Shadow evaluation report of the Law Enforcement Directive (2016/680) implementation

EDRi
European Digital Rights

Table of Contents

1. Acknowledgements

European Digital Rights (EDRi) would like to acknowledge the hard work, continuous engagement and diligence of the seven authors of this study: Alexis Fitzjean Ó Cobhthaigh, Bastien Le Querrec, Charlotte Korenke, Eleftherios Chelioudakis, Liubomir Nikiforov, Primož Križnar and Sebastian Golla. EDRi also thanks Plixavra Vogiatzoglou, Postdoctoral Researcher at the Amsterdam Center for International Law (ACIL) and the Institute for Information Law (IViR), Christian Thönnes, Doctoral Researcher at the Max Planck Institute for the Study of Crime, Security and Law, and Jesper Lund, Chairperson of IT-Pol Denmark and EDRi member, who provided invaluable support and detailed feedback as the Review Committee on this research project. Furthermore, EDRi thanks Una Dimitrijevic for her excellent proofreading services, Chloé Berthélémy, EDRi Senior Policy Advisor, for her project manager role, and EDRi staff members involved in the dissemination and publication stages of this project. Finally, the EDRi Brussels office would like to express our sincere gratitude to EDRi members and all other organisations that document and contest police violence and overreach, upon whose work this study builds.

Disclaimer: The country reports on which this concluding report is based solely reflect their authors' views and not those of EDRi. Conversely, this report does not reflect the authors' views but solely those of EDRi. The majority of the research phase was carried out by the researchers in 2023-2024, and therefore, results must be read in that light.

2. Abbreviations

AI	Artificial Intelligence
ANPR	Automated Number Plate Recognition
BNG	*Banque Nationale Générale* (Belgian police database)
CJEU	Court of Justice of the European Union
CNIL	*Commission Nationale Informatique et Libertés* (French Data Protection Authority)
COC	*Organe de contrôle de l'information policière* (Belgian Police Information Monitoring Body)
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EMFA	European Media Freedom Act
ENAR	European Network Against Racism
EU	European Union
FRA	Fundamental Rights Agency
GDPR	General Data Protection Regulation
IPRS	*Informacijski pooblaščenec* (Slovenian Data Protection Authority)
JHA	Justice and Home Affairs
LED	Law Enforcement Directive (2016/680)
NGO	Non-Governmen tal Organisation
TAJ	*Traitement des Antécédents Judiciaires* (French criminal records database)
UK	United Kingdom
US	United States
ZMVR	*Ministerstvo na vatreshnite raboti* (Bulgarian Law on the Ministry of the Interior)
ZNPPol	*Zakon o nalogah in pooblastilih policije* (Slovenian Police Tasks and Powers Act)

3. Executive Summary

European Digital Rights (EDRi) commissioned the analysis of the implementation of the Law Enforcement Directive (LED) in five Member States in order to feed into the ongoing evaluation led by the European Commission of this crucial EU instrument for digital rights. Often described as the "little sister" of the General Data Protection Regulation (GDPR), the LED provides important minimum protection standards for the processing of personal data by law enforcement authorities.

This assessment is timely and necessary, as it takes place in the wider context of increasing police surveillance and repressive powers, as well as the EU's deregulation agenda against rights-based laws. Instead of weakening rules that enable the exercise of rights enshrined in the EU Charter of Fundamental Rights, more efforts and resources are needed to implement, enforce and interpret rules that were designed to protect our lives against digital harms and surveillance from state and corporate actors. This is why it is important to critically and rigorously evaluate the effectiveness and robustness of the EU data protection framework in the area of justice and home affairs.

The research focuses on four key issues of the LED data protection framework: (1) exercise and restrictions of data subject rights (Articles 13-17 LED); (2) processing of special categories of data (often referred to as "sensitive data", Article 10 LED); (3) alignment of national laws with the LED's requirements (Article 8 LED); and (4) new technologies and big data. It was carried out in Bulgaria, France, Germany, Greece and Slovenia.

The study shows that, eight years after the LED's entry into application, its implementation is still highly fragmented across Member States and in large parts still insufficient, both in terms of legal transposition and in practice:

1. With regards to **data subject rights,** all Member States studied imposed overly broad restrictions or added other grounds for restricting rights compared to the LED. This is liable to give competent authorities wide discretionary powers to refuse data subject access requests. In some cases, the national laws contain blanket restrictions for certain data categories without any individual examination, which is likely non-compliant with the CJEU jurisprudence.

2. Concerning the **processing of special categories of data,** whilst the five Member States surveyed have faithfully transposed the wording of Article 10 LED into their national law, including the requirement of strict necessity, the practical application by authorities of the LED's additional safeguards for processing sensitive personal data generally falls short of the requirements set by the CJEU in its developing case law on Article 10 LED.

3. As regards the **alignment of national sectoral laws with the LED**, the five Member States surveyed appear to have very different interpretations of the LED requirements for a legal basis for data processing. In many cases, legal bases are not specific enough and lack specific conditions regulating the data processing activity; in others, legal bases are very difficult to access and therefore hardly subjected to public scrutiny.

4. With respect to the **use of new technologies and big data,** we observe different levels and types of use among the Member States surveyed. However, they all lack a sufficiently detailed legal basis for their "big data" processing, and remain largely opaque about their practices. The latter point is also a limitation of what the country research reports were able to document.

The objective of the LED is to ensure a high level of protection of personal data throughout the Union. This can only be achieved if the LED implementation and the national sectoral laws providing the legal basis for processing are subjected to a harmonised standard. The study outcomes show clear areas for action and improvement in order to achieve this, at least across the four thematic focus areas that were selected for analysis.

In particular, a better implementation of the LED will require strong, resourced and coordinated enforcement actions from the DPAs, guidance from the Commission and the EDPB, and a further development of the CJEU's case law, ideally with cases from Member States where the national laws fail to meet the LED requirements.

4. Recommendations

EDRi would like to make the following recommendations in light of the study findings below. These recommendations reflect the scope of this study on the Law Enforcement Directive (LED) implementation, its goals and its results, and therefore do not constitute an exhaustive list of EDRi's positions on the processing of personal data by law enforcement.

Data subject rights

1. The Commission should provide guidance on the application of restrictions to data subject rights, in particular the application of restrictions to data subject rights for certain categories of processing (Article 13(4) and Article 15(2) LED):

- As per the Court of Justice of the European Union's (CJEU) Ligue des Droits Humains C-817/19 judgment,[1] the LED has to be interpreted in a way consistent with the EU Charter of Fundamental Rights, and therefore, the Commission should ensure that Member States' legislative measures restricting, wholly or partly, data subject rights are consistent with Article 8(2) of the Charter.

- The Commission should ensure that neither Member States' legislative measures nor competent authorities' practices lead to blanket restrictions of data subject rights without individual examination, and that competent authorities carry out a concrete, case-by-case assessment when restricting data subject rights (as per recital 44 of the LED).

2. The Commission should reinforce the right to notification by providing guidance on the interpretation of "specific cases" in Article 13(2), which leaves too much room for interpretation to Member States. EDRi recommends providing information under Article 13(2) proactively and for all cases, and especially when competent authorities have collected personal data without the knowledge of the individual.

3. The Member States should ensure that Data Protection Authorities (DPAs) have adequate resources and a sufficient degree of independence to process individual and collective data subject complaints, including indirect access requests, in an effective and swift manner. As guardian of the Treaties, the Commission should pay particular attention to this issue in its evaluation of the LED implementation and enforce independence requirements under Article 42(4).

1. CJEU, *C-817/19 Ligue des Droits Humains v Conseil des ministres*, 21 June 2022

Special categories of data (sensitive personal data)

4. The Commission should ensure that the CJEU's interpretation of the strict necessity requirement under Article 10 LED is respected:

- The Commission should launch an infringement procedure against Bulgaria, as the Bulgarian government has, at the time of publication, still not aligned its national law with the CJEU case law.

5. The European Data Protection Board (EDPB) should launch coordinated enforcement action in all Member States studied in order to address law enforcement authorities' persistent practices of processing sensitive personal data not in line with the requirement of strict necessity, and open investigations in all remaining Member States, given that this report has identified several cross-cutting issues which appear to be systemic.[2]

- The EDPB should review in particular all existing national biometric databases and ensure they are brought in line with the requirement of strict necessity, as interpreted by the CJEU, notably by ordering the removal of historically collected data where competent authorities cannot demonstrate that continued retention complies with the LED.

Alignment of national law with the LED's requirements

6. Member States should urgently revise their sectoral laws to ensure that there is a clear, precise and foreseeable legal basis for processing personal data for all activities of law enforcement in accordance with the requirements of recital 33 LED.

7. The Commission should provide guidance on the interpretation of Article 8 with harmonised minimum standards for the specificity of national sectoral laws that provide the legal basis for processing operations. For example, national laws must specify which authority is competent to process the personal data, the public tasks it performs that justify such processing, and the purpose of the processing, as well as retention period limits, periodic reviews and additional safeguards to protect data subject rights.

