Opinion 26/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the United Kingdom

Adopted 16 October 2025

Executive summary

On 22 July 2025, the European Commission started the process towards the adoption of its draft implementing decision on the adequate protection of personal data by the United Kingdom (UK) pursuant to Article 45(2) GDPR. This Draft Decision extends the validity of certain parts of the previous adequacy decision of 28 June 2021 by way of reference until December 2031.

On the same date, the European Commission asked for the opinion of the European Data Protection Board. The EDPB's assessment of the adequacy of the level of protection afforded by the UK has been made on the basis of the examination of the draft decision itself as well as on the basis of an analysis of the documentation made available by the European Commission.

The EDPB focused on the assessment of both, the general data protection aspects of the draft decision and the access by public authorities to personal data transferred from the EEA to the UK for the purposes of law enforcement and national security, including the legal remedies available to individuals in the EEA.

The EDPB also assessed whether the safeguards provided under the UK legal framework are in place and effective.

The EDPB has used as main reference for this work its GDPR Adequacy Referential ("GDPR Adequacy Referential") adopted on 28 November 2017, as last revised and adopted on 6 February 2018 and the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

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, this opinion highlights several points that require further analysis, as well as some issues that the Commission should closely monitor in the coming years as part of its monitoring obligation under article 45(4) GDPR.

The EDPB notes that the UK introduced changes regarding the "inherited" EU general legal framework by virtue of the Retained EU Law (Revocation and Reform) Act 2023 ("REUL Act"), which - inter alia - removes the principle of primacy of EU law (with guarantees for some GDPR provisions) and removes the direct application of the principles of EU law, including the right to privacy and data protection as derived from the Charter of Fundamental Rights. The EDPB invites the Commission to explain and make a more detailed assessment of the changes brought by the REUL Act and assess their impact on the UK legal framework generally and its data protection framework more specifically. The EDPB also considers this an area to be closely monitored in the future by the Commission.

The EDPB notes that the Secretary of State has been granted new powers to introduce changes to the new data protection framework via secondary regulations, which require less Parliamentary scrutiny, in certain cases, for instance, international transfers, automated decision-making, and the governance of the IC. The EDPB invites the Commission to highlight in the final Adequacy Decision the areas which they intend to carefully monitor because there is a risk of further divergence with the EU data protection law via secondary UK legislation.

The EDPB observes changes to the rules governing transfer of personal data, 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 UK adequacy test[1]. This applies both to third country transfers carried out under the UK GDPR and to transfers of data processed for law enforcement purposes. The EDPB encourages the Commission to specifically further elaborate its assessment on these aspects and monitor the developments and the practical implementation of this new adequacy test.

The EDPB invites the Commission to make a more detailed assessment of the restructuring of the Information Commissioner's Office ("ICO") as a board and the rules for appointment and dismissal of executive and non-executive board members. The EDPB also invites the Commission to provide more detail on the ICO's recent consultation, issued after this draft decision, to introduce a new triage system for complaints handling. The EDPB invites the Commission to monitor all these changes once they come into effect. While positively noting the transparency policy of the ICO and the availability of the statistical and analytical data of its enforcement activities, the EDPB also invites the Commission and to make a more detailed assessment and monitor the application of corrective powers, effectiveness of sanctions and of remedies for affected parties in the UK data protection framework.

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 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. The EDPB calls on the 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. The EDPB invites the Commission to monitor 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.

The EDPB welcomes the clarifications reached between the UK and U.S. in the context of the UK-U.S. Cloud Act Agreement, which provide further legal clarity. At the same time, the EDPB would like to recall the need to improve the level of safeguards provided by the EU-U.S. Umbrella Agreement, whose privacy and data protection safeguards are incorporated into the UK-U.S. Cloud Act Agreement. Overall, the EDPB sees a need for clarification as to the Commission's assessment of the UK-U.S. Cloud Act Agreement and any possible impact on the level of protection. The EDPB invites the Commission to continue to include the UK-U.S. Cloud Act Agreement in its future assessments and reviews.

As recently pointed out in Statement 05/2024, the EDPB considers encryption to be essential for ensuring the security and confidentiality of personal data and electronic communications. Technical Capability Notices under the IPA 2016 compelling companies to provide the ability to remove encryption at the government's request create systemic vulnerabilities and pose a direct threat to the

[1] (i) the rules of the third country as regards '"public security, defence, national security and criminal law and access to personal data by public authorities'", (ii) case-law, (iii) the existence of effective and enforceable rights enjoyed by data subjects and the administrative and judicial remedies that data subjects whose personal data are transferred may actually bring, and (iv) one or more independent supervisory authority.

integrity and confidentiality of electronic communications. Such developments merit attention in the adequacy decision, particularly in light of Article 45(2)(a) GDPR, which requires an assessment not only of the legal framework on paper but also of its implementation, and should be monitored.

The EDPB notes that the Investigatory Powers Amendment Act 2024 introduced a specific regime for the retention and examination of bulk personal datasets for which the individuals to whom the personal data relates "could have no, or only a low, reasonable expectation of privacy". The EDPB sees a need for further clarifications with regard to the relevant changes, in particular regarding the concepts of "individual authorisations" and "category authorisations". Furthermore, the EDPB invites the Commission to closely monitor the implementation of the term "low or no reasonable expectation of privacy" in practice.

Table of contents

The European Data Protection Board

Having regard to Article 70(1)(s) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area Agreement (EEA) and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[2],

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

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. SCOPE OF THE COMMISSION'S DRAFT DECISION

1. On 22 July 2025, the European Commission ("Commission") requested the opinion of the European Data Protection Board ("EDPB") on the draft Implementing Decision amending Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to the GDPR on the protection of personal data by the United Kingdom ("Draft Decision"). In its Draft Decision, the Commission concluded that the UK continues to ensure an adequate level of protection for personal data transferred from the European Union into the UK within the scope of the GDPR.

2. The EDPB notes that this Draft Decision extends by 6 years the validity of Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to the GDPR on the protection of personal data by the United Kingdom ("previous UK Adequacy Decision"), which was due to expire on 27 June 2025 (sunset clause). The previous UK Adequacy Decision had been extended by a period of six months, until 27 December 2025 by virtue of Decision (EU) 2025/1225 on 24 June 2025, to allow the UK to finalise its data protection reforms[3].

3. In its Draft Decision, the Commission assessed "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. The Commission focused its assessment on new developments in the UK data protection legislation and notably those introduced by the Data (Use and Access) Act 2025 ("the DUAA"). The Commission specifically considered the elements listed in recital 281 of the previous UK Adequacy decision which all feature in the Draft Decision.

5. The EDPB agrees that the main focus of the assessment should be on all new relevant developments in the UK legislation and the elements highlighted in the previous UK Adequacy Decision insofar as all elements set out in Article 45(2) GDPR are assessed. The EDPB therefore would welcome if in its final

[2] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".
[3] The EDPB, upon request, issued "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".

Adequacy Decision the Commission explicitly clarifies that all the elements listed in Article 45(2) GDPR were assessed in order to conclude 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. The EDPB would also welcome clarification from the Commission that it will be assessing these elements on an ongoing basis as part of its monitoring role.

1.2. SCOPE OF THIS EDPB OPINION

6. 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[4], and to identify insufficiencies in the adequacy framework, if any, and endeavour to make proposals to address these[5]. Due to the specific situation of the UK, the new adequacy decision complements the 2021 adequacy decision which still remains valid for the parts not specifically addressed in this draft decision. Likewise with this Opinion, the EDPB builds upon and further develops its Opinion 14/2021[6]. As a result, the EDPB's analysis and comments provided in its previous Opinion concerning the previous UK Adequacy Decision generally remains relevant.

7. Taking into account the above, the EDPB has focused its comments on selected points presented in the Draft Decision, particularly when further clarification, additional information, or future monitoring by the European Commission is required.

