



Council of the European Union  
General Secretariat

**Brussels, 06 October 2025**

**WK 12924/2025 INIT**

**LIMITE**

**DATAPROTECT**

**JAI**

*This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.*

## **WORKING DOCUMENT**

|          |                                                                                                                                 |
|----------|---------------------------------------------------------------------------------------------------------------------------------|
| From:    | Presidency                                                                                                                      |
| To:      | Delegations                                                                                                                     |
| Subject: | Council position and findings on the evaluation and review of the Law Enforcement Directive (LED)<br>- Revised Presidency draft |

Ahead of the meeting of the Working Party on Data Protection of 10 October 2025, delegations will find in the annex a revised Presidency draft on the Council position and findings on the evaluation and review of the Law Enforcement Directive (LED).

**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 the 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 and 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<sup>1</sup>, which covered only transmission of data between Member States.
2. According to Article 62 of the Directive, the Commission shall submit a report 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 thereafter, thus the next report is due in 2026. The same Article provides that the Commission shall take into account the positions and findings of the European Parliament and the Council, and of other relevant bodies and sources, when preparing the above-mentioned report. The Commission may also request information from Member States and supervisory authorities.

---

<sup>1</sup> 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.

3. In accordance with Article 62 of the Directive, the Commission shall 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<sup>2</sup>. The Council highlighted that the Directive had only been in force since May 2018. Therefore, it was likely that most of the issues identified by Member States would greatly benefit from future experience in the application of the Directive.
5. On 25 June 2022, the European Commission adopted the Communication from the Commission 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’)”<sup>3</sup>.
6. With a view to preparing the second Council position and findings, delegations were requested to send written observations<sup>4</sup>. 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, 10 October 2025 and [X November 2025]. The Council position and findings are based on that preparatory work.

---

<sup>2</sup> ST 13943/21 INIT.

<sup>3</sup> COM(2022) 364.

<sup>4</sup> WK 6930/2025 INIT.

7. The Council highlights the fact that, in addition to the greater practical experience of Member States gained after more than seven ~~six~~ years of application of the Directive, its position and findings also takes 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<sup>5</sup>, ~~which notably contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for remote biometric identification for the purpose of law enforcement, of the use of AI systems for risk assessments of natural persons for the purpose of law enforcement and of the use of AI systems of biometric categorisation for the purpose of law enforcement.~~
8. The Council has made several observations on the application of the Directive. In this document, the Council outlines certain topics that have been considered particularly relevant by Member States. The Council invites the Commission to reflect those issues in the upcoming report in an appropriate manner.

## **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 the 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.

---

<sup>5</sup> 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)

10. The Directive aims at ensuring a consistent and high level of protection of the personal data of natural persons and facilitating 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.
11. The Council notes that in the area of international data transfers, only one adequacy decision has been adopted so far under the Directive<sup>6</sup>. In all other cases (than cases involving the transfer of personal data to UK), the Competent Authorities have to resort to use “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 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 meet the criteria. Furthermore, ~~the lack of clear guidance on~~ **difficulties in assessing the presence of** “appropriate safeguards” leads to a lack of legal certainty and ~~information and guidelines on the interpretation~~ **relevant steps to ease such assessments** should further be considered. In this regard it is crucial to pay attention to the practical needs of, e.g., 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 interactions between the AI Act and EU data protection law. In this context The Council encourages the Commission and the EDPB to consider examining the LED and to provide guidance specific to the activities falling under the scope of the Directive.

---

<sup>6</sup> 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 ~~guidance from the data protection supervisory authorities and the EDPB to controllers and processors~~ may be helpful on specific issues. **Depending on the specific issue and the level of discretion left for Member States in regard to the national implementation of the relevant provisions of the LED, such clarity could be obtained through for example exchange of best practice or through guidance from 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 meet this need.

### III. **DATA SUBJECT'S 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 fostered the overall level of protection for the citizens. The Directive continues to raise data subject's and Competent Authorities' awareness regarding the rights of data subjects reflected in an upward trend in the number of data subjects' requests. Practical experience shows that data subjects make use mainly of the rights of access or erasure.
15. Member states have provided that they have implemented robust procedures that support the effective exercise of the data subjects' rights. Such procedures include, inter alia, standardized submission forms, providing general information to the public, designated contact points or 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 subjects' rights within around one month and duly justify any limitations of the rights. In this context the Council takes the view that Competent Authorities ~~must retain~~ **benefit from** the flexibility to prioritize which requests to handle first based on all relevant factors, ~~thus Competent Authorities should not be bound by a specific deadline.~~
16. According to the Council findings the implementation of the right of access under LED article 14 can in practice cause difficulties; **and** complexities ~~and undesirable outcomes — also in terms of data protection~~. This is notably the case, when the right overlaps or intersects with other rules and procedures regarding access to documents, **professional secrecy** or general criminal procedure rules or principles under national law, **which can cause undesirable outcomes also in terms of data protection.**

