2025/2571

23.12.2025

COMMISSION IMPLEMENTING DECISION (EU) 2025/2571

of 19 December 2025

amending Commission Implementing Decision (EU) 2021/1773 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom

(notified under document C(2025) 8782)

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) ([1]), and in particular Article 36(3) thereof,

Whereas:

1. INTRODUCTION

(1) Commission Implementing Decision (EU) 2021/1773 ([2]) concludes that for the purposes of Article 36 of Directive (EU) 2016/680, the United Kingdom ensures an adequate level of protection for personal data transferred from the European Union to the United Kingdom within the scope of that Directive.

(2) When adopting Implementing Decision (EU) 2021/1773, the Commission took into account that, with the end of the transition period provided by the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community ([3]) and once the interim provision under Article 782 of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part ([4]) would have ceased to apply, the United Kingdom may adopt, apply and enforce a new data protection regime, different to the one in place when it was bound by Union law.

(3) As this may have involved amendments to the data protection framework assessed in Implementing Decision (EU) 2021/1773 or other relevant developments, it was considered appropriate to provide that that Decision would apply for a period of four years as of its entry into force. Implementing Decision (EU) 2021/1773 was therefore set to expire on 27 June 2025, unless extended in accordance with the procedure referred to in Article 58(2) of Directive (EU) 2016/680.

(4) To decide on a possible extension of Implementing Decision (EU) 2021/1773, the Commission must assess 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 Implementing Decision (EU) 2021/1773 with respect to the elements listed in Article 36(2) of Directive (EU) 2016/680.

(5) In particular, on 23 October 2024, the UK Government introduced the Data (Use and Access) Bill ([5]) into the UK Parliament, proposing amendments to the Data Protection Act 2018 (DPA 2018) which is assessed in Implementing Decision (EU) 2021/1773. The Commission on 24 June 2025 adopted Commission Implementing Decision

([1]) OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.
([2]) Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (OJ L 360, 11.10.2021, p. 69, ELI: http://data.europa.eu/eli/dec_impl/2021/1773/oj).
([3]) OJ C 384 I, 12.11.2019, p. 1.
([4]) OJ L 149, 30.4.2021, p. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.
([5]) Available at the following link: https://bills.parliament.uk/bills/3825/news.

(EU) 2025/1225 ([6]), which extended the validity of Decision (EU) 2021/1773 for a period of six months until 27 December 2025. This time-limited technical extension allowed the Commission to finalise its assessment of the adequate level of protection for personal data provided by the United Kingdom on the basis of a stable legal framework, i.e. after the conclusion of the relevant legislative process.

(6) Since the adoption of Implementing Decision (EU) 2021/1773, the Commission monitored, on an ongoing basis, relevant developments in the United Kingdom ([7]). In accordance with recital 165 of Implementing Decision (EU) 2021/1773 special attention was paid to the application in practice of the United Kingdom rules on transfers of personal data to third countries, and the impact it may have on the level of protection afforded to data transferred under Implementing Decision (EU) 2021/1773, and to the effectiveness of the exercise of individual rights, including any relevant development in law and practice concerning the exceptions to or restrictions of such rights. Amongst other elements, case law developments and oversight by the Information Commissioner's Office (ICO) and other independent bodies informed the Commission's monitoring.

(7) Based on the assessment of these developments, including the amendments to the DPA 2018 introduced by the Data (Use and Access) Act, the Commission concludes that the United Kingdom continues to ensure an adequate level of protection for personal data transferred within the scope of Directive (EU) 2016/680 from the European Union to the United Kingdom.

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

2.1. The data protection framework of the United Kingdom

(8) When Implementing Decision (EU) 2021/1773 was adopted, the legal framework for the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security in the United Kingdom was set out in the relevant parts of the DPA 2018 ([8]), as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations) ([9]), and in particular in Part 3 of that Act.

(9) While this Act that closely mirrored the corresponding rules applicable within the European Union continues to form the data protection legislation of the United Kingdom for the relevant processing activities, it has since then been subject to limited amendments, reflecting that the United Kingdom is no longer subject to the law of the European Union.