8. The EDPB also notes that pursuant to Articles 47 and 94 of Regulation (EU) 2018/1725[7], European Union institutions, bodies, offices and agencies may transfer personal data to a third country, territory, sector, or international organisation recognised by the European Commission under Article 45(3) GDPR as ensuring an adequate level of protection, provided the transfer solely serves tasks within the controller's competence, without requiring further authorisation. The EDPB invites the Commission to recall this legal possibility in the recitals of the final Adequacy Decision.

1.3. DEVELOPMENTS IN THE UK LEGAL FRAMEWORK

9. 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

[4] See Article 70(1)(s) GDPR.
[5] See Article 29 Working Party, Adequacy Referential, chapter 2 Procedural aspects for adequacy findings under the GDPR., adopted on 28 November 2017, as last revised and adopted on 6 February 2018, WP254 rev.01 (endorsed by the EDPB, see https://edpb.europa.eu/our-worktools/general-guidance/endorsed-wp29-guidelines); (hereinafter "GDPR Adequacy Referential").
[6] Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, adopted on 13 April 2021, https://www.edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf.
[7] 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.
[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.

regime which would diverge from the EU legal framework. Eventually, the UK enacted limited changes to their existing data protection framework, notably by virtue of the DUAA.

10. Beyond data protection, one of the most important changes to the UK's legal framework, since the previous UK Adequacy Decision was adopted, regards the "inherited" EU general legal framework (called "retained EU law") i.e. legal provisions integrated into UK law via the European Union (Withdrawal) Act 2018. Retained EU law encompassed the general principles of EU law, including the fundamental rights deriving from the EU Charter of Fundamental Rights ("the Charter[10]") and the principles of proportionality and necessity, which have been influential in the development and the interpretation of data protection law in the UK. Under the European Union (Withdrawal) Act 2018, Retained EU law had maintained its status of supremacy over secondary UK legislation and retained EU law was to be interpreted in line with the general principles of EU law. However, since the introduction of the Retained EU Law (Revocation and Reform) Act 2023 ("REUL Act")[11], the UK has removed the direct application of the principles of EU law from its domestic law including the fundamental rights deriving from the Charter. The REUL Act also removed the principle of primacy of EU law, as retained EU law (now called "assimilated law") must now be read compatibly with domestic UK law and not in line with principles of EU law. This constitutes a significant change in the UK legal order.

11. In addition, although currently on hold, a new more relaxed legal test for judges of the Court of Appeal and Supreme Court to depart from retained EU case-law could be introduced by virtue of the REUL Act[12]. This change, if enacted, has the potential to be a significant change in the UK.

12. Despite these changes, the EDPB welcomes the inclusion of guarantees in the REUL ACT to ensure that data protection legislation is not overridden in certain circumstances. These guarantees include the requirements that any piece of legislation "which imposes a duty, or confers a power, to process personal data does not override a requirement under the main data protection legislation relating to the processing of personal data" and that the data protection framework continues to override other UK legislation[13]. Nevertheless, the EDPB notes that these guarantees also include two exceptions, (i) where the UK Parliament can choose to deliberately override data protection requirements[14] and (ii) where certain provisions of the DPA 2018 are exempt and as such will take precedence over the UK GDPR[15]. The implications of the second exemption are still uncertain and debated in the UK.

13. Regarding the protection of fundamental rights enshrined in the Charter, Recital 12 of the Draft Decision explains that any references to fundamental rights and freedoms in the UK GDPR and DPA 2018 were replaced with references to rights under the European Convention of Human Rights, incorporated in domestic legislation under the Human Rights Act 1998[16].

14. The EDPB invites the Commission to make a more detailed assessment of these changes to the UK legal order described under §10, 11 and 12 above in order to explain the changes brought by the REUL Act

[10] Charter of Fundamental Rights of the European Union *(*OJ C 326, 26.10.2012, pp. 391–407).
[11] See Recital 11 of the Draft Decision.
[12] See Section 6 The Retained EU Law (Revocation and Reform) Act 2023 (Commencement No. 2 and Saving Provisions) (Revocation) Regulations 2024.
[13] See Section 183A DPA 2018 as introduced by Section 106(2) DUAA.
[14] See Section 183(A)(3) DPA 2018 as introduced by Section 106(2) DUAA.
[15] These provisions are listed in Section 186(3) DPA 2018. This means that when there is a conflict between Article 23 UK GDPR and one of the listed sections, for example, Schedule 2 DPA 2018 containing the exemptions to data subject rights, the interpretation of the DPA 2018 will take precedence.
[16] See Article 8 of the European Convention of Human Rights.

and assess their impact on the UK data protection framework. The EDPB also considers this an area to be closely monitored in the future by the Commission and invites the Commission to do so.

15. Finally, the EDPB notes several changes under the DUAA on the legal framework applicable to electronic communications, including cookies, and recalls that the processing of personal data might trigger the material scope of the UK GDPR[17]. Therefore, it invites the Commission to include them in its assessment for the final decision insofar as they could have an impact on data protection. The EDPB further calls on the Commission to closely monitor the practical effect of the changes related to cookies exempt from consent.

1.4. GENERAL COMMENTS AND CONCERNS

1.4.1. INTERNATIONAL COMMITMENTS ENTERED INTO BY THE UK

16. In relation to international commitments entered into by the UK [18], the EDPB welcomes that the UK continues to adhere to the ECHR and to be under the jurisdiction of the ECtHR. In addition, the UK has also adhered to Convention 108[19] and its Additional Protocol[20] as well as has signed Convention 108+[21] in 2018. These international commitments are important considerations[22] and should be taken into account as part of the assessment for the renewal of both UK adequacy decisions under the GDPR and the LED.

17. Overall, the EDPB supports efforts towards a prompt ratification of Convention 108+ by third countries as a meaningful step towards aligning with internationally recognised data protection principles, and as a signal of their engagement with broader standards and fundamental rights.

1.4.2. POWERS OF THE SECRETARY OF STATE TO INTRODUCE CHANGES TO THE DUAA VIA SECONDARY REGULATIONS

18. Although most of the changes introduced to the UK's data protection framework aim to clarify and facilitate compliance with the law, some may have an impact, depending on their implementation, on the standard of protection of personal data in the UK.

19. In this regard, the EDPB notes that the Secretary of State has been granted new powers to introduce changes to the DUAA via secondary regulations, which require less Parliamentary scrutiny. In certain cases, for instance, international transfers (see section 2.3), automated decision-making (section 2.4.), and the governance of the IC (section 3), these new powers are broad with no further information provided in the Draft Decision as to what safeguards will be put in place and how these powers are intended to be used in practice.

---

[17] EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019 available at https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf .

[18] See Chapter 1: Some broad information in relation to the concept of adequacy of the Adequacy Referential.

[19] See Convention for the protection of individuals with regard to the processing of personal data, Convention 108, 28 January 1981.

[20] See Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, opened for signature on 8 November 2001.

[21] See Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108+"), 18 May 2018.

[22] See Recital 105 GDPR.

20. The EDPB invites the Commission to highlight in the final Adequacy Decision the areas which they intend to carefully monitor because there is a risk of further divergence with the EU data protection law via secondary UK legislation.

2. GENERAL DATA PROTECTION ASPECTS

2.1. RECOGNISED LEGITIMATE INTERESTS

2.1.1. GENERAL REMARKS

21. In recitals 22, 23 and 24, the Commission focuses its assessment on the introduction of a new legal basis, i.e. processing necessary for the purposes of a recognised legitimate interest. Annex 1 of the updated UK GDPR lists those recognised legitimate interests.

22. According to the ICO's guidance on this topic[23] data controllers relying on a recognised legitimate interest as a legal basis are still required to comply with all the other requirements under the UK GDPR, including ensuring the processing is necessary and proportionate to achieve the pre-approved purpose. As this is not recalled in the Draft Decision and constitutes an essential element to the conclusion that this new legal basis does not undermine the level of protection of data subjects' rights, the EDPB invites the Commission to clarify this point.

23. Listing recognised legitimate interests in the law does not appear problematic in itself, nor does the decision to introduce such new legal basis – which brings greater clarity for controllers and should be welcomed.

