Council of the European Union

Brussels, 20 November 2025
(OR. en)

15616/25

LIMITE

DATAPROTECT 302
JAI 1713
COMIX 416
CH
IS
LI
NO

PUBLIC

'I/A' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
Subject:	Council position and findings on the evaluation and review of the Law Enforcement Directive (LED) - Approval

1. Article 62 of the Data Protection Law Enforcement Directive[1] (LED) requires the Commission to submit regular reports on the evaluation and review of this Directive to the European Parliament and to the Council. The first report was due by 6 May 2022, followed by reports every four years. Thus the next report is due in 2026. The same Article provides that the Commission is to take into account the positions and findings of the European Parliament and the Council, and of other relevant bodies and sources, when preparing the report.

[1] 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

2. With a view to preparing the Council position and findings on the evaluation and review of the LED, delegations were requested in May 2025 to send written observations. On the basis of Member States' comments, the Presidency prepared a draft text that was discussed by the Working Party on Data Protection at its meetings of 12 September and 10 October 2025, and by JHA Counsellors on 3 November 2025.

3. Based on that preparatory work and following an informal written consultation of Member States launched on 11 November 2025, delegations are now able to agree with the text of the Council position and findings on the evaluation and review of the LED, as set out in the Annex to this note.

4. In view of the above, the Permanent Representatives Committee is invited to:

   – confirm its agreement on the text; and

   – recommend that the Council approves the Council position and findings on the evaluation and review of the Law Enforcement Directive (LED) as set out in the Annex to this note.

PUBLIC

ANNEX

Council position and findings on the evaluation and review of the Law Enforcement Directive

PUBLIC

I. INTRODUCTION

1. 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 (hereinafter: ‘'the Directive'' or ''the LED'') entered into application on 6 May 2018, replacing Council Framework Decision 2008/977/JHA. The Directive aims to ensure a consistent and high level of protection of personal data of natural persons while facilitating the exchange of personal data between competent authorities of Member States for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union. The Directive also covers the transfer of such personal data to third countries and international organisations. The Directive is the first instrument that takes a comprehensive approach to data protection in the field of criminal law enforcement and represents a significant development compared with the earlier Framework Decision[1], which covered only the transmission of data between Member States.

[1] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

2. Article 62 of the Directive requires the Commission to submit regular reports on the evaluation and review of the Directive to the European Parliament and to the Council. The first report was due by 6 May 2022, followed by reports every four years. Thus, the next report is due in 2026. The same Article provides that the Commission is to take into account the positions and findings of the European Parliament and the Council, and of other relevant bodies and sources, when preparing the report. The Commission may also request information from Member States and supervisory authorities.

3. Article 62 of the Directive requires the Commission to examine, in particular, the application and functioning of Chapter V on the transfer of personal data to third countries or international organisations, with particular regard to decisions adopted pursuant to Article 36(3) and Article 39 of the Directive.

4. Anticipating the first LED evaluation and review by the European Commission in accordance with Article 62, the Council adopted its first position and findings regarding the Directive in December 2021, outlining the issues relating to the application and interpretation of the Directive that had raised most concerns in Member States at the time, in particular in relation to international data transfers[2]. The Council highlighted that the Directive had only been in force since May 2018. Therefore, it was likely that future experience in the application of the Directive would be highly beneficial in addressing most of the issues identified by Member States.

[2] ST 13943/21 INIT.

5. On 25 June 2022, the European Commission adopted a Communication to the European Parliament and the Council entitled 'First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')'[3].

6. With a view to preparing the second Council position and findings, delegations were requested in May 2025 to send written observations[4]. On the basis of Member States' comments, the Presidency prepared a draft text that was discussed by the Working Party on Data Protection at its meetings of 12 September and 10 October 2025 and by JHA Counsellors on 3 November 2025. The Council position and findings are based on that preparatory work.

7. The Council highlights the fact that, in addition to the greater practical experience of Member States gained after more than seven years of application of the Directive, its position and findings also take into account relevant regulatory developments, in particular the adoption and application of other legal acts in the Digital Rulebook, such as the EU AI Act.

8. The Council has made several observations on the application of the Directive. In this document, the Council outlines certain topics that Member States consider particularly relevant. The Council invites the Commission to reflect those issues in the upcoming report in an appropriate manner.