(10) First, the Retained EU Law (Revocation and Reform) Act 2023 (REUL Act) ([10]), clarified that the general principles of EU law were no longer of the United Kingdom's domestic law after the end of 2023 ([11]). In addition, United Kingdom courts are no longer required to interpret unmodified 'assimilated law', which was previously referred to as

([6]) Commission Implementing Decision (EU) 2025/1225 of 24 June 2025 amending Implementing Decision (EU) 2021/1773 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (OJ L, 2025/1225, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1225/oj).

([7]) Article 36(4) of Directive (EU) 2016/680.

([8]) Data Protection Act 2018, available at the following link:https://www.legislation.gov.uk/ukpga/2018/12/contents. Prior to the United Kingdom's withdrawal from the European Union and during the transition period, the DPA 2018 provided national rules, where allowed by Regulation (EU) 2016/679, specifying and restricting the application of the rules of Regulation (EU) 2016/679, and transposed Directive (EU) 2016/680.

([9]) The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, available at the following link:https://www.legislation.gov.uk/uksi/2019/419/contents/made, as amended by the DPPEC Regulations 2020, available at the following link: https://www.legislation.gov.uk/ukdsi/2020/9780348213522. The DPPEC Regulations amend Regulation (EU) 2016/679 as brought into United Kingdom law through the European Union (Withdrawal) Act 2018, the DPA 2018, and other data protection legislation to fit the domestic context.

([10]) Retained EU Law (Revocation and Reform) Act 2023, available at the following link: https://www.legislation.gov.uk/ukpga/2023/28.

([11]) Section 5 of the European Union (Withdrawal) Act 2018, as amended by the REUL Act.

'retained EU law', in accordance with the general principles of EU law, but such law must instead be read compatibly with domestic UK law ([12]). However, unmodified assimilated law must still be interpreted by relevant courts of the United Kingdom in accordance with the relevant case law of the European Court of Justice issued before the end of the transition period ([13]), as also mentioned in recital 12 of Implementing Decision (EU) 2021/1773. The DPA 2018 has been amended by the Data (Use and Access) Act to clarify the effect of the REUL Act on the United Kingdom's data protection legislation. For example, Section 183A(1) of the DPA 2018 provides as a general rule that any new legislation (passed on or after 20 August 2025) which introduces new duties or powers to process personal data is presumed to be subject to the United Kingdom data protection legislation. This means that the United Kingdom's data protection framework continues to override other legislation. Pursuant to Section 183A(2)(b) of the DPA 2018, this presumption can be disapplied if the United Kingdom Parliament deliberately decides to do so expressly in legislation, preserving parliamentary sovereignty. In addition, Section 186(2A) of the DPA 2018 clarifies that the restrictions to data subject rights listed in Section 186(3) of the DPA 2018 are not overridden by Section 186(1) of the DPA 2018, which provides that enactments prohibiting or restricting the disclosure of information do not override certain data protection rights. This ensures that, for example, restrictions on data subject rights set out in the DPA 2018 are not themselves caught by the general 'data protection override' in Section 186(1) of the DPA 2018.

(11) Second, since the adoption of Implementing Decision (EU) 2021/1773, the data protection legislation of the United Kingdom has been amended through the Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023 ([14]). These Regulations define references to fundamental rights or fundamental freedoms in the DPA 2018 (which were previously defined to cover EU fundamental rights and fundamental freedoms ([15])), as references to rights under the European Convention on Human Rights, which have been given effect in the United Kingdom's domestic law under the Human Rights Act 1998 ([16]). The Human Rights Act 1998 incorporates the rights contained in the European Convention on Human Rights into the law of the United Kingdom. The Human Rights Act grants any individual the fundamental rights and freedoms provided in Articles 2 to 12 and 14 of the European Convention on Human Rights, Articles 1, 2 and 3 of its First Protocol and Article 1 of its Thirteenth Protocol, as read in conjunction with Articles 16, 17 and 18 of that Convention. This includes the right to respect for private and family life (and the protection of personal data as part of that right), and the right to a fair trial ([17]).