24. However, the EDPB takes note that certain recognised legitimate interests consist of: (i) the necessity to process personal data for safeguarding national security, protecting public security or for defence reasons ("national security, public security and defence condition"); (ii) the necessity to process personal data to detect, investigate or prevent a crime ("crime condition"); and (ii) the "disclosure for purposes of processing described in Article 6(1)(e)".

25. As regards the "national security, public security and defence condition" and the "crime" condition, the EDPB notes that no further information on the practical use of these legal bases by controllers and processors has been included in the Draft Decision. The EDPB would appreciate if the Commission could provide further details on the additional information and guarantees received on the practical application of this legal basis from the UK competent authorities and invites the Commission to monitor the application of this legal basis.

26. The EDPB also notes that the ICO is working on specific guidance on this matter, which - at the time of this Opinion - include a definition of such concepts. Given the importance of clarifications around these concepts, the EDPB calls on the Commission to closely monitor the development of the ICO's guidance.

[23] See ICO guidance on legitimate interests, available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/.

2.1.2. DISCLOSURE FOR PURPOSES OF PROCESSING DESCRIBED IN ARTICLE 6(1)(E)

27. The EDPB observes that the newly established recognised legitimate interest that allows "disclosure for purposes of processing described in Article 6(1)(e)" introduces the possibility of sharing personal data with public authorities on a voluntary basis. As the ICO clarifies in its recent guidance[24], this recognised legitimate interest does not in itself confer upon requesting authorities a right of access to personal data, but a controller may invoke this pre-approved interest where authorities indicate they require data for the performance of their public tasks or functions. The EDPB also notes that such public task disclosure requests may not only be issued for personal information intended to be used for purposes covered by the UK GDPR, but may also relate to processing purposes under Part 3 and Part 4 of the Data Protection Act 2018. Consequently, this amendment is also relevant with regard to government access for law enforcement and national security purposes.[25]

28. In this context, the question arises as to which criteria the controller has to assess in order to decide whether to voluntarily provide data in response to a request for information. In particular, as the ICO points out in its guidance[26], the EDPB understands that the necessity test for this recognised legitimate interest condition is different from the other conditions specified in Annex 1. For public task disclosure requests, necessity means the controller has to examine what processing is necessary to disclose the personal information requested. The controller has to consider whether the information they wish to share is proportionate and necessary to meet the request. The necessity test does not, by contrast, extend to whether the personal data is actually necessary to perform the public task or function, as the controller may rely on the requester's declaration that it needs the personal information for a specified public task[27]. In fact, in many cases, particularly where requests are made for law enforcement or national security purposes, the controller will not be in a position to conduct such assessment.

29. Against this background, the EDPB calls upon the Commission to closely monitor the practical application of this provision.

30. In the opinion of the EDPB, law enforcement and national security authorities should not utilise this mechanism to circumvent existing legal restrictions on their binding data collection powers or to obtain more data than is strictly necessary for fulfilling their tasks. Furthermore, the EDPB considers it important that controllers take into account the ICO`s guidance on how to validate a public task disclosure request and invites the Commission to include this aspect into the periodic review of the decision.[28]

2.2. INDIVIDUAL RIGHTS

31. The EDPB acknowledges the Commission's analysis that there have been limited amendments in the area of individual rights. This includes changes to Article 12 and a new 12A UK GDPR which further

[24] See footnote 23.
[25] See ICO guidance on Public task disclosure request condition, available at https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/what-are-the-recognised-legitimate-interest-conditions/public-task-disclosure-request-condition/ .
[26] See footnote 23.
[27] See footnote 23.
[28] The ICO in its guidance on Public task disclosure request condition (see footnote 25) clarifies that controllers should, e.g., ask for the request to be put in writing and make checks to ensure the authenticity of the request or the authority of the organisation's employee to act on its behalf.

detail the time limits for replying to data subjects' requests.[29] Additionally, Article 13(5) UK GDPR includes an exemption to the right to information if personal data is processed for purposes of scientific or historical research under further safeguards in Article 84B UK GDPR. The EDPB considers both changes to not undermine the essentially equivalent level of protection provided by the UK GDPR.

2.2.1. RIGHTS OF ACCESS

32. Article 15(1A) UK GDPR introduces a proportionality assessment, as developed under UK domestic case law. Notably controllers only have to carry out "reasonable and proportionate searches" in order to comply with access requests.

33. The EDPB notes that such a proportionality assessment is not present in the EU data protection framework which does not foresee any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subjects' request under Art. 12 GDPR but only provides grounds for refusal in its subsection 5.[30]

34. Therefore, in the EDPB's view, it is important to define adequately the notion of "reasonable and proportionate searches", which should be interpreted narrowly and in a sufficiently uniform manner. Controllers 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 would welcome if the Commission could provide more detailed information on the interpretation of "reasonable and proportionate searches" based on the domestic guidance and case law available. Against this background, the EDPB invites the Commission to monitor that the right of access is not unduly limited.

2.2.2. SAFEGUARDS FOR "IMMIGRATION EXEMPTION"

35. The former so-called "immigration exemption"[31] allowed controllers involved in "immigration control" to restrict certain data subjects' rights provided by the DPA 2018, if this would be likely to prejudice certain immigration control activities[32]. Due to challenges to its legality at the time of the adoption of the previous UK Adequacy Decision, the processing of personal data under the exemption was excluded from the scope of that decision.

36. Since the previous UK Adequacy Decision, the immigration exemption has been supplemented by safeguards twice[33]. It now incorporates the following safeguards: (i) it must only be invoked on a case by case basis, (ii) the data subject's rights and freedoms and potential vulnerabilities are taken into account (iii) the Secretary of State keeps a record on the use of the immigration exemption and to

[29] Most notably due to the need for confirming a data subject's identity or the payment of a fee.
[30] Article 12(5) GDPR "*Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.*"
[31] See Schedule 2 to the DPA 2018, Part 1 of the previous version of the DPA.
[32] See paragraphs 61 and 62 of EDPB Opinion 14/2021 "prejudice the maintenance of effective immigration control" or "the investigation or detection of activities that would undermine the maintenance of effective immigration control".
[33] Through regulations in 2022 as well as 2024.

generally inform the data subject about its use and (iv) clarification that the use of the immigration exemption is restricted to the processing by the Secretary of State (including the UK Home Office and its agencies). Additionally, the necessary balancing exercise for determining whether the exercise of data subject's rights is likely to prejudice effective immigration control was detailed. The ICO also issued detailed guidance on the use of the exemption. In its guidance, it confirmed the narrow interpretation of the exemption and that restrictions by way of the immigration exemption should only be applied selectively to specific data subject rights. It also stated that when carrying out the balancing test controllers must ensure that the risk to immigration control is substantial and outweighs the risk to the person's interests.

37. The EDPB acknowledges the detailed analysis by the Commission. Against the backdrop of the legal challenges preceding those changes, the EDPB encourages the Commission to monitor its further application.

2.3. RESTRICTIONS ON ONWARD TRANSFERS

38. The EDPB welcomes the Commission's continued attention to the practical application of the UK's rules on transfers of personal data to third countries and it encourages the Commission to maintain and deepen this engagement. This is particularly relevant with regard to the Secretary of State's authority to issue new targeted regulations to approve transfers (i) to a specific sector or geographic area within a third country; (ii) to a specific controller or processor; (iii) to a specific recipient of the personal data; (iv) of certain specific types of personal data; (v) made by certain specific means; or (vi) on the basis of relevant legislation, schemes, lists or other arrangements or documents, as they have effect from time to time; and to confer a discretion on a person (Article 45A(4) UK GDPR).

39. The EDPB understands that Article 45A(4) UK GDPR is meant to enable flexibility to approve certain transfers. For example, regarding points (ii) and (iii), the EDPB understands that they could cover transfers to private entities in a third country. This would mean that such private entities provide commitments to conform to the data protection test. It remains unclear how the Secretary of State would assess in practice that specific controllers based in a third country - not considered as adequate - can conform to the data protection test (for instance, with regard to redress). Likewise, it remains unclear how the data protection test would be carried out for point (iv) and (v) of Article 45A(4) UK GDPR.