PUBLIC

3 COM(2022) 364.
4 WK 6930/2025 INIT.

II. GENERAL REMARKS

9. The Council considers that the Directive remains successful in providing adequate protection of personal data in the scope of the Directive. The Council finds that the introduction of the Directive has had and continues to have a significant impact on awareness, accountability and compliance, and has further increased the security of data processing among competent authorities, as well as transparency, in particular among police authorities. The harmonised framework fosters trust and contributes to facilitating the exchange of operational information between competent authorities within a Member State and between Member States, as well as between Member States' law enforcement authorities on one hand, and Europol, Eurojust and the European Public Prosecutors' Office on the other.

10. The Directive aims to ensure a consistent and high level of protection of the personal data of natural persons and facilitate the exchange of personal data between competent authorities of Members States in order to ensure effective judicial cooperation in criminal matters and police cooperation. In this context, the Council acknowledges the important role of national data protection supervisory authorities in the functioning and consistent application of the Directive.

PUBLIC

11. The Council notes that in the area of international data transfers, only one adequacy decision has been adopted so far under the Directive, in respect of transfers of personal data to the UK.[5] In all other cases, the competent authorities have to resort to using 'appropriate safeguards' or the derogations under Article 38 of the Directive. The Council recalls that adequacy decisions pursuant to Article 36 are an essential tool to facilitate safe international data transfers and requests that the Commission actively take further meaningful and proactive steps towards the adoption of adequacy decisions, including for the purposes of law enforcement, for third countries and international organisations that meet the criteria. Furthermore, difficulties in assessing the presence of 'appropriate safeguards' lead to a lack of legal certainty, so relevant steps to ease such assessments should further be considered. In this regard it is crucial to pay attention to practical needs, such as those of law enforcement and criminal prosecution.

12. The Council foresees that a number of complex legal questions will arise due to the interplay between the recently adopted AI Act and the LED. The Council welcomes the work within the Commission and the European Data Protection Board (EDPB) to provide guidance on the interactions between the AI Act and EU data protection law, as well as the Commission's interaction with the European Artificial Intelligence Board, insofar as the latter's contribution focuses exclusively on the articulation between the two legal frameworks.

[5] Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, (C(2021) 4801 final).

13. Furthermore, the Council deems that more clarity on specific issues would be helpful. Depending on the specific issue and the margin of discretion left for Member States in the national implementation of the relevant provisions of the LED, such clarity could be obtained through the exchange of best practice, for example, or through guidance provided by the national supervisory authorities and the EDPB to controllers and processors. The Commission's upcoming evaluation report could also prove beneficial to highlight the need for specific practical guidelines and other suitable means to increase clarity.

III. DATA SUBJECTS' RIGHTS

14. According to the Council findings, while a number of national transpositions of the Directive build upon national laws which pre-existed the Directive, the Directive further enhanced the overall level of protection for citizens. The Directive continues to raise awareness among data subjects and competent authorities about the rights of data subjects. This is reflected in the growing number of requests submitted by data subjects. Practical experience shows that data subjects mainly seek to exercise their rights of access and erasure.

15. Member States report that they have implemented robust procedures that help data subjects to exercise their rights effectively. Examples of such procedures include standardised submission forms, the provision of general information to the public, designated contact points and dedicated units or desks. The Council notes approvingly that many competent authorities seem to be able to respond to most requests for the exercise of a data subject's rights within around one month, and that they duly justify any limitations of rights. In this context, the Council takes the view that competent authorities benefit from the flexibility to prioritise which requests to handle first based on all relevant factors.

PUBLIC

16. According to the Council findings, the implementation of the right of access under Article 14 of the LED can cause difficulties and create complexity in practice. This is notably the case when the right overlaps or intersects with other rules and procedures regarding access to documents or confidentiality, or with general rules or principles of criminal procedure under national law. This can sometimes lead to unintended consequences, delaying or deterring the effective exercise of the data subject's rights.

17. The Council notes that the EDPB has announced that it intends to issue guidance on data subjects' rights under the LED[6]. The Council encourages the EDPB to tailor these guidelines to the needs of competent authorities when it comes to the practical application of Chapter III of the LED, in particular in relation to access requests, taking into account applicable national laws and Member States' procedural autonomy. The EDPB's guidelines could include general guidance both on legal aspects, such as when authorities can refuse to act on requests considered unfounded or excessive and what information to provide pursuant to Article 17(3), and on practical aspects, such as how to respond to data subjects when refusing their requests, and how to verify the identity of data subjects submitting requests. The Council emphasises that Member States retain the discretion to adopt legislative measures restricting, wholly or partly, data subjects' rights, in particular the right of access, in accordance with Article 15 of the LED.

[6] edpb_work_programme_2024-2025_en.pdf.

