Opinion 27/2025 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data by the United Kingdom

Adopted 16 October 2025

Executive summary

The European Commission endorsed its draft implementing decision on the adequate protection of personal data by the United Kingdom pursuant to the Law Enforcement Directive on 22 July 2025. On the same date, as part of the procedure towards the formal adoption of the draft decision, the European Commission requested the opinion of the European Data Protection Board.

The draft decision amends and complements the previous adequacy decision for the United Kingdom under the Law Enforcement Directive, which dates back to June 2021. The EDPB's assessment of the adequacy of the level of protection afforded in the United Kingdom has been made on the basis of the examination of the draft decision and therefore focuses on the new developments in the United Kingdom data protection legislation and on elements highlighted in the previous adequacy decision.

The EDPB has used its LED Adequacy Referential adopted on 2 February 2021 as main reference for this work, as well as the EPDB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures and the relevant case-law. The EDPB welcomes the continuing alignment between the UK and EU data protection framework, notwithstanding recent developments in the UK relevant legal framework. Against this background, it is important to stress that the EDPB does not expect the United Kingdom legal framework to replicate European data protection laws, the objective of this opinion is to identify specific aspects of the legal changes and developments since the adoption of the first adequacy decision, which may affect the level of protection, and to raise points for additional clarifications, for attention and monitoring or for concern.

In this regard, the EDPB emphasises the following findings:

The EDPB observes changes to the rules governing the onward transfer of personal data to third countries, notably the new indicative list of elements to be considered in the adequacy test which does not include important elements that figured in the previous United Kingdom adequacy test. The EDPB considers that this aspect as well as the new criterion of the "desirability of facilitating transfers of personal data to and from the United Kingdom" need to be addressed in more detail and encourages the European Commission to specifically further elaborate its assessment and monitor the developments and the practical implementation of the new adequacy test.

The EDBP takes note of important changes vis-à-vis how automated decision-making is regulated in the United Kingdom, notably introducing a more permissive approach and conferring new powers to the Secretary of State. The scope and discretion of these powers could give rise to notable concern, e.g. due to their extent, especially in light of the fast-evolving regulatory environment and advancements in automated technologies. The EDPB invites the European Commission to analyse these powers and monitor any developments in this respect. The EDPB also recalls the importance of meaningful human review to ensure compliance with safeguards in automated decision-making and therefore urges the European Commission to further elaborate on possible exemptions from the data subject's right to obtain human intervention in its final adequacy decision and to monitor the implementation of these changes in practice.

The EDPB considers it essential to assess the extended national security exemptions under the law enforcement framework and remains particularly vigilant regarding any exemptions from the principle of proportionality, as well as from the requirement to process personal data for a legitimate purpose. Likewise, any exemptions from the powers of the supervisory authority should be approached with caution. Any limitation on the exercise of rights and freedoms recognised by the EU Charter of Fundamental Rights must respect their essence and, subject to the principle of proportionality, may be made only if necessary and genuinely meeting objectives of general interest recognised by the

Union or the need to protect the rights and freedoms of others. The EDPB calls on the European Commission to complement its assessment in the final adequacy decision and to specifically monitor the application in practice of the national security exemptions for law enforcement authorities.

The EDPB notes that processing activities carried out by authorities competent for law enforcement can, in specific circumstances, fall under the rules normally applicable to the processing of personal data by national security authorities. In this context, particular attention should be paid to ensuring that the data protection regime for national security processing is not being extended to contexts not related to national security. The EDPB invites the European Commission to monitor in practice whether qualifying competent authorities are able to maintain a clear distinction between different processing purposes in order to adhere to the corresponding legal framework accordingly.

Although the EDPB acknowledges that the system of oversight of criminal law enforcement agencies as well as the redress mechanisms remain largely unchanged, it reiterates the need for the European Commission to closely monitor the application of corrective powers and of remedies for data subjects in the United Kingdom data protection framework.

In addition to the reintroduction of a sunset clause and the legal monitoring obligation, the EDPB stresses the importance for the European Commission to conduct the mandatory review within the legal timeframe specified in the Law Enforcement Directive, taking into account the elements already outlined in Commission Implementing Decision 2021/1773 as well as any further relevant developments.