40. The EDPB would appreciate if the Commission could provide further details on the additional information and guarantees received on the practical application of the data protection test and explain its assessment as to how the level of protection is upheld in such situations.[34] The EDPB also invites the Commission to closely monitor the developments in the application of this provision.

41. Furthermore, the EDPB understands from additional information provided by the Commission that the criterion of the "desirability of facilitating transfers of personal data to and from the United Kingdom" 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. The EDPB invites the Commission to clarify this in its final Adequacy Decision as it is not entirely clear from the text of the law as well as to monitor its practical implication and implementation of such criterion.

[34] See Article 45(A)4 UK GDPR.

42. Regarding the new data protection test introduced by the DUAA[35], the EDPB notes that the new indicative list of elements to be considered in the adequacy test is not exhaustive and that the new adequacy test provides 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 United Kingdom data protection legislation. This list removes important elements that figured in the previous UK adequacy test and which play an important role in assessing whether a third country offers an essentially equivalent level of protection of personal data. The new test no longer refers to (i) the rules of the third country as regards "public security, defence, national security and criminal law and access to personal data by public authorities", (ii) case-law (instead now the new test refers to "constitution, traditions and culture of the country"), (iii) the existence of effective and enforceable rights enjoyed by data subjects and the administrative and judicial remedies that data subjects whose personal data are transferred may actually bring (instead the new test refers to (b) the existence, and powers, of an authority responsible for enforcing the protection of data subjects with regard to the processing of personal data in the country or by the organisation, (c) arrangements for judicial or non-judicial redress for data subjects in connection with such processing), and (iv) one or more 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 in the country or by the organisation").

43. While it is acknowledged that the GDPR Adequacy Referential provides only limited detail on this aspect, the EDPB recalls its reference to "the level of protection of natural persons whose data is transferred must not be undermined by the onward transfer"[36] which cannot be interpreted as not including the need for an independent supervisory authority and effective and enforceable data subjects' rights.

44. The EDPB encourages the Commission to specifically further elaborate its assessment on these aspects. Such clarification would provide great legal certainty and contribute to reinforce trust in the adequacy instrument. The EDPB also invites the Commission to closely monitor the developments and the practical implementation of the new adequacy test.

45. As regards the UK (associate) membership to the CBPR, the EDPB notes that the current membership does not entail any facilitation of data transfers from the United Kingdom to other members of the CBPR Forum. The EDPB welcomes the position taken by the Commission in this regard, including the commitment to continue to closely monitor further developments in this regard, especially if the UK intends to progress to a full member, and recalls that CBPRs are not recognised as ensuring a sufficient level of protection for personal data originating from the EU.

2.4. AUTOMATED DECISION MAKING

46. The EDPB takes note of Section 80 of the DUAA (introducing Articles from 22A to 22D UK GDPR) which introduces significant changes to the framework governing automated decision making ("ADM"), particularly when based on the processing of non-special categories of data. Up until the DUAA was adopted, Article 22 UK GDPR was echoing the EU data protection framework with a general prohibition on ADM with limited exceptions.

[35] See Recital 42 of the Draft Decision.

[36] See Chapter 3: General Data Protection Principles to ensure that the level of protection in a third country, territory or one or more specified sectors within that third country or international organization is essentially equivalent to the one guaranteed by the EU legislation, of the GDPR Adequacy Referential.

47. Article 22B(1) UK GDPR prohibits the processing of special categories of personal data for decisions based solely on automated processing that have legal or similarly significant effects for the data subject with certain exceptions (Article 22B(2)(3) UK GDPR, including when the processing is based on consent, contract, or required by law).

48. The EDPB observes that this prohibition does not apply when controllers make significant decisions using automated processes based on non-special categories of data, unless the legal basis for the processing is a recognised legitimate interest pursuant to Article 6(1)(ea) UK GDPR.

49. The emphasis of the law changes from restricting the use of ADM to ensuring that safeguards are in place for significant decisions. These safeguards include (i) providing information to the data subject about the decision-making process, (ii) enabling them to make representations about the decision[37], (iii) contesting such decision as well as (iv) enabling the data subject to request human intervention by the controller. The EDPB notes that although this new approach represents a departure from the previous legal framework, Article 22C UK GDPR requires controllers to implement appropriate safeguards that ensure an adequate level of protection for data subjects.

50. In light of the fast-evolving regulatory environment and advancements in automated technologies, such as AI, the EDPB encourages the Commission to expand their assessment in their final Adequacy Decision of the envisaged practical impacts of this new approach, which has yet to be tested in practice, as well as monitor its implementation.

2.4.1. AUTOMATED DECISION MAKING AND HUMAN INVOLVEMENT

51. The EDPB welcomes the clarification regarding the meaning of automated decision making and human involvement. Article 22A UK GDPR clarifies that a decision that is based solely on automated processing means that there is no meaningful human involvement in the decision-making process. Also controllers are required to assess the extent to which profiling contributes to a decision to determine if human involvement was meaningful.

52. Further to this, Article 22D UK GDPR gives the Secretary of State the power to specify through regulations whether there is or is not meaningful human involvement in the taking of the decision described in the regulation. Similarly the Secretary of State is also given the power to describe whether the decision described in the regulation is or is not considered to have a similarly significant effect on data subjects.

53. The scope and discretion of these powers are unclear. Therefore, the EDPB invites the Commission to analyse these newly conferred powers to the Secretary of State and monitor any developments in this respect. On the other hand, the additional powers of the Secretary of State in regards to the safeguards required by Article 22C UK GDPR are a welcome change since they will add upon and/or supplement the already required safeguards as well as determine what is insufficient in terms of safeguards.

[37] I.e. give additional information and reasoning, which is not a formal legal challenge yet.

3. PROCEDURAL AND ENFORCEMENT MECHANISM

3.1. OVERSIGHT AND ENFORCEMENT

3.1.1. INDEPENDENT OVERSIGHT

54. The EDPB notes that, with the entry into force of the DUA Act[38], the Information Commissioner (ICO), previously structured as a corporation sole, will be transformed into a new structure through the introduction of a body corporate (a board), namely the Information Commission (IC) pursuant to Article 148 and Schedule 12A DPA 2018.

55. The EDPB observes that the restructuring of an authority from a corporation sole to a board does not in itself affect the independence of the authority and its effective enforcement. Attention should be given to other elements such as the rules concerning appointment and dismissal, and further to this point the EDPB welcomes that only His Majesty can remove the chair of the IC from its office following the recommendation of both houses of the UK Parliament in the event of serious misconduct.

56. Detailed rules on the work and functioning of the new IC are contained in Schedule 12A of the DPA 2018. This regulates, among other things, the structural and organisational framework of the IC, the requirements for the appointment of its executive and non-executive members as well as other staff (employees and an external committee) and includes provisions on the term of office, remuneration, account management and dismissal. Numbers 5 and 6 of Schedule 12A[39] contain rules and safeguards that must be observed when appointing non-executive members and that could be relevant to the set up of the body and its independence (e.g. selection on merit and conflict of interests).

57. The EDPB notes that the Draft Decision does not provide any details on the changes to the working and functioning of the new data protection authority. Furthermore, there are no details on the procedure for the appointment and dismissal of executive and non-executive members. As these elements are relevant for the assessment of the oversight mechanism, the EDPB invites the Commission to further describe the changes and the relevant assessment, notably as regards the structure and organisation of the IC, the appointment and dismissal of its members, including its non-executive one.

58. With regard to the independence of the IC, the EDPB notes that under Section 6 of Schedule 12A DPA 2018, conflicts of interest may prevent the appointment by the Secretary of State as Chair or as a non-executive member of the IC. In specifying the term "conflict of interest", Section 6 (5) refers to "a financial or other interest which is likely to affect prejudicially the discharge by the person of the person's function as a member of the Commission". Concerning the independence of the IC members, such “other interest”, e.g. special economic proximity and/or business relationships may also indicate conflicts of interests and should be taken into account in the appointment process for IC members. The EDPB therefore invite the Commission to monitor that the restrictions apply in practice.