8. The Commission should launch infringement proceedings against Member States that merely repeat the general requirements of Article 8 LED, which, as the Commission highlighted in its first report on the application and functioning of the LED, cannot be considered a sufficient legal basis for specific processing operations.

9. The Commission should ensure that no Member State's legislation allows consent as a possible legal basis to process personal data for law enforcement purposes, as per recitals 35 and 37 LED.

10. Member States should ensure that administrative decrees, decisions or orders issued to provide a legal basis for the processing of personal data, as required by Articles 8 and 10 LED, are easily accessible and made available to the public in a timely manner, for example by being published in a central repository with sufficient time before the processing starts.

2. For cross-cutting issues, see section 2.

New technologies and big data

11. Member States' competent authorities should immediately cease the practice of deploying new technologies under the guise of "innovation" or as part of "pilot projects" without a proper legal basis and without ensuring compliance with LED rules on purpose limitation, distinction between data subject categories (Article 6), profiling, automated decision-making and data protection impact assessments.

12. The European Data Protection Board (EDPB) should launch a coordinated enforcement action in all Member States that have deployed systems for the processing of large data sets in order to critically assess whether these systems comply with the requirement in Article 6 LED to distinguish between different categories of data subjects, as well as other requirements of the LED (e.g. data minimisation, purpose limitation, data accuracy, non-discrimination, profiling and automated decision making).

13. Considering the lack of available data, which impeded this study's evidence collection, and the shortcomings of the Artificial Intelligence Act[3] in terms of transparency requirements,[4] which undermine data subjects' access to effective remedies, Member States should proactively publish in a publicly-available database the details of the new technologies (such as algorithmic systems) that their competent authorities use. This database should include technical details of the underpinning system, its functioning, the purposes of using the new technologies, the data sources, and the results of their fundamental rights and data protection impact assessments.

3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)
4. Under the AI Act, all information related to the use of AI in law enforcement and migration is to be included in a non-public database. For an analysis of the shortcomings of the AI Act related to transparency exceptions granted to law enforcement and migration authorities, see Access Now, EDRi et al., "EU's AI Act fails to set gold standard for human rights", 3 April 2024, *https://edri.org/wp-content/uploads/2024/04/EUs-AI-Act-fails-to-set-gold-standard-for-human-rights.pdf*

5. Context of a timely and necessary evaluation of law enforcement data processing in the European Union

As Advocate General Campos Sánchez-Bordona wrote in his opinion in case C-180/21:

> *"The GDPR [General Data Protection Regulation] and Directive 2016/680* **form a cohesive system** *in which:*
> *- the role of the GDPR is to lay down general rules on the protection of natural persons with regard to the processing of their personal data;*
> *- Directive 2016/680 lays down specific rules on the processing of such data in the area of judicial cooperation in criminal matters and police cooperation." (emphasis added)*

Yet Directive 2016/680,[5] hereafter the Law Enforcement Directive (LED), receives far less attention than the GDPR.[6] This text is, however, crucial for the protection of fundamental rights in the European Union (EU) as it regulates the processing operations of personal data by judicial and police authorities for law enforcement purposes, which can have far-reaching consequences for individuals and communities, such as policing interventions, criminal sanctions, deprivation of liberty, etc.

European Digital Rights (EDRi), as a network of civil society organisations and experts, has worked to defend and protect human rights against disproportionate or arbitrary state surveillance for more than 20 years, by monitoring, documenting and advocating against excessive and illegitimate uses of data by law enforcement authorities and intelligence services. From that perspective, the LED is a relevant legal framework to limit law enforcement powers and prevent harmful police practices based on technologies and data processing.

The LED represents one of the instruments in our toolbox as independent watchdogs when we aim to hold those in power accountable. Our member organisations have used

5. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA 2016 (OJ L 119/89) pp. 89–131.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1) pp. 1–88.

the data protection provisions of the LED in their strategic litigation initiatives to counter the unlawful use of mass surveillance technologies or the opaque deployment of digital systems outside any applicable legal framework.

For example, our member in Greece, Homo Digitalis, successfully challenged the deployment of "smart" handheld devices enabling facial recognition and automated fingerprint identification during identity checks. The deploying Greek Ministry had failed to comply with the LED procedural requirements to consult the Hellenic Data Protection Authority (DPA), conduct a Data Protection Impact Assessment (DPIA), and clarify the legal basis that would allow for such data processing activities by the Hellenic Police.[7] In 2020, La Quadrature du Net, EDRi member in France, managed to stop the police from using drones to monitor protests in Paris, by arguing that drones effectively process personal data under the meaning of the LED while recording images, and that there was no legal basis for such processing.[8]

In addition, the LED is a key piece of legislation for EDRi's advocacy work on EU legislative files in the field of Justice and Home Affairs (JHA). Recent legislative reforms in the JHA field aim to align old instruments with the LED requirements for data protection (see section "Successive legislative reforms empowering police, lacking rights protections" below). The LED therefore constitutes a foundational reference point when EU legislators adopt new legislation related to law enforcement matters. The problem that EDRi often observes in these legislative debates is that EU legislators take for granted that (1) the LED affords a sufficient level of protection against new police powers or risks of overreach, or that (2) the LED is implemented correctly and equally across all Member States – which is not currently the case.[9]

It is therefore crucial to review the implementation of the LED to determine whether it fulfils its stated objectives and if not, how they could be achieved. More generally, the question is to effectively determine whether the LED contributes to a high level of fundamental rights protection in the EU or not. Furthermore, its evaluation is timely and necessary for the reasons outlined below.

Ever-expanding state surveillance powers call into question the robustness and adequacy of the EU's data protection legal framework

The political and legal context around the protection and promotion of human rights is severely deteriorating. At the EU and national levels, we observe concerning trends of increasing state surveillance powers and capacities,[10] growing criminalisation of people on the move and human rights defenders,[11] use of unnecessary or excessive force,[12] arbitrary arrests and prosecutions, as well as discriminatory targeting.[13] At the same time, fundamental democratic standards such as the rule of law and the principle of checks and balances are slowly but steadily eroded through successive reforms. As a result, civic space is shrinking and fundamental rights are routinely violated without consequence.[14]

7. Homo Digitalis, "Facial recognition: Homo Digitalis calls on Greek DPA to speak up", EDRi, 1 April 2020, *https://edri.org/our-work/facial-recognition-homo-digitalis-calls-on-greek-dpa-to-speak-up/*
8. La Quadrature du Net, "Interdiction des drones : victoire totale contre le gouvernement", 22 December 2020, *https://www.laquadrature.net/2020/12/22/interdiction-des-drones-victoire-totale-contre-le-gouvernement/*
9. Plixavra Vogiatzoglou and Thomas Marquenie, "Assessment of the implementation of the Law Enforcement Directive", European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, December 2022, *https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf*
10. Privacy International, "The rise of the Surveillance Databases", 24 October 2024, *https://privacyinternational.org/long-read/5455/rise-surveillance-databases*
11. PICUM, "How the New EU Facilitation Directive Furthers the Criminalisation of Migrants and Human Rights Defenders", June 2024, *https://picum.org/wp-content/uploads/2024/06/How-the-New-EU-Facilitation-Directive-Furthers-the-Criminalisation-of-Migrants-and-Human-Rights-Defenders_EN.pdf*
12. Amnesty International, "Europe: Under Protected and Over Restricted: The state of the right to protest in 21 European countries", 8 July 2024, *https://www.amnesty.org/en/documents/eur01/8199/2024/en/*
13. Fundamental Rights Agency, "Addressing Racism in Policing", 10 April 2024, *https://fra.europa.eu/en/publication/2024/addressing-racism-policing*
14. Amnesty International, "Submission to the consultation on the EU Civil Society Strategy 2026-2030", 18 September 2025, *https://www.amnesty.eu/news/submission-to-the-consultation-on-the-eu-civil-society-strategy-2026-2030/* CIVICUS Monitor, see Europe section: *https://monitor.civicus.org/explore/?query=&region=Europe*

As technologies often function as an operational arm of repressive state policies, digital rights naturally come under pressure too. Observing the trends in this field, the situation appears bleak. As highlighted in EDRi position papers,[15] we see deep-rooted problems in the collection, handling, use and exchange of personal data by police in Europe, with huge implications on people's rights and liberties. It is therefore crucial to assess the robustness and adequacy of the LED in light of the following wider issues in European policing.

Mass and systematic data processing for policing purposes

Data-driven policing is widely promoted and deployed in the EU.[16] This model relies on the processing of data or the use of technologies to guide law enforcement decisions, strategies and practices, in a way that exploits data collection mechanisms to enhance pre-existing data sources.

The manifestations of this data-driven policing model are manifold: a multiplication of data sources and data collection tools; opaque and unlawful experimentation with harmful technologies, such as biometric surveillance;[17] the application of mass surveillance techniques; the expansion of police and criminal databases[18] and their interconnection;[19] and the increase and ease of data exchanges among authorities.[20]

Examples

Since 2018, the Czech Republic Police have illegally used a real-time facial recognition system at Vaclav Havel Airport in Prague.[21] The system was shut down in August 2025 after an inspection by the Data Protection Authority, which also found the current national legislation in breach of the LED provisions related to the processing of biometric data.