Table of contents

The European Data Protection Board

Having regard to Article 51(1)(g) of the 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 (herein after "the LED"),

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING OPINION:

1 INTRODUCTION

1.1 General Comments

1. On 22 July 2025, the European Commission ("Commission") endorsed its draft implementing decision on the adequate protection of personal data by the United Kingdom pursuant to the LED ("Draft Decision"). On the same date, as part of the procedure towards the formal adoption of the Draft Decision, the European Commission requested the opinion of the European Data Protection Board ("EDPB"). The EDPB notes that the Draft Decision extends the validity of the existing UK adequacy decision[1] for a period of six years until 27 December 2031. The EDPB recalls that the initial adequacy decision was due to expire on 27 June 2025 and, therefore, had already been subject to a technical and time-limited extension[2] to allow the UK to finalise its data protection reforms.[3] The test the Commission applied to this assessment is "whether the conclusion that the United Kingdom ensures an adequate level of protection remains factually and legally justified in light of developments that took place since the adoption of the previous UK Adequacy Decision".[4] As a result, the Commission focused its assessment on the new data protection legislation, the Data (Use and Access) Act ("the DUAA") which came into force on 20 August 2025. The Commission specifically considered the elements listed in recital 165 of the previous UK adequacy decision which all feature in the Draft Decision, namely:

"*rules on transfers of personal data to third countries, and the impact it may have on the level of protection afforded to data transferred under this Decision, to the effectiveness of the exercise of individual rights, including any relevant development in law and practice concerning the exceptions to or restrictions of such rights. Amongst other elements, case law developments and oversight by the*

[1] Commission Implementing Decision (EU) 2021/1773 of 28 June 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 (notified under document C(2021) 4801).
[2] Commission Implementing Decision (EU) 2025/1225 of 24 June 2025 amending Implementing Decision (EU) 2021/1773 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 (notified under document C(2025) 3898).
[3] Opinion 06/2025 regarding the extension of the European Commission Implementing Decisions under the GDPR and the LED on the adequate protection of personal data in the United Kingdom, adopted on 5 May 2025, available at https://www.edpb.europa.eu/system/files/2025-05/edpb-opinion-202506-uk-adequacyextension-gdpr-led_en.pdf.
[4] Recital 4 of the Draft Decision.

Information Commissioner's Office (ICO) and other independent bodies informed the Commission's monitoring." [5]

2. The Commission concludes that based on this assessment, the UK continues to ensure an adequate level of protection for personal data transferred within the scope of Directive (EU) 2016/680 from the European Union to the United Kingdom.

3. The EDPB agrees that the main focus of the assessment should be on the new developments in the UK data protection legislation and on elements highlighted in the previous adequacy decision. It is the understanding of the EDPB that the Commission has assessed all elements listed in Article 36(2) LED and all relevant developments to the UK's overall legal framework beyond the DUAA when concluding that the UK's overall legal framework continues to ensure an adequate level of protection for personal data transferred from the European Union to the UK within the scope of the LED. Still, the EDPB would welcome explicit clarification in this respect in the final adequacy decision. The EDPB would also welcome a clarification from the Commission that it will continue to assess these elements on an ongoing basis as part of its monitoring role.

4. Given that some legislative changes, legal requirements and safeguards apply similarly under both the government access regime and the LED framework, the corresponding assessments by the EDPB will be incorporated into both this opinion and Opinion 26/2025 to ensure consistency and completeness.

5. The EDPB also notes that pursuant to Articles 47 and 94 of Regulation (EU) 2018/1725[6], European Union institutions, bodies, offices and agencies may transfer personal data to a third country, territory, sector, or international organisation recognised by the Commission under Article 36(3) LED as ensuring an adequate level of protection, provided the transfer solely serves tasks within the controller's competence, without requiring further authorisation. Given the existing cooperation between the Union law enforcement agencies, such as Europol and Eurojust, and their UK counterparts, the EDPB invites the Commission to recall this legal possibility in the recitals of the Draft Decision.

1.2 The scope of this EDPB Opinion

6. In accordance with Article 51(1)(g) LED, the EDPB is expected to provide the Commission with an independent opinion for the assessment of the adequacy of the level of protection in a third country. Due to the specific situation of the UK, the Draft Decision complements the 2021 adequacy decision which still remains valid for the parts not specifically addressed in the Draft Decision. Likewise with this opinion, the EDPB builds upon and further develops its previous opinion[7]. As a result, the EDPB's analysis and comments provided therein generally continue to apply.

7. Taking into account the above, and due to the limited timeframe afforded to the EDPB to adopt this opinion, the EDPB has focused its comments and analysis on selected points presented in the Draft Decision, particularly when further clarification, additional information, or future monitoring by the Commission is required.