59. In relation to the updated objectives that the IC needs to take into account in the performance of their tasks and preparation of their strategy such as, among others, the promotion of innovation and competition (Section 120B of the DPA 2018), the Commission recalls that “Similarly, EU data protection law also balances the protection of personal data with several other fundamental rights and objectives”, and quotes Recital 2 and 4, as well as article 23 GDPR. The EDPB acknowledges that data

[38] See Part 6 “The Information Commission”, DUAA No. 117, p. 133 ff.
[39] See Schedule 12A of the DPA 2018.

protection is not an absolute right and has to be balanced against other fundamental rights and objectives, in accordance with the principle of proportionality. However, the EDPB observes that Recital 2 and 4 GDPR, as well as Article 23 GDPR differs from a legal provision expressly requiring data protection authorities to take into account a range of objectives in the exercise of their functions. For the sake of clarity, the EDPB invites the Commission to reformulate this recital to avoid giving the impression that Recital 2 and 4, as well as article 23 GDPR have the same meaning as Section 120B of the DPA 2018 and to monitor that the implementation of these updated objectives in practice does not lead to an excessive imbalance to the detriment of the right to personal data that would undermine the level of protection of personal data.

3.1.2. ENFORCEMENT, INCLUDING SANCTIONS

60. The EDPB welcomes the fact that the provision contained in the previous bill to reform the UK data protection framework (the Data Protection and Digital Information Bill "DPDI Bill"[40]) and stipulating that the ICO must consider the Secretary of State's opinion in the exercise of their power, is no longer included in the new data protection framework.

61. The EDPB also considers it positive that, since the adoption of the previous UK Adequacy Decision, the ICO has published numerous helpful codes of practices, guidelines, opinions and other guidance documents for the relevant parties.

62. As in its Opinion 14/2021[41], the EDPB highlights that an effective supervision mechanism that allows for independent investigation of complaints, as well as effective administrative and judicial redress procedures are key elements in assessing whether a data protection system provides an adequate level of protection. Furthermore, the existence of effective sanctions plays an important role in ensuring respect for rules.

63. Against this background, the EDPB draws the Commission's attention to the public consultation published by the ICO dated 22 August regarding its proposals for handling complaints[42], which was launched only after issuing of the Commission's draft decision. In its introduction[43] to the proposals in the public consultation, the ICO states that it expects that, once the DUAA t comes into force, more complaints will be resolved by the organisations themselves without the involvement of the ICO. The background to this assessment by the ICO is that the DUAA sets out new requirements for organisations to introduce a complaints procedure specifically for data protection issues. Article 164A DPA 2018[44] stipulates that controllers must take measures to help individuals who wish to lodge complaints about the use of their personal data. For example, they must provide a complaint form which can be completed electronically and by other means, they have to acknowledge complaints within 30 days and "without undue delay' take appropriate steps to respond to the complaint and inform the complainant of the outcome of the complaint. If complaints do need to be dealt with by the ICO, the proposals put forward for public consultation should form the basis for the ICO's complaint handling. In this respect, the ICO proposes a kind of triage system, according to which complaints are to be processed with different priorities and outcomes. This should enable the ICO as a strategic

[40] See Section 32 new article 120 E, F, G, H of Data Protection and Digital Information Bill.
[41] See EDPB Opinion 14/2021, Paragraphs from 112 to 114.
[42] See ICO consultation on draft changes to how we handle data protection complaints: 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
[43] See footnote 41.
[44] See Article 164A DPA 2018.

regulator to focus its resources on the most important risks and identify systemic problems at an earlier stage. The ICO's proposal sets out criteria in a non-exhaustive list that may increase or decrease the likelihood of a complaint being pursued further[45].

64. The changes described in the paragraph 57 may lead to a change in the IC's approach to complaints handling. Due to the launch of the public consultation after issuing the Commission's draft decision, these changes have not yet been reflected in the Draft Decision.

65. The EDPB calls on the Commission to include such element in their assessment and to follow up in particular on the results of the ICO's public consultation. Furthermore, the EDPB invites the Commission to closely monitor the future complaint handling by the IC to ensure that an equivalent level of protection remains guaranteed.

66. The EDPB further notes that the extensive regulatory powers granted to the Secretary of State by the DUA Act, including the power to adopt legal provisions may have implications for the functioning of the work of the IC and its members. The EDPB refers, for instance, to the necessity for the IC to consult the Secretary of State with respect to some of its tasks. In particular, Article 124A DPA 2018[46] requires the IC to establish appropriate codes of practices containing guidelines for the proper processing of personal data where required by a regulation adopted by the Secretary of State. The IC is required to consult the Secretary of State before amending or developing such codes.

67. Given the importance of the IC's independence, the EDPB calls on the Commission to closely monitor these new powers of the Secretary of State, notably their practical effect on the IC's work.

68. 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, the existence of effective sanctions plays an important role in ensuring respect for rules. The EDPB invites the Commission to make a more detailed assessment and monitor the application of corrective powers, effectiveness of sanctions and of remedies for affected parties in the UK data protection framework[47].

4. ACCESS TO AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE UNITED KINGDOM

69. The Draft Decision focuses on developments relevant to the assessment of the level of protection in the United Kingdom since the adoption of the previous UK Adequacy Decision, which remains valid for those aspects of the UK data protection framework that have not been amended of affected. This general approach also covers the Commission's analysis of the access to and use of personal data by public authorities in the UK. This specific aspect is often referred to as "government access" and is one of the elements listed in Article 45(2)(a) GDPR to be taken into account by the Commission in determining whether the level of protection is essentially equivalent.

70. Against this background, the following sections address a number of specific points raised in the Draft Decision currently under consideration which are relevant with regard to personal data transferred

[45] See footnote 41.
[46] Code of practices for the processing of personal data.
47 See EDPB Opinion 14/2021, Paragraph 113.

from the EEA under the UK GDPR Adequacy Decision and accessed and processed by public authorities in the UK, including onward transfers. The EDPB's analysis and comments provided in Opinion 14/2021[48] generally remain valid.

4.1. ACCESS AND USE BY UK PUBLIC AUTHORITIES FOR CRIMINAL LAW ENFORCEMENT PURPOSES

71. The data protection framework governing the access and use by UK public authorities for criminal law enforcement purposes has been subject to legislative changes since the Commission's previous assessment set out in the previous UK Adequacy Decision. These include the National Security Act 2023, the Investigatory Powers Amendment Act 2024, and the introduction of the DUAA. The latter is also addressed in the Commission's Draft decision amending Implementing Decision (EU) 2021/1773, as well as in the EDPB's corresponding opinion issued on the basis of Article 51(1)(g) of the Law Enforcement Directive.

4.1.1. LEGAL BASES AND APPLICABLE SAFEGUARDS

4.1.1.1. INVESTIGATORY POWERS FOR LAW ENFORCEMENT PURPOSES

72. In recitals 81 to 85 of the Draft Decision, the Commission outlines the amendments to the Investigatory Powers Act 2016 ("IPA 2016") as introduced by the Investigatory Powers Amendment Act 2024, insofar as they pertain to law enforcement processing.[49] Overall, the Commission provides detailed information. With regard to one specific amendment, however, the EDPB considers that the draft decision would benefit from further clarification.

73. The Investigatory Powers Amendment Act 2024 revised the definition of "telecommunications operator", i.e., the potential addressees of a retention notice under the IPA 2016.[50] The modified definition now includes any person who "controls or provides a telecommunication system which (i) is not (wholly or partly) in, or controlled from, the United Kingdom, and (ii) is used by another person to offer or provide a telecommunications service to persons in the United Kingdom". While the Commission refers to the explanatory notes of the Investigatory Powers Amendment Act 2024 stating that section 261(10)(c) "provides additional clarification ensuring that large companies with complex corporate structures are covered in their totality by the IPA 2016", as well as that "the amendment […] is not seeking to bring additional companies within scope", the implications of this change remain unclear, e.g. whether it would expand the volume of personal data potentially subject to a retention notice. The EDPB therefore invites the Commission to address the effects of this modification in more detail and to specifically monitor this aspect, particularly in light of the principles of necessity and proportionality.