In 2025, the Belgian Ligue des Droits Humains warned against a pilot project involving the deployment of drones in several municipalities of the Brussels region to purportedly support police interventions, including the prevention and detection of offences or anti-social behaviour in public spaces, and the maintenance of public order.[22] The NGO pointed out the lack of compliance with national and EU key requirements on data protection.[23] The operation was later deemed illegal by the Belgian Police Information Monitoring Body.[24]

Statewatch reported in December 2025 that the Council of the EU has given approval to the European Commission to lead negotiations with the United States (US) with a view to concluding a deal for mutual access to biometric databases.[25] The agreement would grant US border agencies direct access to personal data, including biometric data, stored in EU Member States' databases, as a precondition to remain under the US Visa Waiver

15. EDRi, "Respecting fundamental rights in the cross-border investigation of serious crimes. A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation ('Prüm II')", 7 September 2022, *https://edri.org/wp-content/uploads/2022/10/EDRi-position-paper-Respecting-fundamental-rights-in-the-cross-border-investigation-of-serious-crimes-7-September-2022.pdf*
16. Fieke Jansen, "Data Driven Policing in the Context of Europe. Working paper, ERC-funded project 'Data Justice: Understanding datafication in relation to social justice' (DATAJUSTICE) starting grant (2018-2023)", Cardiff University, 7 May 2018, *https://datajusticeproject.net/wp-content/uploads/2019/05/Report-Data-Driven-Policing-EU.pdf* Access to data for law enforcement is a central priority of the EU's current internal security strategy. On 24 June 2025, the European Commission presented a Roadmap containing proposals to give law enforcement authorities in the EU easier access to data: *https://home-affairs.ec.europa.eu/news/commission-presents-roadmap-effective-and-lawful-access-data-law-enforcement-2025-06-24_en*
17. Luca Montag et al., "The rise and rise of biometric mass surveillance in the EU. A legal analysis of biometric mass surveillance practices in Germany, the Netherlands, and Poland", EDRi, November 2021, *https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf*
18. Statewatch, "EU: Definition of 'potential terrorists' opens door to broad information-sharing", 2 October 2024, *https://www.statewatch.org/news/2024/october/eu-definition-of-potential-terrorists-opens-door-to-broad-information-sharing/*
19. Statewatch and PICUM, "Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status", 18 November 2019, *https://www.statewatch.org/media/documents/analyses/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf*
20. EDRi, "Automated data exchange in Prüm II: The EU's securitisation mindset keeps encroaching on our fundamental rights", 6 February 2024, *https://edri.org/our-work/automated-data-exchange-in-prum-ii-eu-securitisation-mindset-encroaching-on-fundamental-rights/*
21. Iuridicum Remedium (IuRe), "Czech police forced to turn off facial recognition cameras at the Prague airport thanks to the Artificial Intelligence Act", EDRi, 29 October 2025, *https://edri.org/our-work/czech-police-forced-to-turn-off-facial-recognition-cameras-at-the-prague-airport-thanks-to-the-ai-act/*
22. Sibylle Gioe and Pierre-Arnaud Perrouty, "Utilisation de caméras mobiles sur des drones, DIAB (Drones in a box), par la zone de police de Bruxelles Capitale Ixelles", Ligue des Droits Humains, 23 April 2025, *https://www.liguedh.be/wp-content/uploads/2025/04/250423-Courrier-conseil-communal-Ixelles.pdf*
23. The NGO noted the lack of necessity and proportionality of the interference, as well as the lack of mandatory impact assessment before the launch of the pilot project.
24. Arthur Sente, "Bruxelles : des vols de drones illégaux menés par la police", Le Soir, 7 November 2025, *https://www.lesoir.be/709549/article/2025-11-07/bruxelles-des-vols-de-drones-illegaux-menes-par-la-police*
25. Statewatch, "US access to EU citizens' biometric data: ministers approve EU negotiating mandate", 18 December 2025, *https://www.statewatch.org/news/2025/december/us-access-to-eu-citizens-biometric-data-ministers-approve-eu-negotiating-mandate/*

Programme. The EU would seek similar access to US data. The goal is to profile travellers in order to "address irregular migration and to prevent, detect, and combat serious crime and terrorist offences". The plans raise serious questions with regard to the scheme's compliance with the purpose limitation principle established by the LED.

In its 2022 mandate reform, Europol's data protection obligations[26] were intentionally weakened to allow it to process vast stores of personal data transferred by national law enforcement agencies.[27] Europol had received and stored datasets for prolonged periods of time that most likely included the data of individuals with no established link to criminal activities, therefore going beyond the legal limits of the allowed processing set out in its mandate.[28] The reform legalises data mining by the EU police cooperation agency. For the purpose of identifying potential criminals, Europol is allowed to massively collect data, in a general and indiscriminate manner and from multiple sources, and filter them through algorithmic analysis by means of "pre-determined criteria" (country of origin, gender, etc.), in order to single out supposedly suspicious persons.[29] Europol's supervisory authority, the European Data Protection Supervisor (EDPS) questioned the legality of several provisions.[30]

The ideology of "ever more" data processing and its resulting practices contradict the spirit of EU data protection law and more specifically, the legal limits set by the LED, such as the principles of legality, fairness, data minimisation, necessity and proportionality.

Successive legislative reforms empowering police, lacking rights protections

The tension between data protection limits, set notably by the LED, and law enforcement-intensive data processing is particularly perceptible when the EU adopts legislation to expand police abilities to process data or to use certain surveillance technologies.

These new, often continually intensifying, interferences with people's fundamental rights are justified and legitimised by the existence of an allegedly strong European data protection framework.

An illustrative case is the reform of the Prüm framework ("Prüm II" Regulation), which allows police authorities to exchange DNA, fingerprints and vehicle registration data. The 2024 reform adds facial images from national police records and databases to the original Prüm framework and further automates the cross-border sharing of highly sensitive data. The underlying premise of the Prüm II reform is that Member States can be trusted to process policing data in accordance with the LED and the EU Charter of Fundamental Rights.

26. Article 18(6a) of the Europol Regulation creates a derogation from the general rule on categories of data subjects whose data is allowed to be processed by Europol as listed in its Annex II, by explicitly providing the agency with the possibility to process personal data received without Data Subject Categorisation (DSC) for up to 18 months, with a possible extension of up to 36 months in justified cases, solely for the purpose of completing the DSC. Article 18a provides that Europol can process personal data received from a competent authority, the European Public Prosecutor's Office (EPPO) or Eurojust, where necessary for the support of an ongoing criminal investigation, without any need to perform DSC, and by way of derogation, beyond the categories listed in the Europol Regulation. See Regulation (EU) 2022/991: *https://eur-lex.europa.eu/eli/reg/2022/991/oj/eng*
27. EDRi and FairTrials, "Europol's ever-increasing mandate: European Parliament failed to stand up for fundamental rights", 5 May 2022, *https://edri.org/our-work/europols-ever-increasing-mandate-european-parliament-failed-to-stand-up-for-fundamental-rights/*
28. EDPS, "EDPS orders Europol to erase data concerning individuals with no established link to a criminal activity. Frequently Asked Questions", 10 January 2022, *https://www.edps.europa.eu/system/files/2022-01/22-01-10-europol-order_faqs_en.pdf*
29. Prof. Douwe Korff, "The EU's own 'Snowden Scandal': Europol's Data Mining", EDRi, 19 January 2022 *https://edri.org/our-work/the-eus-own-snowden-scandal-europols-data-mining/*
30. EDPS, "Amended Europol Regulation weakens data protection supervision", 27 June 2022, *https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/amended-europol-regulation-weakens-data_en*

However, during its research and advocacy work, EDRi has shown that the reality on the ground reveals a different picture.[31] There is, in fact, a patchwork of rules, and even a lack of rules, as well as systemic data protection failings across Member States' national databases.[32] EDRi assessed that, despite the stated aim of the reform to bring the old framework in line with modern data protection rules, it not only failed to sufficiently align to the LED but also crucially missed the opportunity to enhance rights protections in cross-border investigations.[33]

Prüm II is far from an isolated case. The EU legislature often refrains from harmonising a substantial part of safeguards for fundamental and procedural rights in EU-level instruments in the area of justice and home affairs. It leaves such safeguards to the discretion of Member States because, in theory, national laws must be aligned with the LED and the Charter of Fundamental Rights.

For example, the so-called "e-evidence" Regulation[34] grants powers to law enforcement authorities to access personal data held by private service providers outside their jurisdiction during investigations. By doing so, it bypasses long-established cross-border judicial cooperation channels and the procedural safeguards they guarantee.[35] During political negotiations between the Council of the EU and the European Parliament, draft provisions by the Parliament attempting to provide the same guarantees and safeguards to people in all Member States were discarded.[36] Instead, the final legislative text relies on national procedural rules, which are insufficient to tackle interferences with the fundamental right to privacy.[37]

Similarly, the European Media Freedom Act (EMFA), adopted in 2024, attempts to protect journalists' rights by regulating the conditions under which Member States are allowed to use surveillance techniques against them.[38] Article 4 EMFA completely relies on LED rules concerning the right to be informed when subjected to surveillance. This notification duty for authorities to inform affected individuals, as developed in European jurisprudence,[39] is crucial for the right to access effective remedies and the right to a fair trial. However, a 2022 study commissioned by the European Parliament reports concerns that the LED standards do not sufficiently reflect such notification duty.[40]

As established by the case law of the CJEU, when limitations to fundamental rights are demonstrated as justified, any interference with said rights must still be properly circumscribed and come with adequate safeguards written into EU law. The current inconsistencies across Europe in the areas of criminal justice and law enforcement illustrate the risk of people in different countries enjoying different levels of rights protections due to a lack of harmonised procedures at the EU level. The LED can be part of the solution but, as highlighted in the examples above, an evaluation of its actual contribution to the protection of fundamental rights is warranted.