[5] Recital 6 of the Draft Decision.
[6] Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('EUDPR'), OJ L 295, 21.11.2018, p. 39.
[7] Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom, adopted on 13 April 2021.

1.3 Relevant developments in the UK legal framework

8. As explained in the Draft Decision[8], following the end of the implementation period agreed in the UK–EU Withdrawal Agreement[9] on 31 December 2020, the UK intended to adopt a new data protection regime which differed from the EU legal framework. The UK has since enacted changes to their existing data protection framework, primarily via the DUAA, which provide limited amendments to different aspects of the framework.

9. This opinion addresses the relevant legislative changes introduced by the DUAA and how these changes affect data protection in the UK framework. Although most of the changes introduced to the UK's data protection framework aim to clarify and facilitate compliance with the law, the EDPB considers that some of the new untested legal changes, which may affect the level of protection, depending on their implementation, should be further clarified and carefully monitored by the Commission. From additional explanations provided by the Commission, the EDPB understands that the Commission intends to scrutinise the development of some of these changes and it invites the Commission to highlight in the final decision the areas which they intend to carefully monitor.

2 RELEVANT DEVELOPMENTS REGARDING THE RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

2.1 Safeguards, rights and obligations

2.1.1 Use of consent in the law enforcement context

10. The EDPB takes note of the explanations given by the Commission regarding the technical changes to the definition[10] of, conditions for obtaining consent[11] and overall alignment of the concept of consent in Part Two and Part Three of the Data Protection Act 2018 ("DPA 2018"), as recitals 35 and 36 of Implementing Decision 2021/1773 remain valid – namely that consent does not constitute in itself a legal basis for the processing, including transfer, of personal data in the context of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

11. The EDPB welcomes that the Commission, similarly to the assessment in 2021, examined the use of consent in a law enforcement context. The EDPB recalls that "the consent of the data subject should not provide a legal ground for processing personal data by competent authorities".[12] Therefore, the EDPB reaffirms the necessity to conduct such an analysis when assessing the level of protection under Article 36 of the LED.[13]

[8] See recital 2 of the Draft Decision.
[9] The implementation period is a period of time agreed in the UK–EU Withdrawal Agreement in which the UK will no longer be a member of the EU but will continue to be subject to EU rules and remain a member of the single market and customs union. See European Union (Withdrawal Agreement) Act 2020.
[10] See section 69(2)(1A) of the Data (Use and Access Act) 2025 that will introduce the following definition of consent: "a freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data" that reads as Article 4(11) UK GDPR 2018.
[11] See section 69(4) of the Data (Use and Access Act) 2025 that will define the conditions for consent.
[12] As the EDPB stated in recital 35 of EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021.
[13] See recital 37 of EDPB Opinion 15/2021.

2.1.2 Onward transfers

12. When a competent authority intends to share personal data processed under Part 3 of the DPA 2018 with law enforcement authorities of a third country, specific requirements apply. In particular, such transfers may take place when they are approved by regulations made by the Secretary of State or, in the absence of such regulations, based on appropriate safeguards. If a transfer can neither be based on a regulation nor appropriate safeguards, it can take place only in certain, specified circumstances, referred to as "special circumstances" corresponding to the situations and conditions qualifying as "derogations" under Article 38 of the LED.

13. While the Commission observes that "the regime on international transfers of personal data from the United Kingdom remains very close to the rules set out in Chapter V of Directive (EU) 2016/680", the Draft Decision also indicates that the legal standard for regulations to approve transfers, which were referred to as adequacy regulations in the former section 74A of the DPA 2018, and appropriate safeguards has been reformulated. Instead of referring to an adequate level of protection, the new "data protection test" set out in section 74AB of the DPA 2018 requires that the standard of protection for data subjects in recipient third countries or international organisations is "not materially lower" than the standard provided for data subjects under the relevant UK data protection legislation.

14. In this context, the EDPB notes that the elements to be considered by the Secretary of State in the adequacy assessment as per section 74AB(2) of the DPA 2018 appear to have been reduced compared to the previous assessment for adequacy regulations.[14] The EDPB points out the removal of certain factors that, in its view, play an important role in assessing whether a third country offers an essentially equivalent level of protection of personal data. These include, in particular, (i) the rules of the third country as regards "public security, defence, national security and criminal law and the access of public authorities to personal data", (ii) the case-law, (iii) the overall assessment of the relevant legal framework, including concerning government access to data, (iv) the existence of effective and enforceable data subjects' rights, (v) and the reference to one or more effective functioning independent supervisory authorities (instead, the new test refers to an "authority responsible for enforcing the protection of data subjects with regard to the processing of personal data").