[48] See EDPB Opinion 14/2021.
[49] The Commission point out that, as described in recitals (139) to (141) of Implementing Decision (EU) 2021/1772, specific law enforcement authorities can also use targeted investigatory powers under the IPA 2016 for the purposes of preventing or detecting serious crimes. Amendments to such provisions therefore concern not only access to data for national security purposes, but also for law enforcement purposes.
[50] Section 261(10)(c) of the IPA 2016, as inserted by section 19 of the Investigatory Powers Amendment Act 2024.

4.1.1.2. NATIONAL SECURITY EXEMPTIONS FOR LAW ENFORCEMENT AUTHORITIES

74. 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.[51] While law enforcement authorities are already able to restrict certain obligations on the grounds of protecting national security – such as those concerning data subject rights – section 78A of the Data Protection Act 2018 will[52] also include the majority of data protection principles[53] and certain international data transfer requirements[54] 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[55] may be disapplied in such circumstances.

75. These amendments are not mentioned in either the draft adequacy decision under Article 45 GDPR or the draft adequacy decision under Article 36 of the Law Enforcement Directive. 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.[56] The EDPB is concerned about the exemptions to key data protection principles, international transfer requirements and the Information Commissioner's powers.

76. Under the revised rule, five of the six data protection principles may be disapplied where necessary to safeguard national security.[57] 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 Data Protection Act 2018. This condition requires that transfers be based either on adequacy regulations, appropriate safeguards, or – if neither of these apply – on special circumstances. The

[51] 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.
[52] The DUAA will be phased in over several stages. The main changes to data protection legislation in Part 5 of the Data (Use and Access) Act 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.
[53] See section 78A (1),(2)(a),(3) Data Protection Act 2018, as introduced by section 88 DUAA.
[54] See section 78A (1),(2)(d),(4) Data Protection Act 2018, as introduced by section 88 DUAA.
[55] See section 78A (1),(2)(e),(f),(g) Data Protection Act 2018, as introduced by section 88 DUAA.
[56] See Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, p. 10.
[57] 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).

exemptions also affect the powers of the Information Commissioner, e.g., the authority to issue information and enforcement notices.[58]

77. The EDPB notes that while the exemptions clearly deviate from the Law Enforcement Directive, 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+")[59], 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.[60] In this regard, the EDPB recalls that the Consultative Committee of the Convention for the 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 the Modernised Convention 108[61].

78. 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[62] 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.[63]

79. 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.

[58] 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.

[59] See Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).

[60] https://www.coe.int/en-GB/web/conventions/full-list?module=signatures-by-treaty&treatynum=223

[61] https://rm.coe.int/t-pd-2021-7rev13-interpretation-of-general-principles-article-11-c108-/1680b6c146

[62] See 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.

[63] 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.

4.1.2. JOINT CONTROLLERSHIPS BETWEEN UK INTELLIGENCE AGENCIES AND LAW ENFORCEMENT AUTHORITIES

80. 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.[64] 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 Data Protection Act 2018 is extended to data processing by law enforcement authorities.

81. 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 by the qualifying competent authority as a joint controller with at least one intelligence service for the purpose of safeguarding national security.[65]

82. 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 Data Protection Act 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 ECtHR[66], 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.[67] 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.

4.1.3. THE RIGHT OF ACCESS

83. The DUAA specifies that data subjects are only entitled to access 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.[68]

84. 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 Law Enforcement Directive 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

[64] See recital 72 of the draft decision.
[65] See recital 73 of the draft decision.
[66] See ECtHR, Big Brother Watch and others v. The United Kingdom, 25 May 2021, paragraph 350.
[67] 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.
[68] See Section 78(3) and (4) of the Data (Use and Access) Act, amending sections 45 and 94 of the Data Protection Act 2018.

disproportionate without compromising essential equivalence.[69] The EDPB recalls the analysis and conclusion from paragraph 34 of this Opinion which are equally relevant to the the law enforcement and national security regime.

4.1.4. ONWARD TRANSFERS

4.1.4.1. A NEW DATA PROTECTION TEST

85. 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.

86. 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 Data Protection Act 2028 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 United Kingdom data protection legislation.

87. In this context, the EDPB notes that the elements to be considered by the Secretary of State in the assessment as per section 74 AB(2) of the DPA 2018 appear to have been reduced compared to the previous assessment for adequacy regulations.[70] 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 and recalls the analysis and conclusions made in paragraphs 42-43 of this Opinion. Notably, the EDPB (i) encourages the Commission to specifically address the changes and further elaborate its assessment of the new data protection test. 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 in the area of law enforcement and criminal justice cooperation. 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 effective redress or data subject rights not already established in the legal framework of that third country.

[69] For instance, it might be argued that this is the case for searching seized devices that have not yet been analysed or decrypted.
[70] The provision of section 74A(4) of the DPA 2018, which was omitted by the DUAA, provided for a list of criteria that was identical to Article 36(3) LED.

88. Furthermore, the EDPB recalls the conclusions outlined in paragraph 41 in relation to the use of the criterion of the "desirability of facilitating transfers of personal data to and from the United Kingdom" (Section 74 AA(3) of the Data Protection Act 2018) and invites the Commission to clarify in its decision that this criterion 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 Data Protection Act 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.

4.1.4.2. THE UK-U.S. CLOUD ACT AGREEMENT

89. Another relevant development in the area of onward transfers is the entry into force in October 2022 of the "Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime" ("UK-U.S. Cloud Act Agreement"). As the Commission correctly points out, personal data transferred from the EU to service providers in the United Kingdom could be subject to orders for the production of evidence issued by competent U.S. law enforcement authorities under this agreement.[71]

90. Given that, at the time of adopting the previous UK Adequacy Decision, the agreement had been concluded but not yet entered in force, the Commission emphasised that any information and future clarification regarding the way the U.S. will comply with its obligations under the agreement should be communicated by the UK to the Commission in order to ensure proper monitoring of the previous UK Adequacy Decision in line with Article 45(4) of the GDPR. The Commission noted that particular attention should be given to the application and adaptation of the safeguards established in the EU-U.S. Umbrella Agreement[72] to the specific type of transfers covered by the UK-U.S. Cloud Act Agreement.[73] Following up on this statement, the Commission refers in its Draft Decision to several clarifications reached between the UK and U.S. in the context of the applying the EU-U.S. Umbrella Agreement to the UK-U.S. Cloud Act Agreement. The EDPB welcomes these clarifications, which provide further legal clarity. At the same time, it is worth noting that the EU-U.S. Umbrella Agreement has not yet been reviewed, which limits to some extent the conclusions that can be drawn about the impact and effectiveness of its application to the UK-U.S. Cloud Act Agreement.[74] Furthermore, having regard to the EU-U.S. Umbrella Agreement, the EDPB would like to recall the need to improve the level of safeguards provided by this agreement. This applies in particular to the availability of judicial redress. EU data subjects other than EU citizens have no basis under the Judicial Redress Act to pursue legal remedies. In addition, the Privacy Act contains exceptions, which have not been amended by the Judicial Redress Act, that reduce the ability of individuals to seek redress in certain law enforcement

[71] See Recital 87 of the Draft Decision.
[72] See Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, OJ L 336, 10.12.2016, p. 3–13, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01).
[73] See Recital 155 of the Implementing Decision 2021/1772. As per Article 9(1) of the UK-U.S. Cloud Act Agreement, the EU-U.S. Umbrella Agreement applies *mutatis mutandis* to the UK-U.S. Cloud Act Agreement. It can only be applied on a *mutatis mutandis* basis, as the Umbrella Agreement governs cross border transfers between law enforcement authorities and not direct cooperation between a service provider and a law enforcement authority.
[74] See Article 23 of the EU-U.S. Umbrella Agreement provides that the parties shall conduct periodic joint reviews of the policies and procedures that implement the agreement, with the first review taking place no later than three years from the date of entry into force of the agreement. The EU-U.S. Umbrella Agreement entered into force in February 2017.

and national security situations. While the Commission notes that the Judicial Redress Act is not the only mechanism for seeking redress, the Draft Decision merely states that "depending upon the circumstances and context of the specific case, other applicable US laws provide alternative routes by which judicial redress might be sought"[75]. This leaves unclear whether all EU individuals whose data may be subject to the UK-U.S. Cloud Act Agreement will be afforded rights of judicial redress in the U.S.