(12) Finally, the DPA 2018 has been subject to targeted reforms provided by parts five and six of the Data (Use and Access) Act. While the scope of the Data (Use and Access) Act goes well beyond the protection of personal data, it provides for limited amendments to several aspects of the data protection regime such as, inter alia, the modalities for the exercise of data subjects' rights, the conditions for automated decision-making, and the scope of certain accountability requirements. In addition, the Data (Use and Access) Act makes amendments to the governance structure of the ICO. Once implemented, these measures will replace the ICO with a new entity, the Information Commission. The role and functions of the regulator as the independent data protection supervisory authority in the United Kingdom will remain unchanged. The Act also and introduces new enforcement powers for the regulator.

(13) This Decision assesses legislative, regulatory and other developments that are relevant to the conclusion on the level of protection guaranteed by the United Kingdom made in Implementing Decision (EU) 2021/1773. The assessment made in Implementing Decision (EU) 2021/1773 remains valid for those aspects of the United Kingdom data protection framework that have not been amended or affected by other developments since the adoption of Implementing Decision (EU) 2021/1773.

([12]) Section 5(A2) of the European Union (Withdrawal) Act 2018, as amended by the REUL Act.
([13]) Section 6(3) and (7) of the European Union (Withdrawal) Act 2018, as amended by the REUL Act.
([14]) Available at the following link: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.
([15]) EU fundamental rights and fundamental freedoms had been retained in UK law by Section 4 of the European Union (Withdrawal) Act 2018, which was repealed at the end of 2023 by the REUL Act.
([16]) Regulation 2(3) of the Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023.
([17]) Articles 6, 8, 10 and 13 of the ECHR (see also Schedule 1 to the Human Rights Act 1998, available at the following link: https://www.legislation.gov.uk/ukpga/1998/42/contents).

(14) The legislative, regulatory and other relevant developments are analysed in detail in the following sections on the basis of the adequacy standard, according to which the Commission has to determine whether the third country in question guarantees a level of protection 'essentially equivalent' to that ensured within the European Union ([18]). As clarified by the Court of Justice of the European Union, this does not require finding an identical level of protection ([19]). In particular, the means to which the third country in question has recourse for protecting personal data may differ from the ones employed in the European Union, as long as they prove, in practice, effective for ensuring an adequate level of protection ([20]). The adequacy standard therefore does not require a point-to-point replication of Union rules. Rather, the test lies in whether, through the substance of data protection rights and their effective implementation, supervision and enforcement, the foreign legal system as a whole delivers the required level of protection ([21]).

2.1.1. *Definitions*

(15) Basic data protection concepts mirroring the terminology of Directive (EU) 2016/680 continue to apply in the United Kingdom's data protection regime. These concepts have been assessed in recitals 26 and 27 of Implementing Decision (EU) 2021/1773.

(16) In particular, by specifying the definition and the conditions for obtaining consent, the Data (Use and Access) Act confirms the legal framework governing the use of consent as a lawful basis for the processing of personal data ([22]). The updated provisions replicate the language of the UK GDPR, thereby increasing consistency across the United Kingdom's data protection regimes. This alignment facilitates clearer interpretation by competent authorities when relying on consent as a lawful basis for processing.

(17) First, Section 69 of the Data (Use and Access) Act introduces a new subsection 33(1A) into the DPA 2018, defining 'consent' as a freely given, specific, informed, and unambiguous indication of the data subject's wishes. This indication must be provided through a statement or by clear affirmative action and must signify the individual's agreement to the processing of their personal data.

(18) Second, the same section adds Section 40A into the DPA 2018, which sets out the conditions that must be met when relying on consent. The controller must be able to demonstrate that the data subject has given valid consent. Where the consent is obtained in writing as part of a broader document, it must be presented in a manner that distinguishes it clearly from other matters, using accessible, intelligible, and plain language. Any provision of the document that fails to comply with these standards will not be binding ([23]).

(19) Controllers or processors must also inform the individual, prior to obtaining consent, of their right to withdraw it. The process for withdrawal must be as easy as the process for giving consent. This ensures that the data subject retains genuine control over the use of their personal data throughout ([24]).

(20) Finally, the Data (Use and Access) Act clarifies that when assessing whether consent is 'freely given,' it is necessary to consider whether the provision of a service was made conditional on the data subject agreeing to the processing of personal data that is not required for the provision of that service. If so, this may undermine the validity of the consent ([25]).