15. While it is acknowledged that the LED Adequacy Referential provides only limited detail on this aspect, the EDPB recalls its statement that "the onward transfers of personal data by the initial recipient to another third country or international organisation must not undermine the level of protection, provided for in the Union, of natural persons whose data is transferred", which cannot be interpreted as not including the need for an independent supervisory authority, and effective and enforceable data subjects' rights. Therefore, the EDPB encourages the Commission to specifically address these changes and further elaborate its assessment of the new data protection test.

16. The EDPB understands that the new rules on transfers of personal data to third countries are meant to provide additional flexibility. At the same time, the EDPB invites the Commission to monitor the practical application of these rules. This is particularly relevant with regard to the Secretary of State's new authority to make regulations that identify and approve a transfer, based on the new data protection test, by any means, including by reference to geographical sectors within a country; controllers or processors; recipients of the data; types of data; means of transfer; and legal instruments. It remains unclear, for example, how a specific controller or processor based in a third country that is not considered as adequate would meet the data protection test when it comes to

[14] The now-deleted provision of section 74A(4) of the DPA 2018 provided for a list of criteria that was identical to Article 36(3) LED.

effective redress or data subject rights not already established in the legal framework of that third country.

17. Furthermore, the EDPB invites the Commission to clarify in its decision that the criterion of the "desirability of facilitating transfers of personal data to and from the United Kingdom" (Section 74AA(3) of the DPA Act 2018) is not an element of the data protection test, but merely an additional factor the Secretary of State may consider where the test's criteria are fully met, as this is not entirely clear from the text of the law. In this respect, the EDPB invites the Commission to monitor the practical implications of section 74AA(3) of the DPA 2018, as it remains to be seen which role the "desirability of facilitating transfers of personal data to and from the United Kingdom" will play in this context.

2.1.3 Automated decision-making

18. The EDBP takes note of section 80 of the DUAA that introduces important changes to how automated decision-making is regulated in the UK. The EDPB observes that the DUAA takes a more permissive approach, which constitutes a departure from the more restrictive EU approach. Individuals generally lose the right to not be subjected to automated decisions, except in cases involving sensitive data. With the new sections 50A to 50D of the DPA 2018, law enforcement authorities can make significant decisions using automated processes regardless of which lawful basis they rely on, provided they implement appropriate safeguards. These safeguards include providing information to the data subject about the significant decisions taken on the basis of automated means and associated personal data processing, similarly to Article 11 and recital 38 of the LED. Furthermore, the data subject must be given the opportunity to make representations concerning such decisions, to obtain human intervention from the controller to review the automated decision, and to contest such a decision.[15]

19. As a result, the emphasis of the law changes from restricting the use of automated decision-making to ensuring that transparency, human review, and risk controls are in place. Although the Commission acknowledges this shift in recital 43 and analyses it in recital 47, the EDPB invites the Commission to explain in more detail why it considers that the new approach continues to offer a sufficient level of protection. Accordingly, the EDPB encourages the Commission to incorporate a more detailed consideration of this substantial shift in the final adequacy decision.

20. The EDPB also takes note of the discretion granted to the Secretary of State in the context of automated decision-making.[16] It is the understanding of the EDPB that the Secretary of State is granted broad discretion in relation to determine what qualifies as "meaningful human involvement" and a "significant decision with similarly significant effect". The scope and discretion of these powers could give rise to notable concern, e.g. due to their extent, especially in light of the fast-evolving regulatory environment and advancements in automated technologies, such as AI. Therefore, the EDPB invites the Commission to analyse these newly conferred powers to the Secretary of State and monitor any developments in this respect.

21. In this context, the EDPB specifically points to the role and the relevance of the data subject's right to obtain human intervention. The EDPB's adequacy referential under the LED underlines the importance of this right, in particular to express his or her point of view, to receive an explanation of the decision reached after such assessment or to challenge the decision.[17] While the right to obtain human intervention generally continues to be one of the key safeguards in case of automated decision-

[15] Section 50C(2) of the DPA 2018.
[16] See recital 46 of the Draft Decision.
[17] See recital 66 of EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021.

making, the EDPB notes that a new exemption has been introduced in the UK law enforcement framework that permits law enforcement authorities not to apply the safeguards listed in section 50C(2) DPA 2018, for example to avoid the obstruction of an investigation.[18] This exemption now requires that the automated decision is reconsidered with meaningful human involvement "as soon as reasonably practicable" after the decision is made.[19]