91. The EDPB also notes that a specific reciprocal safeguard established in the UK-U.S. Cloud Act Agreement, whereby both parties limit the impact the agreement may have for UK and U.S. persons respectively, is, by its nature, not applicable to EU individuals.[76] The EDPB observes that, for this reason, robust data protection safeguards are essential to ensure EU data subjects' rights are adequately protected if processed under that agreement. Therefore, the EDPB invites the Commission to continue to include the UK-U.S. Cloud Act Agreement in its future assessments and reviews of the adequacy decision.

92. Overall, the EDPB sees a need for clarification as to the Commission's assessment of the UK-U.S. Cloud Act Agreement and any possible impact of the agreement on the level of protection as assessed in the previous UK Adequacy Decision. The findings of the first review of the UK-U.S. Cloud Act Agreement, which shall, under Article 12(1) of the agreement, be carried out within one year of the agreement's entry into force, could be particularly informative for such further analysis.

4.1.5. OVERSIGHT AND REDRESS

93. The EDPB notes that the system of oversight of criminal law enforcement agencies under the Data Protection Act 2018 and the IPA 2016 as well as the redress mechanisms, available under Part 3 of the DPA 2018, the IPA 2016 and the Human Rights Act 1998, remain largely unchanged. In particular, the oversight in the UK continues to be ensured, in addition to the 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.

94. 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.

95. 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[77]. 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.

96. As already emphasised by the EDPB in Opinion 14/2021, while the ICO is well equipped with the necessary powers, which closely correspond with the powers of EU Member States SAs as set forth in

[75] See Recital 93 of the Draft Decision.
[76] See Articles 4(3) and 7(1) of the agreement which provide for targeting restrictions setting forth that orders subject to the agreement may not intentionally target a "Receiving-Party Person". Therefore, the U.S. may not intentionally target a person located in the territory of the UK, and the UK has to comply with a similar restriction.
[77] See https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner.

Article 58 GDPR, the existence of effective sanctions plays an important role in ensuring respect for the rules[78].

97. The EDPB positively notes the transparency policy of the ICO and the availability of the statistical and analytical data, including examples, of the ICO's enforcement activities vis-a-vis law enforcement bodies[79]. 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[80]. The EDPB also considers it positive that the ICO has published numerous codes of practices, guidelines, opinions and other guidance documents for the relevant parties.

98. In the light of the above and in particular in view of the imminent substantial changes in the structure and organisation of the UK supervisory authority, as already analysed in paragraph 68 of this Opinion, the EDPB invites the European Commission to continue to monitor the effectiveness of sanctions and relevant remedies in the UK Data Protection Framework.

4.2. ACCESS AND USE BY UK PUBLIC AUTHORITIES FOR NATIONAL SECURITY PURPOSES

99. The Draft Decision offers only limited details on the access to and use of personal data by UK public authorities for national security purposes. The Commission explains that the DUAA made only minor amendments to the framework governing data processing by UK intelligence services[81], some of which have also been introduced to the law enforcement regime of the Data Protection Act 2018. These amendments are briefly mentioned in recital 75 of the Draft Decision. Furthermore, the changes made to the IPA 2016 since the adoption of the previous UK Adequacy Decision are already addressed under section 3.2 of the Draft Decision, where they concern both data processing for law enforcement and for national security purposes.[82] Accordingly, the requests for clarification and monitoring outlined in sections 3.1.1.1 and 3.1.3 above apply equally to the access and use of personal data for national security purposes.

4.2.1. THE USE OF TECHNICAL CAPABILITY NOTICES

100. Earlier this year, media reports revealed that the UK Government had allegedly issued a Technical Capability Notice ("TCN") under section 253 of the IPA 2016 to a major technology company, requiring the provider to be able to maintain access to its users' encrypted data in decrypted form.[83] In practice, purportedly, this would mean to circumvent the end-to-end encryption that the provider offers for its cloud storage solution. This measure has thus been referred to as a "backdoor demand".

101. Although the legal basis for TCNs already existed at the time of the adoption of the previous UK Adequacy Decision, this reported case appears to mark the first known instance of an application of this kind. As such, it constitutes a significant development that merits attention, particularly in light of

[78] See EDPB Opinion 14/2021, paragraph 112.
[79] 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/.
[80] See https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/.
[81] See Recital 75 of the Draft Decision.
[82] See Recital 98 of the Draft Decision. The investigatory powers in question may be exercised not only by national intelligence agencies but also by certain law enforcement authorities.
[83] See "U.K. orders Apple to let it spy on users' encrypted accounts" (Washington Post, 7 February 2025), https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/ .

Article 45(2)(a) GDPR, which requires an assessment not only of the legal framework on paper but also of its implementation.[84] The EDPB would therefore have expected the Draft Decision to address this matter explicitly and encourages the Commission to complement the decision accordingly.

102. Despite the fact that the details of this case are not fully known to the public due to the confidential nature of TCNs, it is apparent from the public listing of the application for a hearing in private on the website of the Investigatory Powers Tribunal, as well as by the publicly available extract of the private judgment concerning such hearing that this is not a matter of media speculation.[85] The issue warrants mentioning and the purported application of section 253 of the IPA 2016 to issue a "backdoor demand" should be flagged for future monitoring.

103. As recently pointed out in Statement 05/2024, the EDPB considers encryption to be essential for ensuring the security and confidentiality of personal data and electronic communications. In particular, genuine end-to-end encryption covering the terminal devices and the data therein, with the decryption keys held solely by the user is a crucial tool for ensuring the confidentiality of electronic communications.[86] TCNs compelling companies to provide the ability to remove encryption at the government's request creates systemic vulnerabilities and poses a direct threat to the integrity and confidentiality of electronic communications. In this respect, the EDPB draws attention to the case of PODCHASOV v. RUSSIA, where the ECtHR found that an "obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued".[87]

104. While it is assumed that the UK government would primarily seek to access unencrypted user data if there were a risk to national security, the EDPB considers that the request for an assessment of the use of TCNs, as discussed above, is equally pertinent in the context of government access for law enforcement purposes.

4.2.2. LEGAL BASES AND APPLICABLE SAFEGUARDS

105. The Investigatory Powers Amendment Act 2024 introduced a specific regime for the retention and examination of bulk personal datasets for which the individuals to whom the personal data relates "could have no, or only a low, reasonable expectation of privacy", as the law puts it.[88] For the retention and examination of such specific subset of bulk personal datasets, the IPA 2016 now provides for the possibility of "individual authorisations" and "category authorisations". [89]

106. The notion of bulk personal datasets is broad and can capture a wide range of datasets.[90] It may apply to sensitive information but can also encompass publicly and commercially available data. Against this

[84] In addition, Article 45(3) GDPR specifies that the Commission shall take into account all relevant developments in the third country when periodically reviewing their adequacy findings.
[85] See https://www.judiciary.uk/judgments/apple-inc-v-secretary-of-state-for-the-home-department/ .
[86] See Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, Adopted on 4 November 2024, p. 4, 5.
[87] See ECtHR judgment of 13 February 2024, 33696/19, paragraph 79.
[88] See Section 226A(1) of the IPA 2016.
[89] See Section 226A and 226BA of the IPA 2016, as introduced by section 2 of the Investigatory Powers Amendment Act 2024.
[90] See Section 199 of the IPA 2016 specifies that an "intelligence service retains a bulk personal dataset if (a) the intelligence service obtains a set of information that includes personal data relating to a number of individuals, (b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions, (c) after any initial examination of the contents, the intelligence service retains the set for the

background, the UK government considered it necessary to revise the previous regime that applied the same level of safeguards to all bulk personal datasets and to foresee, instead, different safeguards to the retention and examination of bulk personal datasets, depending on the sensitivity or public availability of their contents, or the level of intrusion associated with the intelligence services retaining and examining them.[91] It is the EDPB's understanding that these considerations ultimately led to the creation of a distinct regime for bulk personal datasets where there is only a low or no reasonable expectation of privacy.