31. See footnote 15.
32. See footnote 15.
33. For example, by introducing minimum criteria and requirements to allow certain data to be shared in the scope of Prüm II. In its advocacy, EDRi had strongly advised that the alignment to the LED should be complemented by additional substantive provisions or safeguards, given that the Prüm II reform risked worsening the abuse of data and that the LED did not offer sufficient safeguards in that regard. See footnote 15, pp.12-13.
34. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023), pp. 118-180.
35. EDRi, "Position paper on the Commission's proposal for cross-border access to data for law enforcement purposes", 12 April 2019, *https://edri.org/files/e-evidence/20190425-EDRi_PositionPaper_e-evidence_final.pdf*
36. Chloé Berthélémy, "e-Evidence compromise blows a hole in fundamental rights safeguards", EDRi, 7 February 2023, *https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/*
37. Namely the conditions of re-use, transfer and admissibility of data and the regulation of data transfers between Member States. See footnote above.
38. Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act) (OJ L, 2024/1083, 17.4.2024)
39. CJEU, C-203/15 Tele2 Sverige, 21 December 2016, pp. 121-123.
40. Plixavra Vogiatzoglou and Thomas Marquenie, "Assessment of the implementation of the Law Enforcement Directive", European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, December 2022, *https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf*

Systemic discrimination in law enforcement

As state surveillance powers grow, existing problems in European law enforcement also worsen, in particular the systemic, disproportionate and unfair targeting of racialised, poor and other marginalised communities. In that context, the use of data-driven technologies by police equally exacerbates structural discrimination and inequalities.

In 2024, a report by the EU's Fundamental Rights Agency (FRA) found "strong indications of possible structural, institutional and systemic racism in policing", such as "discriminatory profiling practices, inappropriate racist communication and excessive use of force".[41] Citing multiple studies, the report states that racial discrimination is one of the likeliest violations of fundamental rights when police use new technologies such as algorithmic profiling, biometric surveillance and predictive policing. These findings confirm those from the European Network Against Racism (ENAR) report on data-driven policing, demonstrating how historical police data, which reflect police institutions' racialised presumptions, are hardwired into new technologies, which in turn perpetuate pre-existing racist biases and social inequalities.[42]

A more recent study, coordinated by EDRi member Statewatch, unpacks how automated decision-making systems and databases are used in the policing and criminal justice systems of several European countries.[43] The research shows that, regardless of their focus on geographical areas or persons, data-based systems and tools to "predict" crime disproportionately target Black and minoritised ethnic people, and people from deprived backgrounds. This discriminatory targeting materialises in racial profiling, leading to unjustified stops and searches, questioning, restraining orders, home raids, arbitrary arrests, and subsequently criminalisation.[44]

The automation of police racism and other forms of discrimination can have dramatic consequences for the people affected, including deadly ones. Automated policing systems, which assess "risks" and send automated alerts, not only reinforce the police's own prejudices but also influence their decisions. These technologies fundamentally shape law enforcement agents' perception of suspicion, their assessment of grounds for intervention, and even the way they intervene and engage with suspects, victims, witnesses, etc.[45]

Example

In the case of Chris Kaba's killing in the UK, an Automated Number Plate Recognition (ANPR) camera flagged the car he was driving as linked to a past "firearms incident". Although the vehicle did not belong to him, the police took that information presumably without further examination. "In addition to the officers' own prejudices, the information provided by the automated system will have influenced every subsequent interaction that followed, up to Kaba's killing. They saw a car marked as 'dangerous' and a young Black man – racialised as a threat – driving it. Instead of de-escalating or investigating further, they used the data they'd received as justification for the extreme violence that followed."[46]

41. FRA, "Addressing Racism in Policing", 10 April 2024, *https://fra.europa.eu/sites/default/files/fra_uploads/fra-2024-addressing-racism-in-policing_en.pdf*
42. Patrick Williams and Eric Kind, "Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices Across Europe", ENAR, November 2019, *https://www.statewatch.org/media/documents/news/2019/nov/data-driven-profiling-web-final.pdf*
43. Griff Ferris and Sofia Lyall, "New Technology, Old Injustice: Data-driven discrimination and profiling in police and prisons in Europe", Statewatch, May 2025, *https://www.statewatch.org/media/4991/new-technology-old-injustice-25_6-english.pdf*
44. Ibid
45. A study on the UK Metropolitan Police's use of facial recognition shows that there is a "presumption to intervene" when the facial recognition system in use detects a match between an image on a police list and an individual in the street. Professor Pete Fussey & Dr. Daragh Murray, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", University of Essex, July 2019, *https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf*
46. Griff Ferris, "Automated Policing Helped Kill Chris Kaba", NovaraMedia, 14 September 2022, *https://novaramedia.com/2022/09/14/a-police-algorithm-helped-kill-chris-kaba/* Although the UK is no longer a member of the EU, studies and examples on British policing may nonetheless inform about law enforcement practices in EU Member States given the proximity of their security culture. Furthermore, the UK maintained access to several EU police cooperation instruments after Brexit, including the exchange of operational information, Passenger Name Records, Prüm data (fingerprints, DNA and vehicle registration data), cooperation with Europol and Eurojust, facilitating the surrender (extradition) of suspects and convicted persons, the rendering of mutual legal assistance, the exchange of criminal records, etc. See the European Commission's website: *https://home-affairs.ec.europa.eu/policies/international-affairs/engagement-partner-countries/united-kingdom_en*

Racial and other prejudices plague every step of the law enforcement and criminal justice technological chain: from the databases underpinning traditional surveillance systems to newer algorithmic tools. These interconnected policing systems must, in principle, comply with EU data protection and privacy law, which requires that any processing of personal data must be lawful, fair and transparent in relation to the persons concerned, and only processed for specific purposes laid down by law. Particularly relevant to the issue of systemic discrimination, the principle of fairness implies that a reasonable balance of power must be maintained between the entity processing the data and the person affected. However, given the scale and gravity of the problem as evidenced by the examples provided above, these protections seem unheeded and meaningless in day-to-day law enforcement practices. Therefore, the role of data protection law in this context needs to be urgently assessed.

Errors, mistakes, opacity and impeded exercise of rights

Systemic discrimination issues are compounded by the significant problems of repeated human errors, opacity, obfuscation and barriers to the exercise of fundamental rights.

Inaccurate and poor-quality data are included at a vast scale in many European law enforcement databases. They are also retained there for longer than is necessary and proportionate, to the point that they have long become outdated. The extremely poor management of policing data and failures to process them in accordance with the LED are unfortunately the reality in many European countries. Given the lack of compliance with LED requirements with regard to transparency, lawfulness of processing, and data subject rights, many people are unaware that their data are being unlawfully processed, and are therefore unable to exercise their rights to information and redress.

Example

In Belgium, the National General Database (BNG) is a sprawling database in which millions of people are listed without their knowledge. The BNG is the largest database accessible to the police, the state security services and, since 2016, the Immigration Office; it includes all the information collected by the judicial and administrative police in the course of their duties.[47] Data can cover "hard facts" but also second-hand information (e.g. hearsay). According to estimates, the BNG currently covers nearly one in four Belgians,[48] ranging from individuals convicted of criminal offences to those suspected of administrative offences, informers, threatened witnesses and victims. The data are sometimes kept for up to 30 years. The Belgian Police Information Monitoring Body (COC) regularly points out the poor quality of stored data, the lack of compliance with data retention statutory limits and the incorrect classification of facts.[49] In 2023, the COC revealed that illegal searches of the database by police officers were so common that the problem is, in fact, structural in nature.[50]

In January 2026, POLITICO reported on the suspected systematic registration by German authorities of former Ukrainian prisoners of war (in Russian-occupied territories or forcibly transferred by Russian forces from Ukrainian prisons) in the Schengen Information System (SIS), the EU's largest police and border control database.[51] Alerts in the Schengen Information System lead to refusal of entry into the Schengen area, and in those cases prevent people from reuniting with their families and loves ones who

47. Catherine Forget, "*L'effacement des données policières et judiciaires : un parcours du combattant ?*", e-legal ULB, July 2022, *https://e-legal.ulb.be/volume-n06/la-peine-ne-s-arrete-pas-a-la-sortie-de-prison/l-effacement-des-donnees-policieres-et-judiciaires-un-parcours-du-combattant*
48. Olivier Bailly, "*BNG, la Base Non Gérée*", Médor, 14 April 2021, *https://medor.coop/hypersurveillance-belgique-surveillance-privacy/police-justice-bng/episodes/bng-la-base-non-geree-15-quizz/*
49. Organe de contrôle de l'information policière (COC), Executive Summary, *https://www.organedecontrole.be/files/Executive_Summary_COC_AV_RA_2020.pdf*
50. Organe de contrôle de l'information policière (COC), "Rapport concernant les infractions commises par des membres de la police intégrée dans le cadre de traitements dans la BNG", 2023, *https://www.organedecontrole.be/files/DIO23001_F.pdf*
51. Ekaterina Bodyagina, "Separated by war— and by Schengen", POLITICO, 25 January 2025, *https://www.politico.eu/article/uukraine-refugees-european-union-schengen-russia-war/*

fled to the EU. Former prisoners face high barriers to exercise their right to remedies and challenge the alerts on the basis of data protection law. Given the number of people affected, it is questionable whether the recording of their data in the SIS database went through a careful case-by-case assessment and therefore casts doubts as to the data processing compliance with the principles of necessity and proportionality.