22. Introducing such exemptions could pose a risk to the rights and freedoms of data subjects if not closely monitored. To this end, the exemption's requirement for timely reconsideration must be applied carefully to avoid gaps in oversight. If the criteria for this human involvement are interpreted too loosely or the review is delayed, it could lead to inadequate scrutiny and diminish accountability. In this context, the EDPB recalls the case law of the Court of Justice of the EU (CJEU), in particular the Court's PNR judgement, which mandated that a meaningful and substantive human review must precede any actionable outcome from automated profiling or matching systems.[20] The CJEU's stance on prior human review in the PNR context provides important guidance about the implementation of the safeguards concerning automated decision-making laid down in the LED. Since meaningful human intervention is essential for ensuring compliance with safeguards in automated decision-making, the EDPB urges the Commission to include its evaluation of this newly introduced exemption in the decision and to monitor its implementation in practice.

2.1.4 Logging requirements

23. The EDPB recalled in its 01/2021 Recommendations that measures in a third country data protection framework allowing a competent authority to demonstrate its compliance "should include keeping records or logs files of data processing activities for an appropriate period of time".[21] In its Draft Decision, the Commission acknowledges that such an obligation still exists in the UK framework but has been altered by the DUAA as there is no longer an obligation for the data controller to register the specific reason for the consultation or the disclosure of personal data[22]. The removal of this obligation defers from the LED requirements, which provide for comprehensive logging to ensure transparency and accountability. The LED expects detailed records demonstrating lawful processing, including justification for access, to facilitate audits and prevent misuse. The absence of mandatory justification logging under the new regime could make it more challenging to verify whether data was accessed lawfully, both for the controller and for supervisory authorities. The EDPB invites the Commission to further address these reduced logging requirements in its final decision and to monitor whether or not this alteration negatively affects the supervision and the exercise of rights by data subjects.

2.1.5 National security exemptions for law enforcement authorities

24. Section 88 of the DUAA updates the existing national security exemptions under the law enforcement framework to mirror those available under the UK GDPR and the intelligence services regimes.[23] While law enforcement authorities are already able to restrict certain obligations on the grounds of

[18] Article 50C(4)(b) DUAA.
[19] See also Department for Science, Innovation & Technology, Data (Use and Access) Act factsheet: UK GDPR and DPA, published 27 June 2025, p. 14, https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa.
[20] Judgment of 21 June 2022, C-817/19, EU:C:2022:491. para. 179.
[21] See recital 66 of EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021.
[22] See recitals 48 and 49 of the Draft Decision.
[23] See also Department for Science, Innovation & Technology, Data (Use and Access) Act factsheet: UK GDPR and DPA, published 27 June 2025, p. 14, https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa .

protecting national security – such as those concerning data subject rights – section 78A of the DPA 2018 will[24] also include the majority of data protection principles[25] and certain international data transfer requirements[26] as provisions that may be disapplied if required for the purposes of safeguarding national security. In addition, some of the Information Commissioner's powers of entry to conduct inspections and to take enforcement action[27] may be disapplied in such circumstances.

25. These amendments are not mentioned in either the Draft Decision or the draft adequacy decision under Article 45 GDPR. However, the EDPB considers it essential to assess these extended exemptions against the principles of necessity and proportionality. In this context, the EDPB recalls the second of the four so-called "European Essential Guarantees": any limitation on the exercise of rights and freedoms recognised by the Charter must respect their essence and, subject to the principle of proportionality, may be made only if necessary and genuinely meeting objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[28] The EDPB is concerned about the exemptions to key data protection principles, international transfer requirements and the Information Commissioner's powers.

26. Under the revised rule, five of the six data protection principles may be disapplied where necessary to safeguard national security.[29] These principles stipulate, among other things, that the law enforcement purpose for which personal data is collected must be specified, explicit, and legitimate, and that personal data must be adequate, relevant, and not excessive in relation to that purpose. They also specify that personal data must be accurate and retained only for as long as necessary. As mentioned above, the future exemptions additionally encompass some of the international transfer requirements, such as the so-called second condition for international transfers set out in section 73(3) of the DPA 2018. This condition requires that transfers be based either on adequacy regulations, appropriate safeguards, or – if neither of these apply – on special circumstances. The exemptions also affect the powers of the Information Commissioner, e.g., the authority to issue information and enforcement notices.[30]