([18]) Recital 67 of Directive (EU) 2016/680.
([19]) Case C-362/14, Schrems ('Schrems I'), ECLI:EU:C:2015:650, paragraph 73.
([20]) Schrems I, paragraph 74.
([21]) See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, Exchanging and Protecting Personal Data in a Globalised World, COM(2017)7 of 10.1.2017, Section 3.1, pages 6-7, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0007.
([22]) Sections 33 and 40A of the DPA 2018, as introduced by Section 69(1), (2) and (4) of the Data (Use and Access) Act.
([23]) Section 40A(2) and (3) of the DPA 2018, as introduced by Section 69(4) of the Data (Use and Access) Act.
([24]) Section 40A(5) and (6) of the DPA 2018, as introduced by Section 69(4) of the Data (Use and Access) Act.
([25]) Section 40A(7) of the DPA 2018, as introduced by Section 69(4) of the Data (Use and Access) Act.

(21) Importantly, under the revised Part 3 of the DPA 2018, consent continues not to be a legal basis that is relevant for processing operations falling within the scope of the present Decision, as explained in recital 35 of Implementing Decision (EU) 2021/1773. In addition, as noted in recital 36 of Implementing Decision (EU) 2021/1773, processing in a law enforcement context continues not to be possible solely on the basis of consent, as a competent authority must always have an underlying power that enables it to process the data. More specifically, and similarly to what is allowed under Directive (EU) 2016/680 ([26]), this means that consent serves as an additional condition to enable certain limited and specific processing operations that could otherwise not be carried out, for example the collection and processing of a DNA sample of an individual who is not a suspect.

2.2. **Safeguards, rights and obligations**

2.2.1. *Processing of sensitive personal data*

(22) The United Kingdom's data protection framework continues to provide specific safeguards where special categories of data are involved, as assessed in recitals 38 to 42 of Implementing Decision (EU) 2021/1773.

(23) Both the definition of special categories of personal data and the specific rules applying to the processing of these categories of data in Part 3 of the DPA 2018 remain in place. At the same time, the Data (Use and Access) Act confers new regulation-making powers to the Secretary of State to add new special categories of data and to tailor the conditions applicable to their use, if necessary ([27]). Importantly, this power does not allow the Secretary of State to remove or amend any existing special categories of data, or to alter the conditions for the processing of these categories ([28]).

(24) Therefore, these amendments do not affect the level of protection for special categories of personal data found essentially equivalent to the protection within the EU in Implementing Decision (EU) 2021/1773.

2.2.2. *Individual rights*

(25) Under the United Kingdom's legal framework, data subjects continue to benefit from the same individual rights as under Directive (EU) 2016/680 which can be enforced against the controller or processor, in particular the right of access to data, the right to object to the processing, and the right to have data rectified and erased, as assessed in recitals 57 to 65 of Implementing Decision (EU) 2021/1773.

(26) The Data (Use and Access) Act clarifies certain modalities under which those rights can be exercised.

(27) First, under the current regime, data controllers are entitled to refuse a request or to charge a reasonable fee if a request is manifestly unfounded or excessive ([29]). In this respect, the Data (Use and Access) Act confers a new regulation-making power upon the Secretary of State, enabling the Secretary of State to issue regulations that require data controllers to produce and publish guidance concerning the fees that they charge in such circumstances. In addition, when data controllers refuse to comply with a request on the aforementioned ground, the Data (Use and Access) Act clarified that they remain obliged to notify the data subject of the reasons for the refusal and of the data subject's right to lodge a complaint with the Information Commissioner. Such notification must be provided without undue delay ([30]).

(28) Second, the Data (Use and Access) Act specifies the time limits within which controllers need to respond to data subject's requests. More specifically, it aligns the required response periods with those set out in the UK GDPR. The revised provisions also allow for an extension of the response period up to two additional months in cases where the

([26]) See recitals 35 and 37 of Directive (EU) 2016/680.

([27]) Section 74 of the Data (Use and Access) Act. Such regulations are subject to the affirmative resolution procedure, which means that they require active approval by the UK Parliament.