Unlawful storage of personal data in police databases1 not only generates a feeling of injustice but can also lead to harmful consequences for the persons affected. They may be forced to undergo enhanced identity checks at the airport, be subjected to searches without justification, or be unable to obtain a security clearance for their professional activities, effectively preventing them from doing their job.[53]

The example from Belgium also demonstrates how difficult it can be to exercise one's rights to redress. The right to be informed is far from being duly respected in practice.[54] Furthermore, the Belgian transposition of the right to access was declared contrary to the LED by the CJEU in 2023, as it deprived the individual of the possibility to seek judicial review in order to challenge the assessment made by the supervisory authority concerning the lawfulness of the data processing and the decision as to whether or not to adopt corrective measures.[55] The barriers to exercise data protection rights are even higher when the data processing involves several authorities, notably in cross-border cooperation.

Example

An inspection by the European Data Protection Supervisor (EDPS) illustrates law enforcement authorities' reluctance to comply with data subjects' access rules.[56] In 2018, the Dutch police sent the personal data of a political activist to their German counterparts and Europol, labelling him as a potential terrorist. The Dutch citizen, whose request for access to their personal data was denied by Europol, sought redress before the EDPS. First, it was revealed that the Dutch police authority at the origin of the data transfer failed to correctly inform Europol that it had withdrawn the data transfer and thus, that the data should have been deleted. Second, after receiving the data subject request for access, the Dutch police suggested that Europol should delete the personal data from its database as a "solution to the problem", in order to avoid disclosing the data to the complainant. Europol did delete the data, but not permanently, as it was still possible to retrieve them. This can be understood as an attempt to obstruct the individual's right of access to personal data. The EDPS clearly warned that "should Europol have erased (permanently deleted) the personal data concerning the complainant, this would constitute a failure to cooperate with the EDPS and a serious infringement of the Europol Regulation".[57]

Limits to a sole data protection approach

In light of all the challenges raised by law enforcement's processing of personal data described above, it is clear that while compliance with data protection rules is very important, it is not enough. A purely data protection-led approach on its own is unable to

53. See Catherine Forget, footnote 47
54.Ibid
55. Judgement of 16 November 2023, Ligue des droits humains, C-333/22, EU:C:2023:874
56. Chloé Berthélémy, "Rather delete than comply: how Europol snubbed data subject rights", EDRi, 28 September 2022, *https://edri.org/our-work/rather-delete-than-comply-how-europol-snubbed-data-subject-rights/*
57. EDPS, "Decision of the European Data Protection Supervisor in complaint case 2020-0908 against the European Union Agency for Law Enforcement Cooperation (Europol)", 8 September 2022, *https://edri.org/wp-content/uploads/2022/09/22-09-08_EDPS-Decision_2020-0908_redacted.pdf*

address all the harms caused by abuses of power, systemic inequalities and overlapping forms of discrimination in our current police and judicial systems. Europe's approach to data protection is fundamentally individualistic and thus struggles to account for big asymmetries of power, such as those involving the police and its surveillance and repressive powers. Data protection rights put too much onus on individuals to protect themselves when the problems posed by state surveillance and control are systemic. As EDRi's strategy points out: "digital rights do not exist in a vacuum".[58] "For people to live in dignity in the digital age, other conditions must also be in place, such as democracy, transparency, participatory decision-making, equity, peace and justice."[59]

The LED is only one piece of the puzzle when working towards more access to justice and aiming to achieve a high level of fundamental rights protection across the EU. This is why it is essential to assess its effectiveness and robustness in the face of growing police powers.

The scope of the Commission's first evaluation was too limited to properly assess Member States' compliance with the legal requirements of the LED

Article 62 of the LED obliges the Commission to submit a report on the evaluation and review of the Directive every four years. In July 2022, the Commission published its first report on the evaluation and review of the LED.[60]

The report mainly focused on the state and validity of the implementation of the LED's provisions into Member States' national laws, the enforcement by national Data Protection Authorities (based on the EDPB report), and the development and use of rules for international data transfers. Unfortunately, it did not include the review of national sectoral laws, which must provide the legal basis for data processing according to Article 8 LED. National sectoral laws usually include legislation concerning public security, defence and national security, as well as public order and criminal law. For example, sectoral legislation may regulate the operation and powers of specific competent authorities. The Commission explained that not enough data were available at the time and that most Member States were late with regard to the transposition and even more so to law enforcement authorities' practice.

In November 2022, the European Parliament released an independent study assessing the implementation of the LED, identifying shortcomings and proposing a set of recommendations.[62] The study seriously questioned the quality of the Commission's first evaluation by assessing the sources used against the standards of quantitative and qualitative data imposed by the Better Regulation Guidelines. The study further notes that "looking ahead to the second report on the evaluation and review of the LED scheduled in 2026 (...) a strong continuous monitoring and ex post evaluation system should provide for sufficient information on the effectiveness, efficiency, relevance, coherence, and EU added value of the LED transposed into national law. To that end, attention should be paid to the collection of wide range of data from a variety of sources on a continuous basis." It notably points out the work of civil society organisations and citizen representatives as an important source of evidence to take into account.

58. EDRi, "Network Strategy 2025-2030", 25 June 2025, https://edri.org/wp-content/uploads/2023/04/Strategy-2025.pdf
59. Ibid.
60. European Commission, "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", COM(2022) 364 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0364
61. Plixavra Vogiatzoglou and Thomas Marquenie, "Assessment of the implementation of the Law Enforcement Directive", European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, December 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf
62. EDRi, "Shadow evaluation report on the Data Retention Directive (2006/24/EC)", 17 April 2011, https://www.edri.org/files/shadow_drd_report_110417.pdf

The Commission's second evaluation of the LED is expected in May 2026. The second report will include four sections: another conformity assessment, including sectoral laws, notably criminal procedural laws; a study conducted by the Fundamental Rights Agency including empirical and qualitative data; the results of the EDPB questionnaire; and results from the public call for evidence and input from the European Parliament.

Consequently, EDRi's attempt to document and gather outputs from civil society monitoring of the respect for data protection rules by EU Member States in law enforcement contexts seems warranted. In the process of doing so, we faced multiple obstacles, which are further exposed in the Methodology section below.

6. Methodology

This study is composed of five country reports on EU Member States with respect to their legal and practical implementation of the LED. The country-focused approach aims to complement and contribute to the Commission's and Parliament's past and upcoming evaluations of the LED's effectiveness, efficiency, relevance, coherence and added value. This approach seeks to provide an overview of the level of implementation and enforcement of the Directive in specific national contexts, and to source concrete examples of gaps, shortcomings and violations. Similar to EDRi's contribution concerning the Data Retention Directive[62] and national laws,[63] we believe civil society plays a crucial role in the evaluation of EU laws and policies to ensure the impacts on individuals and communities, their fundamental rights and their freedoms are taken into account.

The countries selected for the study are Bulgaria, France, Germany, Greece and Slovenia. This selection attempts to achieve a balance in terms of geographical representation and country size, as well as to complement the scope of the 2022 European Parliament study.[64] We commissioned six researchers from these Member States (two for Germany) to produce the country reports. It must be pointed out that for Germany, the researchers focused on the Bundesland Hamburg, as police law is a regional matter in Germany. Given the study's constrains, the authors chose Hamburg as a case study, which is however reflective of general tendencies in Germany, because most regional police laws follow a similar structure. Unfortunately, we were not able to find a researcher for a Nordic or Baltic Member State; both geographical areas are also not meaningfully represented in the Parliament's study, and we thus recommend that the Commission particularly focus its evidence collection efforts on them in future evaluations.

EDRi designed research questions to guide the researchers' work in order to ensure overall coherence and provide avenues for comparison between the situations in the different Member States, as well as to narrow down the scope of the research by focusing on those issues which are highly relevant for the protection of fundamental rights. The research is divided into four sections: data subject rights; sensitive personal data and the requirement of strict necessity; alignment of the legal basis for data processing with the Law Enforcement Directive; and new technologies and big data.