17. The Council encourages the notes that the EDPB has announced its intention to issue guidance on data subject rights under the LED<sup>7</sup>. The Council encourages the EDPB to consider issuing expeditiously guidelines tailor-made these guidelines to the needs of Competent Authorities regarding the practical application of Chapter III of the LED, in particular in relation to access-requests, taking into account applicable national laws as well as Member States' procedural autonomy, including. This could include general guidance on both legal aspects such as when authorities can refuse to act on requests as unfounded or excessive and what information to provide pursuant to Article 17(3) as well as practical aspects such as how to respond to data-subjects in case of refusal, and how to verify the identity of data subjects submitting such requests ~~and the possible provision of copies.~~ The Council emphasizes that Member States retain the discretion to adopt legislative measures restricting, wholly or partly, the data subject's right of access in accordance with article 15 of the LED.
18. ~~The Council further considers that Competent Authorities may be further supported in complying with the LED through a template for the information to be provided in accordance with Article 13.~~

#### IV. INTERNATIONAL DATA TRANSFERS

19. According to the Council's findings the comprehensive and harmonized 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 ensuring secure transfers of personal data from Member States' judicial and police authorities to those of third countries.
20. 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 even more so the case for the LED, which contains fewer alternative transfer tools ~~alternatives~~ to adequacy decisions compared to the GDPR. In this respect, 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

---

<sup>7</sup> [edpb\\_work\\_programme\\_2024-2025\\_en.pdf](#)

ongoing monitoring and periodic review, as required by Union law, which is essential to ensure effective protection of the rights of the data subject.

21. 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<sup>8</sup>. In this context the Council welcomes the Commissions intention to consider other possible candidates for future adequacy decisions under the LED<sup>9</sup>. The Council notes however that in the intervening years no further adequacy decisions under this Directive have been adopted.
22. 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**~~meet the criteria~~. 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, taking 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.
23. 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 on a regular basis of any progress **including the substance of the discussions from the start of the adequacy process and all along** once the Commission engages in such a dialogue.
24. The Council observes that in the absence of adequacy decisions Competent Authorities must rely on article 37 and 38 of the Directive. In this context the Council **takes note of** ~~welcomes~~ EDPB's guidelines on article 37 of the LED<sup>10</sup>.

---

<sup>8</sup> 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).

<sup>9</sup> COM(2022)364 final, point 3.5.1.

<sup>10</sup> [edpb-guidelines-202301\\_art\\_37\\_led\\_final\\_0\\_en.pdf](#)



25. ~~The Council welcomes that Supervisory Authorities engage actively with Competent Authorities in relation to e.g., negotiations regarding bilateral police cooperation.~~ **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 guidance on minimum safeguards is of particular importance when a Member State is negotiating a bilateral police cooperation treaty or a mutual legal assistance treaty with a third country, or when carrying out the assessment according to Article 37(1)(b) of the Directive. **The Council welcomes that national Supervisory Authorities engage actively with Competent Authorities in relation to e.g., negotiations regarding bilateral police cooperation.**
26. The Council notes that ~~many~~ **some** Competent Authorities find it difficult and burdensome to comply with ~~the provisions~~ **Article 37** of the LED in relation to international data transfers. Owing to e.g., 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**(b)** LED ~~in whole or in part~~.
27. ~~According to the Council's findings the lack of a structured mechanism for transferring information to authorities in third countries, which are not competent authorities, can cause difficulties in practice, in particular in regard to organizations 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.~~
28. The council **considers that exchanges of best practice in relation to international data transfers in compliance with the LED** ~~calls on the EDPB to maintain its efforts and provide even more practical, concrete and specific guidance on international data transfers in accordance with the Directive, including guidelines on article 38 of the LED,~~ **could alleviate the identified difficulties.**
- 28a. **The Council notes that article 39 of the LED provides for transfers of personal data to recipients, which are not Competent Authorities, established in third countries in**

individual and specific cases. According to the Council's 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 regard to organizations 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.

## **V. RAISING AWARENESS AND INCREASING COMPETENCES ON DATA PROTECTION**

29. 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.
30. The Council values the role and the function of Data Protection Officers ('DPOs') which have had a positive impact on the Competent Authorities regarding their compliance with the data protection rules on the one hand and raising awareness on the other. It is valuable that DPO's 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.
31. Member States have provided 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 provided that trainings, which focus on topics related to protection of personal data, are held regularly.
32. ~~The Council considers that DPOs may be supported in their function by the development of educational turnkey material at the EU level.~~ The Council further considers that fostering an EU-level framework for trainings of **and exchange of best practice between** DPOs within Competent Authorities could support DPOs further in carrying out their roles and functions. In this regards 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, ~~and~~ was set up, and **that it** is consistently financially and logistically facilitated by the Commission.