([28]) See new Section 42A of DPA 2018 introduced by Section 74 of the Data (Use and Access) Act, as well as Explanatory Notes to the Data (Use and Access) Bill, paragraph 577, available at the following link: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

([29]) Section 53(1) of the DPA 2018. See also recital 64 of Implementing Decision (EU) 2021/1773.

([30]) Section 53(4A), (6) and (7) of the DPA 2018, as introduced by Section 75 of the Data (Use and Access) Act.

request is complex or when multiple requests are received. In such instances, the controller must inform the data subject of the extension and the reasons for it ([31]). The Data (Use and Access) Act also introduced a mechanism that permits controllers to suspend the deadline for responding to a request in cases where further information is needed from the data subject to identify the data requested ([32]).

(29) Third, with respect only to the right of access to information and personal data, the Data (Use and Access) Act amends Section 45 of the DPA 2018, to incorporate the clarification developed under existing domestic case-law – drawing on the principle of proportionality under EU law – that controllers only have to carry out reasonable and proportionate searches for information and personal data requested ([33]). The new provision is expected to be interpreted in line with existing case-law, which provides that '[…] what is weighed up in the proportionality exercise is the end object of the search, namely the potential benefit that the supply of the information might bring to the data subject, as against the means by which that information is obtained. It will be a question for evaluation in each particular case whether disproportionate effort will be involved in finding and supplying the information as against the benefits it might bring to the data subject' ([34]).

(30) Therefore, while the modalities for responding to data subject requests are subject to more detailed rules, the United Kingdom system continues to ensure that data subject requests have to be handled in reasonable time periods defined on the basis of objective factors. Moreover, the controller's substantive obligations when responding to requests for access are framed on the basis of established legal standards that take into account also the interests of the data subject. Finally, it is already set out in current ICO guidance that a controller is not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information ([35]).

(31) Moreover, the Data (Use and Access) Act introduced a new Section 45A into the DPA 2018, creating an explicit exemption from the obligation to provide access or information to a data subject where the information is protected by legal professional privilege ([36]). This exemption applies specifically to the duties under Sections 44(2) and 45(1) of the DPA 2018, which require controllers to inform individuals about the processing of their personal data and to grant them access to that data ([37]). It clarifies that controllers are not required to disclose information if doing so would breach legal professional privilege. A similar exemption exists under the UK GDPR ([38]).

(32) In terms of safeguards, when relying on this exemption, controllers must inform the data subject in writing and without undue delay that the exemption has been applied, explain the reasons for doing so, and inform them of their right to seek a review by the Information Commission or to pursue legal remedies ([39]). To ensure accountability, Section 45A(4) of the DPA 2018 requires controllers to keep a record of the reason for their decision to apply the exemption and to make this record available to the Information Commission upon request ([40]).

([31]) Section 54(3A) and Section 54(b3) of the DPA 2018, as introduced by Section 76(6) of the Data (Use and Access) Act.
([32]) Section 54(3C) and (3D) of the DPA 2018, as introduced by Section 76(5) and (6) of the Data (Use and Access) Act.
([33]) Section 45(2A) of the DPA 2018, as introduced by Section 78 of the Data (Use and Access) Act.
([34]) *Dawson-Damer* v *Taylor Wessing LLP* [2017] EWCA Civ 74.
([35]) Available at the following link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.
([36]) Section 45A, as introduced by Section 79 of the Data (Use and Access) Act. In the UK, legal professional privilege is a core legal right that shields specific confidential communications between a client and their legal adviser from being disclosed without the client's consent. It includes two main categories: legal advice privilege, which protects exchanges made for the purpose of obtaining or providing legal advice, and litigation privilege, which applies to communications made in preparation for or during legal proceedings.
([37]) Competent authorities under Part 3 previously relied on other available exemptions within Section 44(4) (Right to be informed) and Section 45(4) (Right of access) of the DPA 2018.
([38]) Schedule 2, paragraph 19 of the DPA 2018.
([39]) Section 45A(2) of the DPA 2018, as introduced by Section 79 of the Data (Use and Access) Act. An exception to this notification requirement applies where providing such notice would itself undermine the privileged or confidential nature of the information. In such cases, the controller is not required to reveal that the exemption has been used or to provide any further explanation.
([40]) Section 45A of the DPA 2018, as introduced by Section 79 of the Data (Use and Access) Act.