Data subject rights

The LED strengthens data subject rights (i.e. rights of access, rectification, erasure and restriction of processing) because it gives them direct access to the controller, unless restricted in specific cases. It is an improvement compared to the previous EU Framework

61. Plixavra Vogiatzoglou and Thomas Marquenie, "Assessment of the implementation of the Law Enforcement Directive", European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, December 2022, *https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf*
62. EDRi, "Shadow evaluation report on the Data Retention Directive (2006/24/EC)", 17 April 2011, *https://www.edri.org/files/shadow_drd_report_110417.pdf*

Decision 2008/977 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which put direct and indirect access on an equal footing. The LED also introduces a right to notification, although with considerable ambiguities and wide discretion for Member States.

We were interested to know whether the Member States have revised their existing legal frameworks where necessary, or whether they have maintained their previous legal framework, with potential misalignments with the LED requirements in terms of data subject rights. We were particularly interested in empirical evidence to document changes in practice. However, such evidence has not been readily accessible in all Member States, especially with the resources available for this study.

The following questions aimed to guide researchers' evidence collection:

- Does the Member State implement restrictions of data subject rights provided for by the LED (in particular the right to access and the right to notification), and if so, how?

- Under what conditions does the national transposition of the LED provide for individual notification in accordance with Article 13(2)?

- To what extent has the exercise of data subject rights been improved in practice compared to the situation before the transposition of the LED? If possible, document the changes in practice with empirical evidence (e.g. case studies or statistical information from Data Protection Authorities or law enforcement authorities).

Sensitive personal data and the requirement of strict necessity

Article 10 of the LED introduces a requirement of strict necessity for the processing of sensitive personal data, which was interpreted for the first time by the CJEU in C-205/21.[65] Article 10 also requires appropriate safeguards for the rights and freedoms of the data subject when processing sensitive personal data. Both conditions under Article 10 (strict necessity and appropriate safeguards) suggest that national law must have special conditions for the processing of sensitive personal data, which was confirmed by the judgment in C-205/21.

We were interested in documenting whether Member States have revised their legal framework to reflect this substantially higher level of protection for special categories of data, or whether they kept their previous legal framework, and if so, whether this previous legal framework is missing such a higher threshold authorising the processing.

We asked the researchers the following questions on this topic:

- How did the Member State transpose Article 10 of the LED and its requirements for strict necessity and appropriate safeguards?

- How did the Member State transpose the definition of sensitive data, extended to include biometric data for unique identification?

65. Judgement of 26 January 2023, *Criminal proceedings against V.S*, C-205/21, EU:C:2023:49.

- Is the legal basis in national law for processing sensitive personal data more detailed or specific than non-sensitive personal data? If so, how?

- If applicable, how did the national courts apply the provisions on sensitive data?

Alignment of the legal basis for data processing with the Law Enforcement Directive

The LED requires any processing of personal data to be based on national law or Union law (Articles 8 and 10 LED). Recital 33 LED states that the legislative measure "should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights" and sets out some specific requirements for the legislative measures (e.g. purposes of the processing and retention periods). In its evaluation of the LED,[66] the Commission emphasises that "merely repeating the general requirements of Article 8 LED in national law cannot be considered a sufficient legal basis for a specific processing operation". In some Member States, these requirements may be stricter than the previous legal framework for police processing of personal data.

We therefore asked the researchers:

- To what extent did the Member States adjust their existing national laws or adopt new ones (e.g. in criminal procedure or police laws) to fulfil the requirements of Article 8 and Article 10 of the LED?[67]

New technologies and big data

Law enforcement agencies increasingly rely on data collection about the entire population for predictive policing and artificial intelligence systems ("big data analytics"). If such systems exist, we were interested in documenting the legal basis in national law for the processing of personal data and how it relates to the LED rules on the following themes: purpose limitation, fairness of processing and other data protection principles (Article 4); data subject categories (Article 6); data quality (Article 7); the legal basis for data collection and processing (Article 8); profiling and automated decision making (Article 11); and data protection impact assessment for new technologies (Article 27).

The following questions were asked to assess the application of the LED rules to new technologies and big data processing operations in Member States:

- To what extent do national laws providing for the processing of personal data by law enforcement authorities take into consideration existing big data analytics practices, considering the various requirements introduced by the Law Enforcement Directive (e.g. impact assessment, purpose limitation, differentiation between the data subject categories, the right to obtain human intervention, etc.)?

- Are there national laws explicitly providing the legal basis for big data analytics activities by law enforcement?

66. See European Commission, footnote 60, page 14.
67. The requirements of Articles 8 and 10 include the existence of a specific legal basis for each processing operation, determining which authority is competent to process the personal data, the public tasks it performs that justify such processing, and the purpose of the processing, etc.

- Is the type of data that can be collected for and processed in these systems clearly defined by national law?

- Did the Member State change its national laws following the adoption of the LED to reflect its requirements?

- To what extent do these national laws account for likely discriminatory impacts of big data analytics practices and the ban of discriminatory profiling under Article 11?

- If public information is available, provide an analysis or description of the actual tools and technologies used (or intended to be used in the future) for predictive policing, artificial intelligence or data-mining analysis (e.g. systems based on Palantir Gotham),[68] along with an assessment of their legal compliance with the LED.

With regards to the methodology, researchers have mainly relied on the analysis of primary sources such as national legal texts, case law and institutional reports, as well as publicly available information such as governmental records, civil society documentation and media reports. In each report, the researchers provide details on their sources and a bibliography. Some of them tried to submit freedom of information requests to Ministries, notably Bulgaria, but with limited success. This restriction on access to information and the overall lack of publicly accessible information prevent independent research and public scrutiny from being exercised vis-à-vis law enforcement activities and their impacts on fundamental rights.[69] We therefore recommend that the Commission should focus part of its evaluation on examining the level of transparency of data processing by law enforcement in EU Member States, both in terms of data practices and accessibility of a legal basis, and draw recommendations for Member States in that regard.

68. Palantir Gotham is an intelligence tool used by the military and law enforcement agencies across the world to combine and analyse large volumes of data from multiple sources, in order, for example, to predict criminal activity. See Palantir's website: *https://www.palantir.com/platforms/gotham/europa/*
69. See also Statewatch's research: Griff Ferris and Sofia Lyall, "New Technology, Old Injustice: Data-driven discrimination and profiling in police and prisons in Europe", Statewatch, 30 June 2025, *https://www.statewatch.org/media/4991/new-technology-old-injustice-25_6-english.pdf*

7. Summary of the results of the study

Data subject rights

The right of access (Article 14) ensures that people can become aware of personal data that law enforcement authorities have collected about them and verify the lawfulness of the processing. This is emphasised by recital 43 of the LED.

Direct access means that the individual obtains a copy of their personal data directly from the competent authority. With indirect access, the right is exercised through the supervisory authority, which must verify the lawfulness of the processing. Since the individual does not get a copy of the personal data collected, it is much more difficult, if not close to impossible, for the individual to obtain rectification of inaccurate personal data.

The LED requires Member States to provide for direct access (Article 14). In principle, this is a significant improvement over the previous EU data protection rules for law enforcement that allowed Member States to choose between direct and indirect access.[70]

However, the LED also allows Member States to restrict the (direct) right of access in order to protect ongoing investigations, public security, national security and the rights of others (Article 15). In those situations, only indirect access will be available if an individual wants to verify the lawfulness of the processing.

EDRi's study seeks to investigate how Member States have implemented restrictions of data subject rights and to what extent the exercise of data subject rights has been improved in practice compared to the situation before the implementation of the LED. Of particular interest here are blanket restrictions of data subject rights for certain categories of data. Such restrictions are not based on a concrete and individual examination of each case, even though this constitutes a crucial condition to satisfy the necessity and proportionality test for the restriction of a fundamental right. Unfortunately, the LED itself is not clear on this point. While recital 44 states that "the controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted", Article 15(2) allows Member States to determine categories of processing for which data subject rights may be wholly or partly restricted.

In all five Member States, the provisions to restrict data subject rights have elements that are either overly broad or introduce additional grounds for restricting rights compared to the LED. This is liable to give competent authorities wide discretionary powers to refuse data subject access requests. In some cases, the national laws have blanket restrictions for certain data categories without any individual examination.

70. Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, Article 17.

The **German** (Hamburg)[71] transposition has a general exception from data subject rights for data either originating from intelligence services or the transfer of data to these services. This exception existed before the LED.

In **Bulgaria**, the LED requirement of necessity and proportionality when restricting data subject rights does not feature in the national law, and "public order" without proper definition is included as an additional ground for restrictions. Moreover, the Bulgarian transposition merely restates the wording of the LED. More concrete provisions specifying the circumstances under which data subject rights can be restricted are set out only in administrative instructions and ordinances, which does not meet the requirement of being provided for by law. This deficiency was criticised by the Commission in 2019 and has still not been rectified.

In **Greece**, data subject rights can be restricted in order to enable competent authorities to perform their duties. The wording "enable" suggests that any action or decision that contributes to the authorities' ability to execute their responsibilities could justify withholding information from a data subject. This contrasts with the more narrowly-tailored exceptions in the LED, which only permit such actions when there is a clear risk of obstructing or prejudicing specific legal or investigative processes. Moreover, under the Greek law, data subject rights can be restricted to protect the legitimate interests of third parties, which is broader and more ambiguous than "rights and freedoms of others" in the LED.