27. The EDPB notes that while the exemptions clearly deviate from the LED, they are very similar to exceptions and restrictions for national security provided for in Article 11 of the Modernised Convention 108 of the Council of Europe ("Convention 108+")[31], which the UK has signed on 10 October 2018 but which, at the date of this opinion, has not been ratified by the UK or entered into force yet.[32] In this regard, the EDPB recalls that the Consultative Committee of the Convention for the

[24] The DUAA will be phased in over several stages. The main changes to data protection legislation in Part 5 of the DUAA will take effect as part of stage 3, approximately 6 months after Royal Assent, https://www.gov.uk/guidance/data-use-and-access-act-2025-plans-for-commencement.
[25] Section 78A (1),(2)(a),(3) Data Protection Act 2018, as introduced by section 88 DUAA.
[26] Section 78A (1),(2)(d),(4) Data Protection Act 2018, as introduced by section 88 DUAA.
[27] Section 78A (1),(2)(e),(f),(g) Data Protection Act 2018, as introduced by section 88 DUAA.
[28] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, p. 10.
[29] Pursuant to section 78A(2) and (3) Data Protection Act 2018, Chapter 2 of Part 3 of this Act does not apply if required for the purposes of safeguarding national security, except for (a) section 35(1) (the first data protection principle) so far as it requires processing of personal data to be lawful; (b) section 35(2) to (5) (lawfulness of processing and restrictions on sensitive processing); (c) section 42 (safeguards: sensitive processing); and (d) Schedule 8 (conditions for sensitive processing).
[30] Information notices require a controller or processor to provide the Commissioner with information reasonably necessary for the performance of the Commissioner's functions. Enforcement notices empower the Commissioner to require a person to take (or refrain from taking) specific actions, where the Commissioner is satisfied that the person fails to comply with particular data protection obligations.
[31] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).
[32] https://www.coe.int/en-GB/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD) has recently issued Guidelines on the general principles of Article 11 of Convention 108+.[33]

28. In its guidance, the Council of Europe explicitly stresses that no exception is applicable, inter alia, for the proportionality, and the legitimacy of the purpose of the processing principles. That implies that the proportionality of the data processing has to be ensured, as well as the requirements to process personal data for a legitimate purpose. Consistent with the T-PD's guidance, the EDPB remains particularly vigilant regarding any exemptions from the principle of proportionality, as well as from the requirement to process personal data for a legitimate purpose. Likewise, in the EDPB's view, any exemptions from the powers of the supervisory authority should be approached with caution. While specific requirements for supervisory activities – such as security clearances – may be appropriate in the context of national security-related processing, it is essential to ensure effective oversight to prevent the creation of a supervisory vacuum. In the same spirit, Article 11(3) of Convention 108+ stipulates that exemptions to its Article 15[34] are "without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation" of the parties to the Convention. Furthermore, any exemptions should be interpreted as restrictively as possible. The fact that personal data is processed for national security purposes should not on its own be sufficient for an exemption to be invoked. It should be clear that an exemption from the data protection regime has to be applied on a case by case-basis and only if it is necessary and proportionate to do so.[35]

29. Since the draft adequacy decisions do not address this point, the EDPB calls to the Commission to complement its assessment in the Draft Decision as well as to specifically monitor the application in practice of the national security exemptions for law enforcement authorities.

2.1.6 Joint controllerships between UK intelligence agencies and law enforcement authorities

30. Based on the amendments effected by the DUAA, processing activities carried out by authorities competent for law enforcement can, in specific circumstances, fall under the rules normally applicable to the processing of personal data by national security authorities.[36] In other words, subject to the conditions laid down in section 89 of the DUAA, the data protection regime for national security processing established in Part 4 of the DPA 2018 is extended to data processing by law enforcement authorities.

31. The Commission emphasises that the conditions of section 89 of the DUAA provide strict safeguards: a competent authority has to be specified as "qualifying competent authority" in regulations made by the Secretary of State, who, additionally, has to designate a particular processing activity carried out

[33] https://rm.coe.int/t-pd-2021-7rev13-interpretation-of-general-principles-article-11-c108-/1680b6c146.
[34] Article 15 of Convention 108+ specifies how the parties to the Convention, by providing for one or more supervisory authorities, shall ensure compliance with the Convention's provisions.
[35] See also Article 11 of Convention 108+ that specifies that exceptions need to be provided for by law, respect the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society. According to the TP-D`s guidelines on the general principles of Article 11, this implies that a weighing of the interests involved between the need to provide for exceptions to certain provisions of the Convention and respect for the human rights and fundamental freedoms of individuals must be carried out and justified.
[36] See recital 72 of draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679, which is equally relevant to both EDPB Opinions in this regard (see also section 4 above).