(33) Finally, the Data (Use and Access) Act has amended and consolidated existing exemptions in Part 3 of the DPA 2018 available to competent authorities for national security purposes. The national security exemption allows competent authorities to disapply certain provisions of Part 3 of the DPA 2018 if exemption from that provision is required for the purposes of safeguarding national security ([41]). It mirrors the national security exemptions provided for the processing of personal data under the UK GDPR (provided in Section 26 of the DPA 2018) and under Part 4 of the DPA 2018 (provided in Section 110 of the DPA 2018).

(34) The national security exemption is subject to the same limitations and safeguards as the exemptions under the UK GDPR and Part 4 of the DPA 2018, as analysed in recitals 64 to 67 and 126 of Implementing Decision (EU) 2021/1772. In particular, the exemption can only be applied if and to the extent that it is required to safeguard national security. It is not a blanket exemption and must be considered and invoked by the controller on a case-by-case basis ([42]). Moreover, any application of the exemption must be in compliance with human right standards (underpinned by the Human Rights Act 1998 and the European Convention on Human Rights), according to which any interference with privacy rights should be necessary and proportionate in a democratic society ([43]). This is also confirmed in the ICO's guidance on the application of national security exemptions ([44]).

2.2.3. *Restrictions on onward transfers*

(35) The level of protection afforded to personal data transferred from the European Union to law enforcement authorities in the United Kingdom continues not to be undermined by the further transfer of such data to recipients in third countries. 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, as assessed in recitals 74 to 87 of Implementing Decision (EU) 2021/1773.

(36) While the Data (Use and Access) Act amended Chapter 5 of Part 3 of the DPA 2018 on transfers of personal data to competent authorities in third countries, it retains the core requirement that (a) the transfer must be necessary for a law enforcement purpose; (b) the transfer must be based on (i) regulations approving the transfer (replacing the previous adequacy regulations); (ii) is made subject to appropriate safeguards; or (iii) is based on special circumstances; and (c) the recipient of the transfer must be: (i) a relevant authority (i.e. the equivalent of a competent authority) in a third country; (ii) a relevant international organisation; (iii) a processor processing on behalf of a competent authority; or (iv) a person other than a relevant authority, but only where the transfer is strictly necessary for performing one of the law enforcement purposes ([45]). These general principles for data transfers are reflected in Section 73 of the DPA 2018, which also specifies that transfers of personal data to a third country or international organisation are only allowed if the transfer is carried out in compliance with the other provisions of Part 3 of the DPA 2018 ([46]).

(37) With respect specifically to the regulations approving a transfer, Section 74AA(2) of the DPA 2018 specifies that the Secretary of State may only make such regulations if (s)he considers that the data protection test is met. This means that the possibility for the Secretary of State introduced in Section 74AA(3) of the DPA 2018 to take into account the desirability of facilitating data flows when making such regulations is always subject to the condition that the data protection test being met. The new Section 74AB ([47]) of the DPA 2018 formulates the legal standard for the data protection test to be met, requiring that the standard of protection for data subjects in recipient countries or in international organisations is not materially lower than the standard provided for data subjects under the relevant United Kingdom data protection legislation. Section 74AB(2) of the DPA 2018 then provides for a non-exhaustive

([41]) Section 78A(1) of the DPA 2018, as introduced by Section 88 of the Data (Use and Access) Act. Pursuant to Section 78A(2) – (4) of the DPA 2018, the exemption allows to disapply the data protection principles (except the principle of lawfulness and the conditions and safeguards for the processing of sensitive data), the individual rights, the obligations of data controllers and processors with respect to data breaches, certain parts of the rules on international data transfers, and some of the Information Commissioner's powers of entry to conduct inspections and to take enforcement action.

([42]) See *Baker* v *Secretary of State for the Home Department* [2001] UKIT NSA2 ('*Baker v Secretary of State*').

([43]) See also *Guriev* v *Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), paragraph 45; *Lin* v *Commissioner of the Police for the Metropolis* [2015] EWHC 2484 (QB), paragraph 80.