107. While the Commission briefly discusses the new concept of a "category authorisation", the Draft Decision states that "importantly, for the retention and examination of bulk personal datasets, the regime assessed in recitals (239) and (240) of Implementing Decision (EU) 2021/1772 remains in place, in particular the need for a warrant that is approved first by the Secretary of State and then by the Judicial Commissioner, subject to the requirements of necessity and proportionality of the measure, as provided by Part 7 of the IPA 2016"[92]. However, this analysis appears to be incomplete. The EDPB notes that not only the introduction of "category authorisations" but also of "individual authorisations" constitutes a relevant change implemented by the Investigatory Powers Amendment Act 2024 concerning the above mentioned specific dataset: an "individual authorisation", which can be granted by the head of an intelligence service, or a person acting on their behalf, replaces the necessity to obtain a warrant in order to retain, or to retain and examine bulk personal datasets for which there is only a low or no reasonable expectation of privacy.[93] The terms "warrant" and "individual authorisation" should thus not be confused and cannot be used interchangeably.[94] This is particularly so because the judicial approval required for individual authorisations is limited to the question of whether the specific dataset fulfils the criteria to be classified as warranting only a low or no reasonable expectation of privacy under section 226A of the IPA 2016.[95] A "category authorisation" is different from an "individual authorisation" and effectively disapplies – per section 226B(6)(a) of the IPA 2016 – the requirement for such judicial approval of an individual authorisation where such authorisation pertains to a dataset that falls within a category authorisation. That is because a decision will already have been made, and approved by a Judicial Commissioner, that any dataset that falls within the description in the category authorisation is indeed a dataset to which section 226A would apply.

108. While these amendments concern the retention and examination of bulk personal datasets and not their initial interception or collection, the EDPB would like to emphasise the importance the ECtHR attaches to prior independent authorisation in the context of processing personal data in bulk. The Court ruled that "in order to minimise the risk of the bulk interception power being abused, […] the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an

purpose of the exercise of its functions, and (d) the set is held, or is to be held, electronically for analysis in the exercise of those functions".

[91] See Home Office, Policy paper Investigatory Powers (Amendment) Bill: Bulk Personal Datasets and Third Party Bulk Personal Datasets, https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-bulk-personal-datasets-and-third-party-bulk-personal-datasets.

[92] See Recital 99 of the Draft Decision.

[93] Section 200(1) and (2) of the IPA 2016.

[94] This appears to be the case, however, in recitals 99 and 100 of the draft decision.

[95] Section 226BB(1) of the IPA 2016 stipulates that in deciding whether to approve a decision to grant an individual authorisation or a category authorisation, a Judicial Commissioner must review the conclusions of the person who granted the authorisation to verify whether section 226A applies to the bulk personal dataset described in the authorisation or, respectively, whether section 226A applies to any dataset that falls within the category of datasets described in the authorisation.

assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review."[96] With this in mind and based on a holistic approach, taking into account all the circumstances of the case in assessing adequacy, the EDPB considers that the retention and examination of bulk personal datasets should at least be subject to either a prior authorisation by an independent authority or to a systematic independent review ex post by a court or an equivalently body, i. e., an independent body that can render binding decisions.

109. In view of the remaining clarifications needed the EDPB urges the Commission to further examine the concepts of "individual authorisations" and "category authorisations" under the Investigatory Powers Amendment Act 2024. Furthermore, the EDPB invites the Commission to closely monitor the implementation of the term "low or no reasonable expectation of privacy" in practice. Although section 226A of the IPA 2016 establishes a number of criteria for such finding, the EDPB considers it important to observe their application, as they are potentially open to broad interpretation.[97]

4.2.3. OVERSIGHT AND REDRESS

110. As indicated in the Draft Decision and previously analysed in Opinion 14/2021, the Investigatory Powers Commissioner (IPC) and his Office (IPCO) play central role in the oversight of the use of investigatory powers by the UK intelligence agencies. Furthermore, the Investigatory Powers Tribunal (IPT) is the judicial body competent to provide redress in this regard. As already indicated in section 3.1.5. on the oversight in the law enforcement area, the Investigatory Powers Amendment Act 2024 has made only limited modifications, in particular through the introduction of deputy IPCs. Hence, the EDPB comments in its Opinion 14/2021 remain fully valid[98].

111. The EDPB positively notes the transparent annual reporting by the IPCO, including the availability of detailed statistics for the period 2019 - 2023, including about the use of bulk powers by the UK intelligence community and on the targeting decisions and the targeted authorisations for the purpose of acquiring data pursuant to the UK-US Data Access Agreement. The EDPB also takes specifically note of the oversight activities by the IPCO over bulk interception of data by the Government Communications Headquarters (GCHQ), highlighted by the Commission in recital 102 of the Draft Decision. In this context, the EDPB invites the Commission to continue to monitor closely the effectiveness of the oversight system in this area, in particular as regards the proportionality of the bulk interception requests[99].

112. In addition, the EDPB notes that the Investigatory Powers Tribunal has also issued a public report of its activities and case law for the period 2021-2023[100]. The report highlights, among others, important and relevant developments such as the judgment of the European Court of Human Rights in case *Wieder and Guarnieri v UK,* which has ruled that individuals anywhere in the world can make a claim in the IPT, if the conduct was by a UK public body and occurred in the UK. The EDPB therefore invites

[96] ECtHR, Big Brother Watch and others v. The United Kingdom, 25 May 2021, § 350.
[97] Section 226A oft he IPA 2016 refers to, e. g., the nature of the data, the extent to which data has been made public, or the extent to which the data is widely known about.
[98] See Opinion 14/2021, paragraphs from 200 to 215.
[99] For more information see 2023 Annual Report of the Investigatory Powers Commissioner, available at the following link: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf , page 31, paragraph 6.41.
[100] https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf

the Commission to include also the activities of the IPT in its assessment and in the future reviews of the Draft Decision.

5. REVIEW, DURATION AND RENEWAL OF DRAFT DECISION

113. The EDPB notes that the final Adequacy Decision would apply for six years, i.e. until 27 December 2031. It would thus continue being the only third country whose adequacy decision has a sunset clause which is combined with the mandatory periodical review set out in article 45(3) GDPR. The EDPB understands that the new UK legal framework will deserve specific attention and calls on the Commission to carefully monitor the implementation of the DUAA, including the areas of focus highlighted in this Opinion, as well as all other relevant developments in the UK in this regard.

114. The EDPB welcomes that recital 68 of the Draft Decision refers to the role of the EDPB (and civil society groups) in the periodic review mechanism, in accordance with EDPB recommendation 01/2021[101]. 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.

115. From additional explanations provided by the Commission in relation to Recital 113, the EDPB understands that the intention is to conduct a review at the end of the four years on the basis of which the Commission will prepare a public report[102]. This review will help inform the Commission as to whether, at the latest six months before the end of the Draft Decision, they initiate the procedure to extend the duration of the Draft Decision[103].

116. The EDPB welcomes this intention and notes that as the review serves a different purpose than the sunset clause and plays an important role in monitoring the legal framework. The EDPB, therefore, expects the review to take place in four years, and encourages the Commission to proceed with it in due course.

117. It is the understanding of the EDPB that this future review will take into account the elements outlined in the Commission Implementing Decision 2021/1772 and that the recitals concerning the suspension and repeal of the decision are still valid[104]. For the sake of legal certainty, the EDPB believes that such a clarification could appear in the final Adequacy Decision.

For the European Data Protection Board

The Chair

(Anu Talus)

[101] See recital 19 of EDPB recommendation 01/2021.
[102] See recital 110 of the Draft Decision.
[103] See recital 113 of the Draft Decision.
[104] See recitals 168 to 171 of Commission Implementing Decision 2021/1173.