by the qualifying competent authority as a joint controller with at least one intelligence service for the purpose of safeguarding national security.[37]

32. While acknowledging that these safeguards entail significant restrictions, the EDPB invites the Commission to monitor the practical implementation of these rules. Particular attention should be paid to ensuring that Part 4 of the DPA 2018 is applied strictly to processing operations for national security purposes, without being extended to other contexts. Although States are granted a broad margin of discretion in national security matters, as also recognised by the European Court of Human Rights[38], the EDPB takes the view that threats to national security must be distinguishable by their nature, their seriousness, and the specific circumstances from general risks for public security, or from serious criminal offences. Only in such cases is the operation of law enforcement authorities under the intelligence services data protection regime compatible with the principles of necessity and proportionality[39]. In addition, the EDPB considers it necessary to monitor whether qualifying competent authorities are able in practice to maintain a clear distinction between different processing purposes in order to adhere to the corresponding legal framework accordingly.

2.1.7 The right of access

33. The DUAA specifies that data subjects are only entitled to the relevant information as far as the controller is able to provide those based on a reasonable and proportionate search. This amendment is introduced in both the law enforcement and national security regime.[40]

34. The Commission explains this as a clarification in line with established standards developed under domestic case-law, which take into account also the interests of the data subject. Still, the EDPB would have welcomed more detailed information as to how the notion of "reasonable and proportionate search" is interpreted, also since Article 14 of the LED does not contain such element. The EDPB recognises that there may indeed be scenarios in which the efforts of a controller to identify and locate information about the data subject could be considered unreasonable and disproportionate without compromising essential equivalence.[41] Nevertheless, it is important to define adequately the notion of a "reasonable and proportionate search", which, in the EDPB's view, should be interpreted narrowly and in a sufficiently uniform manner. Competent authorities should have a consistent understanding of what is "reasonable and proportionate", whether informed by case-law or by guidance from a supervisory authority, as the application of this notion could potentially lead to different standards in complying with the right of access, in particular depending on the level of technical and organisational measures the controller put in place to handle access requests. The EDPB invites the Commission to monitor that the right of access is not unduly limited.

2.1.8 Oversight and redress

35. The EDPB notes that the system of oversight of criminal law enforcement agencies under the DPA 2018 and the Investigatory Powers Act 2016 as well as the redress mechanisms, available under Part 3 of the DPA 2018, the Investigatory Powers Act 2016 and the Human Rights Act 1998, remain largely

[37] See recital 73 of draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679, which is equally relevant to both EDPB Opinions in this regard (see also section 4 above).
[38] ECtHR, Big Brother Watch and others v. The United Kingdom, 25 May 2021, § 350.
[39] It stems from the case-law of the CJEU, when applying the necessity and proportionality test to Member States' legislation allowing for retention and access to personal data by public authorities, that legitimate objectives, such as national security or fighting serious crimes, are different and, and might therefore justify different types of interference. See CJEU, joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, 6 October 2020.
[40] Section 78(3) and (4) of the DUAA, amending sections 45 and 94 of the Data Protection Act 2018.
[41] For instance, it might be argued that this is the case for searching seized devices that have not yet been analysed or decrypted.

unchanged. In particular, the oversight in the UK continues to be ensured, in addition to the Information Commissioner's Office ("ICO"), by a combination of different Commissioners, namely the Investigatory Powers Commissioner ("IPC"), assisted by other Judicial Commissioners, as well as the Biometrics and Surveillance Camera Commissioner.

36. As explained by the Commission in recital 97 of the Draft Decision, the Investigatory Powers Amendment Act 2024 has made only limited modifications, in particular through the introduction of deputy IPCs to which the IPC can delegate specific powers when they are unable or unavailable to carry out their functions. Such deputy IPCs must be Judicial Commissioners and are appointed by the IPC.

37. The EDPB positively notes that the previous ideas under the Data Protection and Digital Information Bill, which preceded the DUUA, to abolish the Biometrics and Surveillance Camera Commissioner and to transfer the role to the Investigatory Powers Commissioner, has been discarded[42]. In this regard, the EDPB invites the Commission to give further attention and to provide more detailed assessment of the role of the Biometrics and Surveillance Camera Commissioner in the system of oversight during its monitoring and future reviews of the Draft Decision.

38. As already emphasised by the EDPB in Opinion 14/2021, the ICO is well equipped with the necessary powers, which closely correspond with the powers of EU Member States supervisory authorities as set forth in Article 58 GDPR. At the same time, as already highlighted by the EDPB, that the existence of effective sanctions plays an important role in ensuring respect for rules[43].

