations are unavailable. Lawful alternatives exist that balance investigatory needs with fundamental rights.

The most proportionate mechanism is the “quick-freeze” model, where service providers are required to preserve specific data relevant to an identified investigation, subject to prior judicial authorisation and limited to serious crimes.⁴⁶ This ensures that data retention is necessary, targeted, and temporary, avoiding the risks of mass stockpiling.

Any retention or access regime must include prior authorisation by a judge, applied only in relation to serious crime.⁴⁷ Lowering this threshold risks normalising surveillance for minor offences and therefore diluting proportionality.

Special safeguards must apply to communications involving lawyers, journalists, human rights defenders, and Members of Parliament.⁴⁸ These groups play essential roles in safeguarding democratic institutions. Retention or access in such cases must either be categorically excluded or require a higher threshold and independent review.

To minimize systemic risks, data that is preserved under quick-freeze orders must be stored securely, separately from commercial datasets, and subject to audit logs. Strong safeguards must also apply to cross-border requests, ensuring that data is not disclosed in cases of political persecution, SLAPPs, or transnational repression.⁴⁹

⁴⁵ Open Dialogue Foundation, *SLAPP & Transnational Financial Repression across Belgium/EU and the United States: The Case Against Lyudmyla Kozlovska and the Open Dialogue Foundation* (ODF, 11 June 2025), available at: https://en.odfoundation.eu/content/uploads/2025/06/slapp_transnational_financial_repression_across_belgium_u_s.pdf

⁴⁶ EDRI, *Answering Guide for Civil Society on the Public Consultation on Data Retention* (12 Aug 2025)

⁴⁷ CJEU, *Tele2/Watson* (C-203/15, C-698/15, 2016)

⁴⁸ Patrick Breyer MEP, *Stop the Return of Indiscriminate and General Communications Data Retention* (2022)

⁴⁹ ODF, *SLAPP & Transnational Repression Case* (2024)

Finally, retention and access regimes must include transparent reporting, independent oversight, and user remedies. Aggregate public reports on the volume and nature of requests (including refusals) are essential to accountability. Civil society participation in evaluating these regimes should be built into EU law.

These alternatives demonstrate that it is possible to reconcile effective investigations with fundamental rights. A regime built on targeted quick-freeze orders, judicial oversight, privilege protections, and robust safeguards is not only more lawful but also more effective, as it avoids overwhelming investigators with excessive data and mitigates cybersecurity vulnerabilities.

3. Why the Consultation Structure is Problematic

The European Commission’s public consultation is presented as a neutral exercise in gathering views on data retention. In practice, its structure reflects a significant bias toward expanding retention obligations, while limiting the ability of respondents to express concerns consistent with CJEU jurisprudence.

a. Leading and Biased Questions

Many of the consultation’s multiple-choice questions are framed on the presumption that more data retention is needed. Respondents are often asked to “agree or disagree” with statements such as whether crimes cannot be primary obstacle is insufficient data, while disregarding other well-documented challenges: resource limitations, skills gaps, and member State non-compliance with existing law.⁵⁰

b. Limited Scope for Civil Society Input

The Commission reserves the right to remove “abusive” feedback. Civil society organisations have raised concerns that this discretionary filter could be used to suppress critical perspectives, undermining the transparency and inclusiveness of the consultation process. Combined with the exclusion of NGOs from expert working groups on data access and retention, this contributes to a perception of bias.⁵¹

c. Limited Space for Nuance

The binary nature of the “yes/no/somewhat” format restricts nuanced responses. For example, questions asking whether harmonisation of EU rules is needed do not allow respondents to clarify that the real issue lies in enforcing existing CJEU limits rather than introducing new blanket obligations.⁵² This creates a misleading impression of support for further legislative initiatives.

⁵⁰ Europol. *Common Challenges in Cybercrime Investigations* (2024)

⁵¹ Patrick Breyer MEP, *Going Dark Expert Group: Bias and Exclusion of Civil Society* (2022)

⁵² EDRi, *Answering Guide for Civil Society on the Public Consultation on Data Retention* (12 Aug 2025)

THE PRINCIPLES OF DATA RETENTION UNDER CJEU JUDGEMENTS

Prepared for Open Dialogue Foundation by:

Gracjan Pietras, attorney-at-law

Marcin Liszka, attorney-at-law

The principles governing data retention by service providers were originally set out in the EU Data Retention Directive and subsequently transposed into the national laws of Member States. However, by its judgments of 8 April 2014 in joined cases C-293/12 and C-594/12, the Court of Justice of the European Union (“**CJEU**”) annulled the Directive on the grounds of its manifest incompatibility with the Charter of Fundamental Rights of the European Union.