Similar to Bulgaria, Greece has opted for wide restrictions that are likely to undermine data subject rights by giving competent authorities wide discretionary powers to refuse requests.

The **Slovenian** transposition closely follows the wording of the LED regarding the right to access and its limitations. In itself, this way of transposing gives competent authorities wide discretionary powers to refuse access because all reasons in Article 15 LED are available in all situations. This is likely incompatible with the EU principles of legality and necessity, which require that restrictions of data subject rights must be regulated by more specific conditions than the general terms of Article 15 LED. When disclosure would reveal a covert investigative measure, competent authorities are required to refuse access to personal data. This is a legally questionable addition compared to the LED standards for restricting data subject rights, which never require competent authorities to refuse access.

The **French** Data Protection Act closely follows the language of the LED regarding data subject rights. For police files, such as the TAJ criminal records database, direct access is possible since August 2018, unless the right of access is restricted in individual cases. In that case, the controller must inform the data subject of the possibility of exercising their rights through indirect access via the French Data Protection Authority (CNIL).

If the CNIL finds that the personal data can be communicated to the data subject without prejudicing the purposes of the processing, and the controller is opposed to such communication, the CNIL only has to inform the data subject that the necessary verifications have taken place, without elaborating on any action taken. This constitutes a narrow implementation of Article 17(3) LED, which requires that the supervisory authority inform the data subject at least that the said verifications were made. For the data subject, the boilerplate response does not give any useful information about protecting their rights.

71. Note that when German law is referred to in the rest of the summary of results, the analysis is based on Hamburg's law but can be generalised to all other German Länder.

For some sensitive databases, data subject rights can only be exercised through the supervisory authority. This must be regarded as a blanket restriction of direct access, which France has maintained for some databases after, and despite, the transposition of the LED.

However, one positive aspect of the French implementation of Article 15 LED is that data subject rights can only be restricted if the administrative order identifying the data to be collected and the purposes of processing also specifies which of the five restrictions in paragraph 1 can be applied to the processing.

On 17 October 2024, the CNIL delivered a decision on the TAJ database and found severe violations of data protection rights. The right to information was improperly restricted because the administrative order for the TAJ database did not specify possible restrictions. Many data subjects are not even aware that their personal data is processed by the TAJ database. The CNIL also found severe violations of the rights of access, rectification and erasure due to a large backlog of applications. The CNIL ordered the controller to bring the processing into compliance before 31 October 2026. The two-year delay is noteworthy considering that the CNIL decision is about compliance with basic, essential data protection principles.

The CNIL decision highlights that individuals are often not aware that their personal data are processed by law enforcement authorities. Article 13(2) LED requires that the controller provide the data subject with further information in order to enable the exercise of their rights. However, there is a lot of ambiguity around what constitutes "specific cases", thus giving Member States considerable discretion about individual notifications, at least until the CJEU has developed sufficient case-law.[72]

According to the **Hamburg** data protection law, individuals must be given further information when their personal data have been collected in secret by the police. In **Slovenia**, the additional information must be provided, especially if the data were collected without the knowledge of the individual. This is similar to the German law.

The **Bulgarian** law has simply repeated the wording of Article 13, and there is no clear distinction between paragraphs 1 and 2. This makes it unclear when the controller must provide additional information without a request from the data subject. Similarly, the **French** Data Protection Act requires additional information to be made available in specific cases without clarifying the circumstances. It is evident from the CNIL decision on the TAJ database that data subjects are not always given information to enable the exercise of their rights.

Statistical data about the number of access requests to law enforcement controllers are not available across the Member States studied, with the exception of **France** where the CNIL publishes the number of indirect access requests on a yearly basis. This excludes direct requests to controllers for which no statistical data is available. In France, there has been a significant increase in the number of indirect access requests since 2018, even though direct access was made possible for some police databases in August 2018, e.g. criminal records in the TAJ database and Schengen Information System (SIS) records.

72. Assessment of the implementation of the Law Enforcement Directive, European Parliamentary Research Service, December 2022, p. 55.

This evidence shows an increased awareness of exercising data subject rights in France. For the other four Member States surveyed, it is not possible to conclude whether the exercise of data subject rights has been strengthened in practice due to a lack of statistical information.

Special categories of data (sensitive personal data)

When law enforcement agencies process sensitive personal data, Article 10 of the LED requires strict necessity and appropriate safeguards for the rights and freedoms of the data subject. The requirement of strict necessity for processing sensitive personal data did not exist before the LED.

Both conditions in Article 10 (strict necessity and appropriate safeguards) suggest that national law must have special conditions for the processing of sensitive personal data. This was confirmed by the CJEU judgment in C-205/21.

Biometric data for the purpose of unique identification of a natural person, e.g. fingerprints and facial images (for facial recognition), are sensitive data under the LED (and GDPR). This was not the case in the former EU instruments on data protection for law enforcement. Since processing biometric data for identification is widely undertaken by law enforcement agencies in their work, the new LED requirements for sensitive personal data in Article 10, notably strict necessity, should have considerable impact on law enforcement practices.

Whilst the five Member States surveyed have faithfully transposed the wording of Article 10 LED, including strict necessity, into their national law, the practical application by authorities of the LED's additional safeguards for processing sensitive personal data generally falls short of the requirements set by the CJEU in its developing case law on Article 10 LED.

The **Bulgarian** law contains a literal transposition of Article 10. However, the practical implementation of the LED for sensitive personal data is seriously lacking, as has been demonstrated through two CJEU cases: C-205/21 and C-80/23.

The Bulgarian police law (ZMVR) requires the collection of facial images, fingerprints and DNA when a police record is created for an intentional offence subject to public prosecution. The CJEU ruled in C-205/21 that this systematic collection of biometric data is precluded by Article 10 LED and the principle of strict necessity. The mere fact that a person is accused of a criminal offence cannot be a factor that makes the collection of biometric data strictly necessary. Instead, there must be a case-by-case assessment, which takes into account factors such as the gravity of the offence, the particular circumstances of the offence, and any links between the offence and other criminal investigations in progress.

In a subsequent case, C-80/23, the CJEU clarified that national law must impose an obligation on competent authorities to verify and demonstrate that their collection of special categories of data, such as biometric and genetic data, is strictly necessary. The assessment of strict necessity cannot be delegated to a court, but must be carried out by competent authorities themselves.

73. European Commission, "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')", COM(2022) 364 final. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0364*

As of May 2026, the Bulgarian government has not proposed any amendment to its transposition of the LED in order to address the serious deficiencies identified in the two CJEU cases. The systematic collection of biometric data, in violation of EU law, continues in Bulgaria.

In **Slovenia**, processing of sensitive personal data by law enforcement agencies is permitted if there is a legal basis, statutory conditions ensuring adequate protection of human rights and fundamental freedoms, and if the processing is absolutely necessary. These conditions reflect the formal requirements of the LED. The Supervisory Authority (IPRS) has consistently found that the cumulative conditions for processing sensitive data were met by competent authorities.

Article 10 LED has been transferred verbatim into the **Greek** Data Protection Act, according to which the processing of sensitive personal data can be based on the consent of the data subject. This stands in contradiction to the LED, which recognises that the data subject's consent cannot be regarded as freely given in most interactions with law enforcement agents. Instead, the legal basis for processing personal data must be provided for by law, with appropriate safeguards for the data subject. The voluntary participation of the data subject can be a safeguard, but not generally the legal basis for processing.

The **French** Data Protection Act has literally transposed Article 10. However, the legal basis for sensitive personal data is not more detailed or specific than it is for processing non-sensitive personal data. French courts have set a low bar for meeting the strict necessity requirement in the LED, to the point of confusing it with mere usefulness.

Article R40-26 of the French Code of Criminal Procedure explicitly allows the police to use facial recognition on millions of images in the TAJ database. This was considered strictly necessary by the *Conseil d'État* because the size of the database made it impossible to manually compare images.

The *Conseil d'État's* interpretation of the "strictly necessary" condition seems to deviate significantly from the requirements of EU law, as most recently stated by the CJEU in C-205/21, as no real distinction with necessity is made.

The **German** data protection law transposes the strict necessity requirement for the processing of sensitive personal data. German data protection and police laws did not previously recognise the concept of strict necessity, and the CJEU interpretation in C-205/21 has not yet been taken into account in the German implementation of the LED.

When sensitive personal data are processed, appropriate safeguards for the data subject's rights and freedoms must be provided. Possible safeguards are listed in the Hamburg law as examples, including stricter access rules, special deadlines for review of whether the data should be erased, separate processing from other personal data, pseudonymisation, and specific procedural rules to ensure lawfulness when the sensitive personal data are transmitted or processed for other purposes. The listed safeguard measures are illustrative and non-binding, and the specific choice of safeguards is left to the discretion of the controller. The internal specification of safeguards is not available to data subjects, which contradicts the transparency requirement in recital 26 of the LED.