## **VI. FOSTERING TRUST AND FACILITATING EXCHANGES OF OPERATIONAL INFORMATION**

33. According to the Council's findings the harmonized 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.
34. In this regard 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 efficient implementation of high security standards.
35. In this context, the Council takes the view that ensuring a harmonized interpretation, implementation and enforcement of the Directive is essential to retaining and increasing the benefits achieved.

## **VII. ADMINISTRATIVE BURDENS**

36. The Council recalls 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 the law enforcement area. The Council considers that administrative burdens on Competent Authorities should be kept as low as possible, **taking into account particularly in the light of the importance of the functions carried out by such authorities as well as 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, which the Directive is built on.
37. Maintaining a record of processing activities, preparing data protection impact ~~assessments~~ **assessments** (DPIAs) and processing access requests, notably requests covering a large period of time or a large amount of data, is ~~often~~ **sometimes** perceived as particularly burdensome by Competent Authorities.
38. **The Council takes the view that DPIAs are an important tool to ensure a high level of data protection. As regards DPIAs some In practice some Ceompetent Aauthorities find report that difficulties uncertainty in relation to the general threshold of in assessing the**

presence of “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 in this regard would be beneficial.

39. As regards access requests the burden can be amplified by the fact that data subjects are under no specific requirement to specify their requests, particularly in the light of large data sets.

**While respecting that data subjects have the right to access his/her 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 a large period of time or a large amount of data.**

40. The Council considers that exchanges of best practices between ~~M~~member ~~S~~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, such exchanges could also include data protection practitioners.**

41. ~~The Council encourages Supervisory Authorities and the EDPB to engage actively with Competent Authorities to provide practical guidance tailor-made to the law enforcement context and in line with the risk-based approach to alleviate these burdens. In this context 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 upon request tailored-made to the law enforcement context and in line with the risk-based approach to alleviate these burdens.**

## **VIII. DIFFICULTIES AND POTENTIALS IN RELATION TO SPECIFIC TYPES OF PROCESSING AND NEW TECHNOLOGIES**

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

43. 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 the relevant legal framework when processing operational data for the purposes of development of systems can dampen innovation.

44. 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 in LED article 4(1)(b). 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 it contains necessary (or as regards special categories of data - strictly necessary) information. This can create operational difficulties, e.g., 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 to reconcile the LED with modern data-driven investigation methods.** ~~the EDPB to address this issue in specific guidelines.~~

## **IX. THE PRACTICAL INTERPLAY BETWEEN THE GDPR AND THE LED**

45. 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 Commissions last evaluation of the LED<sup>11</sup>. 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 e.g., using the same data, when personal data is transferred between or jointly processed by Competent Authorities and other public bodies, when developing IT-systems to be used for law enforcement purposes or in relation to surveillance cameras.
46. 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. It is undesirable that both the GDPR and the LED are applied to the same processing activity as this may entail further administrative burdens.

---

<sup>11</sup> COM(2022) 364 final, point 2.2.1.

47. The Council encourages the EDPB to consider issuing guidelines on the interplay between the GDPR and the LED including in particular determining whether a given processing of personal data falls under the scope of the GDPR or the LED and determining 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**

48. The Council especially foresees that a number of complex legal questions will arise due to the interplay between ~~the recently adopted AI Act<sup>12</sup>~~ and the LED and **the recently adopted AI Act<sup>13</sup>, which notably contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for remote biometric identification for the purpose of law enforcement, of the use of AI systems for risk assessments of natural persons for the purpose of law enforcement and of 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.

49. The Council welcomes the work within the Commission and the EDPB to provide guidance on interactions between the Artificial Intelligence Act and EU data protection law. **In this context the Council also welcomes the work within the AI-Board, which should serve to inform the work where appropriate.** ~~In this context~~ The Council encourages the Commission and the EDPB to consider examining the LED and to provide guidance specific to the activities falling under the scope of the Directive, this could include guidance on how to perform impact assessments fulfilling the requirements of both the LED and the AI Act as foreseen by article 27(4) of the AI Act, ~~and~~ clarification of the applicable rules, when

---

<sup>12</sup> 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).

<sup>13</sup> 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).

personal data from Competent Authorities is used to train AI-models and systems<sup>14</sup> as well as clarifications regarding any possible divergences of the relevant definitions<sup>15</sup>. It might also be beneficial to examine the interplay between the LED's and the AI Act's rules regarding traceability<sup>16</sup>.

50. The Council takes the view that guidance on the joint application of the LED and other EU-legal acts should be consistent and operational. **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 different relevant EU-legal acts, whilst respecting the mandate and independence of each authority.
- 

---

<sup>14</sup> In this regard reference is made to article 59(2) of the AI Act.

<sup>15</sup> See notably article 3(13) of the LED and article 3(34) of the AI Act.

<sup>16</sup> See notably article 25 of the LED and article 12(3) (b-c) of the AI Act.