IV. INTERNATIONAL DATA TRANSFERS

18. According to the Councils findings, the comprehensive and harmonised framework contained in the LED for international transfers of personal data has been an important development, in that it ensures the most comprehensive protection for data subjects while also ensuring secure transfers of personal data from Member States' judicial and police authorities to those of third countries.

19. The Council finds in particular that adequacy decisions are an essential tool for controllers to transfer personal data safely to third countries and international organisations. This is particularly the case for the LED, which, compared to the GDPR, contains fewer transfer tools that could serve as alternatives to adequacy decisions. The Council also considers it crucial that such adequacy decisions are based on compliance with all the conditions set for such decisions, including for onward transfers. Adequacy decisions must also be subject to ongoing monitoring and periodic review, as required by Union law. This is essential to ensure effective protection of the rights of the data subject.

20. When the Council last examined the LED and adopted its position and findings in 2021 it noted that only one adequacy decision had been adopted so far, and that was for the United Kingdom[7]. The Council therefore welcomes the Commission's intention to consider other possible candidates for future adequacy decisions under the LED[8]. The Council notes, however, that in the intervening years no further adequacy decisions have been adopted under the Directive.

---

7 Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, (C(2021) 4801 final).

8 COM(2022)364 final, point 3.5.1.

21. The Council reiterates its request that the Commission actively take further meaningful and proactive steps towards the adoption of adequacy decisions, including for the purposes of law enforcement, for third countries and international organisations that ensure an essentially equivalent level of data protection. The Commission should intensify its efforts to proactively and persistently seek consultations on adequacy decisions pursuant to Article 36(3) of the Directive with potentially eligible third countries/international organisations, especially with important international partners of the Union in the field of judicial and police cooperation. In doing so, it should take into account the extent and type of data transfers for criminal law enforcement purposes and whether the conditions for adopting an adequacy decision are likely to be met.

22. The Council invites the Commission to maintain close dialogue with the Council on possible priority countries for engaging in an adequacy dialogue and to inform the Council, and Member States through the comitology procedure, on a regular basis of any progress, including on main elements discussed and substance, once the Commission engages in such a dialogue. The Council takes the view that the Council and its preparatory bodies are the appropriate forum to inform and consult Member States at a strategic level, in particular on which countries to prioritise for the initiation of adequacy dialogues. The committee established by Article 93 of Regulation (EU) 2016/679 provides the applicable forum to consult Member States on whether the identified countries ensure an essentially equivalent level of data protection. The Council is of the view that the Commission should consult the above-mentioned committee appropriately in accordance with Article 58 of the LED and Regulation (EU) No 182/2011 and inform it in a timely manner ahead of substantial progress made in the negotiations.

PUBLIC

23. The Council observes that in the absence of adequacy decisions, competent authorities must rely on Articles 37 and 38 of the Directive. In this context, the Council takes note of the EDPB's guidelines on Article 37 of the LED[9].

24. The Council recalls that law enforcement needs often include operational cooperation with third countries which do not necessarily afford an essentially equivalent level of protection of personal data. The Council is therefore of the view that the exchange of best practice on appropriate safeguards would be particularly useful for Member States negotiating bilateral police cooperation treaties or mutual legal assistance treaties with third countries, or for competent authorities when carrying out the assessment referred to in Article 37(1) point (b) of the Directive. The Council welcomes the fact that national supervisory authorities can engage actively with competent authorities, and support or advise them upon request, in relation to the assessment of appropriate safeguards. This should help to foster a mutual understanding of the complex legal and practical landscape in such areas as bilateral police and judicial cooperation with third countries.

25. The Council notes that many competent authorities find it difficult and burdensome to comply with Article 37 of the LED in relation to international data transfers. For reasons such as uncertainty as to what constitutes 'appropriate safeguards' the resources required to assess 'all circumstances surrounding the transfer of personal data' and difficulties in obtaining reliable and accurate information from third countries, some competent authorities do not find it practicable to utilize Article 37(1) point (b) of the LED.

26. The Council considers that exchanges of best practice in relation to international data transfers in compliance with the LED could alleviate the identified difficulties.

---

9 edpb-guidelines-202301_art_37_led_final_0_en.pdf

27. The Council notes that Article 39 of the LED allows for transfers of personal data to recipients established in third countries which are not competent authorities, in individual and specific cases. According to the Councils findings, the lack of a structured mechanism for transferring information to authorities, which are not competent authorities can cause difficulties in practice, in particular in relation to organisations engaged in crime prevention. Further clarity on the definition of 'competent authority', particularly in third countries, could be helpful in this regard. The rules on international transfers can also limit the availability of IT tools for competent authorities and pose particular challenges in relation to cloud services, where the use of and reliance on such tools and services involves the transfer of personal data to third countries.