([44]) See ICO's guidance on the national security and defence exception, available at the following link https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

([45]) Section 73 of the DPA 2018, as amended by paragraph 3(4) and (5) of Schedule 8 to the Data (Use and Access) Act.

([46]) Section 73 of the DPA 2018, as amended by paragraph 3(3) of Schedule 8 to the Data (Use and Access) Act.

([47]) As introduced by paragraph 4(2) of Schedule 8 to the Data (Use and Access) Act.

list of elements to consider when assessing whether that test is met, such as respect for the rule of law and for human rights, the existence and powers of a data protection authority, the arrangements for judicial or non-judicial redress, the rules about the transfer of personal data from the country or by the organisation to other countries or international organisations, the relevant international obligations of the country or organisation, and the constitution, traditions and culture of the country or organisation. While reformulating the list of relevant elements as provided under former section 74A of the DPA 2018, the new provision retains the core elements of that list and therefore remains close to what is provided in Article 36 of Directive (EU) 2016/680. Moreover, the United Kingdom authorities have confirmed that the Secretary of State will take into account elements not listed in Section 74AB(2), such as the laws and practices in a third country relating to how public authorities access personal data for purposes such as national security or law enforcement, to the extent that they affect the overall standard of protection. In addition, the United Kingdom authorities consider relevant case law in the third country will be an essential component of consideration of the matters listed non-exhaustively in Section 74AB(2) of the DPA 2018.

(38) Regulations approving a transfer continue to be subject to the 'general' procedural requirements provided for in Section 182 of the DPA 2018, as set out in recital 77 of Implementing Decision (EU) 2021/1773. Under this procedure, the Secretary of State must consult the Information Commissioner when proposing to adopt UK adequacy regulations ([48]). Once adopted by the Secretary of State, those regulations are laid before Parliament and subject to the 'negative resolution' procedure under which both Houses of Parliament can scrutinise the regulations and have the ability to pass a motion annulling the regulations within a 40 day period ([49]).

(39) With respect to appropriate safeguards, Section 75 of the DPA 2018, as amended by paragraph 6 of Schedule 8 to the Data (Use and Access) Act, sets out that such transfers may only proceed if: (a) an appropriate legal instrument binds the intended recipient of the data, meaning an instrument that satisfies the conditions set out in newly inserted paragraph 4, in particular that each United Kingdom competent authority party to the instrument, acting reasonably and proportionately, considers that the data protection test is met; or (b) the controller, acting reasonably and proportionately, considers that the data protection test is met in relation to the transfer or that type of transfer. The inserted Section 75(5) of the DPA 2018 clarifies that the data protection test is met if, due to the required safeguards, the standard of protection provided for data subjects is not materially lower after the transfer than the standard under the relevant United Kingdom data protection legislation. This is similar to the measures set under Article 37 of Directive (EU) 2016/680. As a result, the same legal standards apply in the EU and the UK concerning the approval of a transfer subject to appropriate safeguards. According to the newly inserted Section 75(6) of the DPA 2018, what is reasonable and proportionate is to be determined by reference to all the circumstances, or likely circumstances, of the transfer or type of transfer, including the nature and volume of the personal data transferred.

(40) Concerning transfers based on special circumstances pursuant to Section 76 of the DPA 2018, several technical amendments are introduced clarify the conditions under which such transfers may take place, but do not affect the level of protection for personal data in the United Kingdom ([50]).

(41) In terms of implementation of the United Kingdom's international transfer rules, there have been several developments since the adoption of Implementing Decision (EU) 2021/1773.

(42) First, following the conclusion of a Memorandum of Understanding in 2022 between the Home Office and the ICO, which defined their respective roles in conducting law enforcement adequacy assessments ([51]), the United Kingdom carried out evaluations of the data protection frameworks in the Bailiwicks of Jersey and Guernsey, as well as the Isle

([48]) See the Memorandum of Understanding between the Secretary of State for the Department for Digital, Culture, Media and Sport and the Information's Commissioner's Office on the role of the ICO in relation to new UK adequacy assessment, available at following link https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([49]) If such a vote is passed the regulations will ultimately cease to have any further legal effect.

([50]) Paragraph 7 of Schedule 8 to the Data (Use and Access) Act.