39. The EDPB positively notes the transparency policy of the ICO and the availability of statistical and analytical data, including examples, of the ICO's enforcement activities vis-a-vis law enforcement bodies[44]. In that regard, the EDPB observes a preference of the UK SA for reprimands in case of breaches of data protection legislation by police forces. A notable exception is the Enforcement Notice issued to the Crown Prosecution Service in January 2024[45]. The EDPB also considers it positive that, since the adoption of the Implementing Decision 2021/1773, the ICO has published numerous codes of practices, guidelines, opinions and other guidance documents for the relevant parties.

40. The EDPB also notes that with the entry into force of the DUAA, the independent oversight of the ICO, previously structured as a corporation sole, will be transformed into a new structure through the introduction of a body corporate, namely the Information Commission (IC)[46].

41. The EDPB provides an initial analysis of the possible implications of this change in its Opinion 26/2025 regarding the Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom. The observations and the recommendations in that opinion are fully valid also in the context of the oversight and supervision in the law enforcement area.

42. In particular, the EDPB invites the Commission to supplement the draft adequacy decision with further details specifically on the structure and organisation of the IC, the appointment and dismissal of the members of the IC, especially on the appointment of non-executive members of the IC by the Secretary of State. The EDPB also considers that the Commission should pay particular attention in its future reviews to the balancing by the IC of the different tasks and interests. Furthermore, the EDPB calls on

[42] See https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner.
[43] EDPB Opinion 14/2021, para. 112.
[44] See e.g. the detailed data protection complaints data sets available at https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-protection-complaints/
[45] https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/.
[46] See new Article 114A DPA 2018 and Section 6 of the DUAA.

the Commission to follow up on the results of the public consultation published by the ICO on 22 August 2025 regarding handling of complaints[47] and to monitor the resulting policies of the IC.

43. In the light of the above, the EDPB reiterates the need for the Commission to closely monitor the application of corrective powers and of remedies for affected parties in the UK data protection framework.

3 REVIEW, DURATION AND RENEWAL OF THE DECISION

44. The EDPB notes that the present Draft Decision applies for six years, with an expiration date set for 27 December 2031, and notes that the UK continues being the only third country whose adequacy decisions contain a sunset clause. The EDPB understands that the new legal framework deserves specific attention and calls on the Commission to carefully monitor the implementation of the DUAA, including the areas of focus highlighted in this opinion and all relevant developments in the UK in this regard. The EDPB also takes note that the "sunset clause" is combined with the mandatory periodical review set out in Article 36(3) of the LED, which should take place at least every four years.

45. The EDPB understands that the Commission's intention is to conduct a review at the end of the four year-period on the basis of which it will prepare a public report. The EDPB welcomes the intention to carry out the review, which serves a different purpose than the sunset clause and plays an important role in monitoring the legal framework, particularly in terms of accountability. The EDPB, therefore, urges the Commission to conduct the review within the legal timeframe specified in Article 36(3) of the LED, also taking into account the elements already outlined in Commission Implementing Decision 2021/1773[48] as well as any further relevant developments.

46. In addition, it is the understanding of the EDPB that the analysis in Commission Implementing Decision 2021/1773 concerning the suspension and repeal of the decision[49] is still valid. For the sake of legal certainty, the EDPB believes that such a clarification could appear in the final adequacy decision.

47. The EDPB welcomes that recital 68 of the Draft Decision refers to the role of the EDPB, as well as civil society groups and other stakeholders in the periodic review mechanism, in accordance with EDPB Recommendations 01/2021[50]. Concerning the practical involvement of the EDPB and its representatives in the preparation and proceeding of the future review, the EDPB reiterates that any relevant documentation should be shared in writing with the EDPB sufficiently in advance of the review.

48. Given the specific characteristics of this Draft Decision, the EDPB invites the Commission to detail and clarify as much as possible the elements relating to the duration, monitoring, suspension, revocation, amendment and renewal of the decision.

For the European Data Protection Board

The Chair

Anu Talus

[47] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2025/08/ico-consultation-on-draft-changes-to-how-we-handle-data-protection-complaints/; https://ico.org.uk/media2/nrljbhr2/proposed-dpt-framework-20250822.pdf.
[48] See recitals 165 to167 of Commission Implementing Decision 2021/1773.
[49] See ibid, recitals 168 to 171.
[50] Recital 19 of EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021.