V. RAISING AWARENESS AND INCREASING COMPETENCES AS REGARDS DATA PROTECTION

28. The introduction of the Directive has had and continues to have a major impact on awareness among competent authorities regarding the importance of data protection.

29. The Council values the role and the function of Data Protection Officers (DPOs), who have had a positive impact on competent authorities' awareness of and compliance with the data protection rules. It is valuable that DPOs are able to provide both *ex ante* advice as well as *ex post* monitoring of compliance. It remains a challenge to strike the right balance between ensuring a strong internal position for the DPO and ensuring the DPO's independence.

30. Member States report that they have implemented robust frameworks and practices to ensure that data protection supervisory authorities are systematically consulted on draft legislation and administrative measures of general application that relate to the protection of personal data. With respect to raising awareness, Member States have further stated that training on topics related to protection of personal data is held regularly.

31. The Council considers that fostering an EU-level framework for trainings competent authorities' DPOs and exchanging best practice between them could support DPOs further in carrying out their roles and functions. The Council notes with appreciation that the Network for Data Protection Officers of Competent Authorities, Justice and Home Affairs Agencies and the European Public Prosecutor's Office has been set up, and that it is consistently facilitated by the Commission, both financially and logistically.

VI. FOSTERING TRUST AND FACILITATING EXCHANGES OF OPERATIONAL INFORMATION

32. According to the Council findings, the harmonised framework provided by the Directive has fostered increased trust in the exchange of operational information within and between Member States, especially in cross-border cases.

33. The Council finds that the Directive also helps to raise the level of security in the processing of personal data, which in turn fosters mutual trust. Practical experience shows that the integration of cybersecurity and data protection within joint compliance frameworks can foster the efficient implementation of high security standards.

34. The Council takes the view that ensuring the harmonised interpretation, implementation and enforcement of the Directive is essential to retaining and increasing the benefits achieved.

PUBLIC

VII. ADMINISTRATIVE BURDENS

35. The Council reiterates that the purpose of the LED is to provide a consistent and high level of protection of personal data of natural persons while facilitating the exchange of personal data between competent authorities of Member States, taking into account the specificities of law enforcement. The Council considers that administrative burdens on competent authorities should be kept as low as possible, taking into account the importance of the functions carried out by such authorities and the level of risk linked to the processing of personal data in such functions. In the context of the LED, this balance between operational requirements and a consistent high level of data protection is found through the risk-based approach on which the Directive is built.

36. Maintaining a record of processing activities, preparing data protection impact assessments (DPIAs) and processing access requests, notably requests covering a long period of time or a large amount of data, is sometimes perceived as particularly burdensome by competent authorities.

37. The Council takes the view that DPIAs are an important tool to ensure a high level of data protection. In practice some competent authorities find that difficulties in assessing whether there is a 'high risk to the rights and freedoms of natural persons' may lead to unnecessary prior consultations with the relevant supervisory authority. The term 'new technologies' in Article 27 of the Directive also requires further specification. The Council considers that a uniform methodology for DPIAs would be beneficial to address these issues.

PUBLIC

38. The burden associated with access requests can be increased by the fact that data subjects are under no specific requirement to specify their requests, which is particularly problematic when the data sets in question are large. While respecting that data subjects have the right to access their personal data without specifying the reason for their requests, Member States could exchange best practice allowing for the amicable and quick resolution of access requests covering long periods of time or large amounts of data, as well as best practice and effective approaches in the implementation of Article 15 of the LED.

39. The Council considers that exchanges of best practices between Member States to share their national approaches, and experiences to avoid excessive administrative burdens in applying the LED could be beneficial. The Network for Data Protection Officers provides a forum for such exchanges. Where relevant, data protection practitioners and experts from competent authorities and other relevant national public bodies could also be involved in such exchanges.

40. The Council takes the view that guidance on the minimum safeguards and procedures required by the LED to ensure a high level of protection of personal data is particularly relevant for competent authorities. The Council encourages national supervisory authorities to engage actively with competent authorities to provide practical advice on how to alleviate those burdens, upon request. That advice should be tailored to the law enforcement context and in line with the risk-based approach.

PUBLIC

VIII. DIFFICULTIES AND POTENTIAL IN RELATION TO SPECIFIC TYPES OF PROCESSING AND NEW TECHNOLOGIES

41. The Council underlines the importance of the technologically neutral nature of the Directive, which allows for continued technological development.