Alignment of national law with the LED requirements

The LED requires any processing of personal data to be based on national law or Union law (Articles 8 and 10 LED). Recital 33 LED states that the legislative measure "should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights" and sets out some specific requirements for the legislative measures (e.g. purposes of the processing and retention periods).

In its evaluation of the LED,[73] the Commission emphasises (page 14) that "merely repeating the general requirements of Article 8 LED in national law cannot be considered a sufficient legal basis for a specific processing operation". Instead, the legal basis must be provided in sectoral laws, e.g. the national police law. The Commission does not address the more difficult question of how detailed these laws must be in defining and circumscribing the specific data processing activities of law enforcement agencies.

The five Member States surveyed appear to have very different interpretations of the LED requirements for a legal basis for data processing. This is not particularly surprising because the legal basis must be provided for mainly in national law, and Member States have different legal traditions for granting powers to public authorities.

In **Germany**, the implementation of the LED has had little influence on the legal bases for police data processing because a differentiated discourse on the limits of police powers had already taken place in Germany.

Comprehensive clauses such as Section 11 of the Hamburg Law on Police Data Processing form the legal basis for the processing of personal data, which does not significantly affect the rights of the data subject. For intrusive processing activities, such as dragnet searches, ANPR and police use of AI for data mining, the legal basis must be more specific.

How specifically the police data processing powers must be defined essentially depends on how intensively the processing interferes with the rights of the data subject. The German Federal Constitutional Court has developed criteria for assessing the intensity of interference by specific measures. The criteria include the personal relevance of the data (which may cover sensitive personal data) and whether the persons affected are aware of the interference.

A problematic element of the German implementation of the LED is the possibility of using the consent of the data subject as the legal basis for processing. The Hamburg police law requires consent to be given voluntarily and further outlines criteria for assessing whether this is the case. However, the reliance on consent as the legal basis stands in conflict with the LED, which expressly states that the consent of the data subject cannot be assumed to be freely given in the context of law enforcement. The voluntary participation of the data subject can be a possible safeguard, but the legal basis for the processing itself must still be provided for by law.

In **France**, administrative decrees and orders are issued at the national and local level in order to provide a legal basis for the processing of personal data, as required by Articles 8 and 10 of the LED. The orders at the local level are much less accessible than those at the national level, as they are not published in a central repository, and often only published after a prolonged delay.

The **Bulgarian** implementation of the LED only restates the general requirements of Article 8 LED. In sectoral laws, there are no specific provisions for police data processing that meet the requirements for a legal basis. For example, the Bulgarian police law (ZMVR) allows the police to process all necessary categories of data without further defining them. The striking absence in Bulgarian law of clearly defined purposes pursued by law enforcement, and links to the data processing necessary for these purposes, was noted by the Advocate General in point 61 of his Opinion on case C-205/21.

In **Greece**, the situation is similar to Bulgaria. The study only identified one piece of legislation that appears to comply with the requirements of the LED for a sufficiently specific legal basis. The law in question is a presidential decree for the installation and operation of surveillance systems in public spaces. The decree limits the purposes of the surveillance systems to specific criminal acts as well as traffic management, and only allows the deployment of surveillance systems if the objectives cannot be achieved by lesser means. There is also a transparency obligation for the police to publish deployment decisions on their website (which has so far not been complied with by the police).

The **Slovenian** implementation of the LED provides that the processing of personal data is lawful only if it is necessary for the performance of tasks by competent authorities as determined by other laws, e.g. the Criminal Procedure Act. This reference to other laws for the legal basis does not address the issue of how detailed or specific these laws must be in describing the processing operations for law enforcement.

The specificity of the legal basis for processing is of utmost importance for the Slovenian Data Protection Authority, which has searched for and examined the legal basis for data processing by law enforcement and judicial authorities. In some of the cases investigated, the DPA concluded that the processing operations did not have a sufficient legal basis.

New technologies and big data

Regarding "big data analysis", the study seeks to document the legal basis in national law for the processing of personal data in such systems, and how it relates to the LED rules on the following: purpose limitation, fairness of processing and other data protection principles (Article 4); data subject categories (Article 6); data quality (Article 7); the legal basis for data collection and processing (Article 8); profiling and automated decision making (Article 11); and data protection impact assessment for new technologies (Article 27).

Whilst the five Member States surveyed are quite different in terms of the actual use of new technologies, they all lack a sufficiently detailed legal basis for their "big data" processing, and are not transparent about their practices. The latter point is also a limitation of what the national studies are able to document.

In **Germany**, the Bundesländer Hamburg, North Rhine-Westphalia, Bavaria and Hesse have amended their police laws and, with the exception of Hamburg, use automated data analysis platforms based on the Palantir Gotham system. The Hessen law allows the police to process stored personal data through automated analysis, including combining information from different databases, in order to combat serious offences. There is little publicly available information about the exact technical functioning of the Hessen DATA platform, a typical problem for systems based on Palantir Gotham, which is very opaque.

There are no provisions in German data protection law that clearly define the data quality necessary for automated analysis, only the general provision on data quality in the LED. Flawed data will invariably lead to flawed results, and with complex data analysis systems, the problems with the underlying data accuracy may be difficult to ascertain. German law also has no provisions that deal with the possible discriminatory effects of automated data analysis systems or the training data used for such systems.

The restrictions on automated individual decision-making in Article 11 of the LED have not had any noticeable impact on the legal bases and practices for AI-supported data analysis in Germany. This is because German authorities take the position that the automated data analysis systems are only used to support and prepare human decisions. However, according to the CJEU judgment in the SCHUFA case C-634/21, there may be automated decision-making within the meaning of the similar GDPR provision if the human decision draws strongly on the output of the automated data analysis.

In February 2023, the Federal Constitutional Court declared the predictive policing provisions in Hamburg and Hesse unconstitutional. Considering the far-reaching possibilities of automated data analysis systems, the Court ruled that the police laws did not provide for a sufficiently high threshold for using such systems.

The **French** study identified a number of big data analytic practices in law enforcement, including algorithmic video surveillance, web data mining for tax authorities (considered to fall within the scope of the LED and not the GDPR), and predictive policing systems. The French practices in this area appear to pay little attention to the additional requirements of the LED for new technologies. Instead, the focus is on the supposed effectiveness and efficiency of the automated analysis systems.

A similar situation exists in **Greece**. For a smart policing system with mobile devices for facial recognition and fingerprint identification, competent authorities did not originally conduct a Data Protection Impact Assessment (DPIA), according to an investigation by the Data Protection Authority. Moreover, the police failed to establish a clear legal basis for the system and demonstrate that the processing met the requirement of strict necessity (Article 10 LED). Greek authorities have also developed a system for social media monitoring, which will process sensitive personal data and monitor private conversations. It is unclear

whether a DPIA was made. The social media monitoring system has not yet been deployed by authorities.

The **Slovenian** law does not currently provide any specific legal basis for big data analytics by competent authorities. The police law (ZNPPol) allows the police to process fingerprints and palm prints, photographs, and DNA profiles in an automated manner if this is necessary and essential based on the circumstances of the specific criminal offence. However, the automated searches must be for a specific investigation, and the provision cannot be used for big data analysis, predictive policing or similar technologies. One of the biometric matching systems is Face Trace, which is a facial recognition system used since 2014, according to a report by Algorithm Watch.

In **Bulgaria**, there is a serious lack of transparency about the use of new technologies in law enforcement. The study could only identify one public document which explicitly refers to new technologies ("Concept for the development of AI in Bulgaria until 2030", published in 2020).

The Law on the Ministry of the Interior (ZMVR) mentions several automated systems. The list includes systems for biometric recognition technologies and other algorithmic automation processes. The instructions governing these systems contain an obligation to conduct a DPIA, which mirrors the requirements of Article 27 of the LED. There is no information available about the technical details of these systems, only that the Ministry of the Interior uses "specialised software".

The use of AI-based technologies in Bulgaria is mainly linked to the implementation of EU law in the field of home affairs and migration control rather than motivated by national projects and initiatives. The Border Violence Monitoring Network (BVMN) reported that biometric data collection and database capacities were supported by EU funding.

Conclusion: legal fragmentation and insufficient implementation

The overarching conclusion of the summary of the five country reports is that the implementation of the LED is highly fragmented and, in parts, largely insufficient. This is not particularly surprising given that the LED is anchored in national police and criminal procedural laws, and Member States have different legal traditions for granting powers to law enforcement. The state of implementation therefore does not guarantee equal application of and access to rights across the EU.

However, the objective of the LED to ensure a high level of protection of personal data throughout the Union can only be achieved if the LED implementation and the national sectoral laws providing the legal basis for processing are subjected to a harmonised standard. The study outcomes show clear areas for action and improvement in order to achieve this, at least across the four thematic focus areas that were selected for analysis.

In particular, a better implementation of the LED will require strong, resourced and coordinated enforcement actions from the DPAs, guidance from the Commission and the EDPB, and a further development of the CJEU's case law, ideally with cases from Member

States where the legal basis appears to lack the desired specificity, such as the Bulgarian case on biometric data collection, which was instrumental in interpreting the notion of strict necessity under Article 10.

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram

EDRi
European Digital Rights