Despite these rulings, the majority of Member States have failed to amend their national legislation accordingly. This persistent non-compliance has been confirmed in numerous subsequent judgments of the CJEU, in which the Court found that the contested provisions of national laws were incompatible with the Charter. On the basis of this jurisprudence, the Court has established a set of conditions that must be met for the retention of data and its disclosure to law enforcement authorities to be lawful:

1. The purpose of data retention must be strictly defined and justified

According to the CJEU, data may only be retained for the purposes of preventing serious crime, detecting and prosecuting serious offences, preventing serious threats to public security, and protecting national security.

The concept of “*serious crime*” encompasses offences that endanger life or health (e.g. terrorism, murder, kidnapping), have an organised character (e.g. organised crime, human trafficking), involve large-scale property damage (e.g. financial fraud, cybercrime), or undermine state security (e.g. espionage, sabotage of critical infrastructure). For example, in Case C-746/18, the CJEU held that access to location data may be justified only in cases of serious crime, and not, for instance, for traffic offences or petty theft.

By “*national security*”, the CJEU understands protection against terrorist threats, counterintelligence activities, protection of critical infrastructure (e.g. energy or telecommunications networks), or preventing the destabilisation of the state (e.g. in wartime or crisis situations). In Case C-203/15, the Court accepted the possibility of targeted data retention in situations involving threats to national security, but only on condition that strict proportionality and oversight requirements are met.

2. Guarantees that data may be disclosed solely for the purposes of preventing, detecting, and prosecuting serious offences

Legislation must establish objective criteria to ensure that competent national authorities may access data exclusively for the prevention, detection, and prosecution of serious offences. It must also specify the substantive and procedural conditions under which such access may be granted, and limit the number of individuals authorised to access and subsequently use the data.

3. Prohibition of general and indiscriminate retention

Preventive and indiscriminate retention of traffic and location data for the purposes of combating crime and addressing serious threats to public security is incompatible with the Charter of Fundamental Rights.

Retention may be permissible only in the context of targeted retention, provided that it is strictly necessary and limited to a specific geographical area (e.g. high-risk zones), a defined period of time (e.g. during a threat), and particular categories of individuals who may, in some manner, be connected to a serious crime, or whose retained data could, for other reasons, contribute to the prevention, detection, or prosecution of serious offences (CJEU, Case C-140/20, 5 April 2022).

4. Access to data must be subject to prior supervision by an independent authority

Access to data retained by a service provider must, in all cases, be authorised by an independent authority. Such authorisation should be granted upon a request from law enforcement authorities, specifying the circumstances and evidence justifying access to the data. Authorisation must be obtained prior to any disclosure. The independent authority granting access must be functionally, hierarchically, and legally independent from the requesting authority. This may take the form of a court or another body providing adequate guarantees of independence. Only once such authorisation has been obtained may the service provider disclose the data to law enforcement authorities.

5. Data retention period must be limited

Data retention should be limited to the period strictly necessary to achieve the legitimate purpose of retention. Legislation should also set out objective criteria for determining the duration for which data will be retained, in order to ensure that it is confined to what is strictly necessary. In particular, data retention periods should vary depending on the categories of persons and data, the status of the individuals, and the usefulness of the data for the intended purpose (CJEU judgments in cases C-293/12 and C-594/12).

6. Right to information, review, and appeal

A person whose data is being retained should be informed by the public authority about the retention of their data and its disclosure to the relevant authorities. Furthermore, they should have the right to request a review of the lawfulness of the disclosure of their data to public authorities and to appeal any decision that granted access to their data. To ensure the application of these principles, legislation should provide for sanctions for the unjustified retention, disclosure, or use of data by public authorities.

Conclusion

In light of the recent public consultation initiated by the European Commission, it is evident that any new legislation concerning the retention of data by service providers must adhere to the principles established by the aforementioned jurisprudence of the CJEU. These principles emphasise the need for targeted, proportionate, and time-limited data retention, subject to independent oversight and limited to the purposes of combating serious crime or protecting national security.

Implementing these principles into a binding EU Regulation would ensure the harmonisation of data retention standards across all Member States. Such unification is essential to eliminate the current

fragmentation and inconsistent application of CJEU jurisprudence at the national level. It would also prevent the continued disregard of the Court's rulings by certain Member States, which undermines the rule of law and the uniform protection of fundamental rights within the Union.

By codifying the CJEU's standards into a Regulation, the European Union would also provide legal certainty for service providers and other businesses, ensure effective oversight mechanisms, and reinforce the protection of privacy and data rights for all individuals. This approach would mark a decisive step towards aligning national practices with the Charter of Fundamental Rights and restoring trust in digital governance across Europe.

Prepared for Open Dialogue Foundation by:

Gracjan Pietras, attorney-at-law

Marcin Liszka, attorney-at-law