42. The Council takes the view that it is essential to ensure~~,~~ that competent authorities are equipped with sufficient tools, including modern IT tools and systems, to carry out their tasks. In this context the Council observes that ambiguities as to which is the relevant legal framework when processing operational data for the purposes of development of systems can dampen innovation.

43. The Council notes that the processing of large unstructured datasets for law enforcement purposes requires careful balancing of operational needs and fundamental rights, as well as adequate safeguards. In this context, the Council observes that practical challenges may arise from the tension between modern data-driven investigation methods and laws in line with the principle of purpose limitation as required by Article 4(1)(b) of the LED. While the principle requires that processing be linked to a specific, defined purpose, some initial processing of ~~a~~ large unstructured datasets may be required to determine whether they contain necessary (or, as regards special categories of data, strictly necessary) information. This can create operational difficulties, for example, when special categories of data are being processed, in relation to biometric processing, or in situations of emergency. The Council encourages exchanges of best practices on how to reconcile the LED with modern data-driven investigation methods.

PUBLIC

IX. THE PRACTICAL INTERPLAY BETWEEN THE GDPR AND THE LED

44. The Council recalls that the difficulty of delineating between the scope of application of the LED and the GDPR was raised as an issue of concern ahead of the Commission's last evaluation of the LED[10]. Experience shows this delineation can cause difficulties in practice when a public body carries out both functions falling under the scope of the GDPR and functions falling under the scope of the LED. This situation can arise, for example, when-the same data are used, when personal data are transferred between or jointly processed by competent authorities and other public bodies, when developing IT systems to be used for law enforcement purposes, including AI, or in relation to surveillance cameras.

45. The Council takes the view that ambiguity or doubt as to whether a given processing activity falls under the scope of the GDPR or the LED is detrimental to ensuring a high level of data protection, and causes uncertainty about the legitimacy of the processing of data in the above-mentioned contexts. It is undesirable that both the GDPR and the LED are applied to the same processing activity, as this may entail further administrative burdens.

PUBLIC

[10] COM(2022) 364 final, point 2.2.1.

46. The Council encourages the EDPB to consider issuing guidelines on the interplay between the GDPR and the LED covering, in particular, how to determine whether a given operation involving the processing of personal data falls under the scope of the GDPR or the LED and whether the rights of the data subject under the GDPR or the LED apply.

X. THE PRACTICAL INTERPLAY BETWEEN THE LED AND OTHER LEGAL ACTS IN THE DIGITAL RULEBOOK

47. The Council especially foresees that a number of complex legal questions will arise due to the interplay between the LED and the recently adopted AI Act[11], which notably contains specific rules on the protection of individuals with regard to the processing of personal data that restrict the use of AI systems for remote biometric identification for the purpose of law enforcement, the use of AI systems for risk assessments of natural persons for the purpose of law enforcement and the use of AI systems of biometric categorisation for the purpose of law enforcement. The joint application of the LED and the cybersecurity *acquis* may also give rise to such questions.

[11] 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).

48. The Council welcomes the work within the Commission and the EDPB to provide guidance on interactions between the AI Act and EU data protection law. The Council also welcomes the work undertaken within the European Artificial Intelligence Board in relation to the articulation between the AI Act and the LED, which should serve to inform the work of the Commission and the EDPB where appropriate. The Council strongly encourages the Commission and the EDPB to consider examining the LED and to provide guidance specific to the activities falling under its scope. This could include guidance on how to perform impact assessments fulfilling the requirements of both the LED and the AI Act as provided for by Article 27(4) of the AI Act, clarification of which rules apply when personal data from competent authorities is used to train AI models and systems[12], and clarifications regarding any possible divergences in the relevant definitions[13]. It might also be beneficial to examine the interplay between the rules on traceability in the LED and in the AI Act[14].

49. The Council takes the view that guidance on the joint application of the LED and other EU - legal acts should be consistent and tailored to operational work. Such guidance should clarify key concepts in practical terms and aim to limit the administrative burden. To this end, the Council encourages the Commission to facilitate continued dialogue between supervisory authorities designated according to the various relevant EU- legal acts, whilst respecting the mandate and independence of each authority.

---

12 See also Article 59(2) of the AI Act.
13 See, in particular, Article 3(13) of the LED and Article 3(34) of the AI Act.
14 See, in particular, Article 25 of the LED and Article 12(3) (b-c) of the AI Act.