([51]) Available at the following link: https://ico.org.uk/media2/about-the-ico/mou/4025752/ico-ho-mou.pdf.

of Man. As a result, the United Kingdom adopted Adequacy Regulations for Guernsey in July 2023 ([52]), for Jersey in November 2023 ([53]), and for the Isle of Man in January 2025 ([54]). These regulations confirm that each jurisdiction ensures an adequate level of protection for personal data transferred under Part 3 of the DPA 2018. Although these regulations were originally adopted under the previous legal framework, the assessment underpinning them remains valid under the updated framework. As a result, the regulations continue to facilitate international cooperation in the area of law enforcement.

(43) The Commission also assessed the data protection frameworks for the processing of personal data in the context of criminal law enforcement well as the rules on access to personal data by public authorities for purposes of national security in the Bailiwicks of Jersey and Guernsey and the Isle of Man when evaluating the functioning of the adequacy decisions adopted on the basis of Article 25(6) of Directive 95/46/EC in accordance with Article 97 of Regulation (EU) 2016/679. Based, inter alia, on this assessment, the Commission concluded that all three jurisdictions continue to provide an adequate level of personal data transferred from the EU ([55]).

(44) Second, in 2022, the United Kingdom and the United States concluded the UK-US Data Protection and Privacy Agreement ([56]), which applies the terms of the EU-US Umbrella Agreement ([57]) *mutatis mutandis*, ensuring equivalent protections in the context of data exchanges between the United Kingdom and the United States for law enforcement purposes.

(45) Third, the ICO in 2023 and 2025 updated its guidance on international transfers under Part 3, Chapter 5 of DPA 2018 ([58]). The update in 2023 clarified the meaning of the 'strictly necessary' requirement for data transfers to recipients other than relevant law enforcement authorities, thus offering greater certainty for data controllers assessing the legality of such transfers. In 2025, the list of adequate countries and territories was updated following the United Kingdom adequacy regulations for the Isle of Man.

2.2.4. *Automated decision-making*

(46) While keeping several elements of the rules on automated decision-making assessed in recitals 72 and 73 of Implementing Decision (EU) 2021/1773, the Data (Use and Access) Act has amended some aspects of these rules.

(47) First, the newly introduced Section 50B of the DPA 2018 establishes a general prohibition against significant decisions based entirely or partly on the processing of special categories of personal data. However, it outlines two exceptions to this prohibition: the data subject has provided explicit consent for such processing; or the decision is required or authorised by law ([59]).

(48) Second, the newly introduced Section 50C of the DPA 2018 mandates that controllers implement safeguards for any significant decision based entirely or partly on personal data and based solely on automated processing. These safeguards must include providing information to the data subject about the decision-making process, allowing the

([52]) Available at the following link: https://www.legislation.gov.uk/uksi/2023/1221/contents/made.
([53]) Available at the following link: https://www.legislation.gov.uk/uksi/2023/744/made.
([54]) Available at the following link: https://www.legislation.gov.uk/uksi/2025/89/contents/made.
([55]) Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC of 15 January 2024, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0007; and Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC – Accompanying the document – Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, available at the following link: https://commission.europa.eu/document/download/f8229eb2-1a36-4cf5-a099-1cd001664bff_en?filename=JUST_template_comingsoon_Commission%20Staff%20Working%20Document%20-%20Report%20on%20the%20first%20review%20of%20the%20functioning.pdf.
([56]) Available at the following link: https://www.gov.uk/government/publications/ukusa-exchange-of-notes-on-the-protection-of-personal-information-relating-to-prevention-investigation-detection-and-prosecution-of-criminal-offe.
([57]) 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), available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN.
([58]) Available at the following link: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/international-transfers/.
([59]) Section 50B of the DPA 2018, as introduced by Section 80(3) of the Data (Use and Access) Act.

data subject to contest the decision or make representations, and ensuring the data subject can request human intervention in the decision-making process ([60]). While Section 50C(4) of the DPA 2018 creates an exemption from the application of these safeguards if such exemption is required to avoid obstructing an official or legal inquiry, investigation or procedure, to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, to protect public security, or to safeguard national security or to protect the rights and freedoms of others, the application of these safeguards is only temporarily suspended, given that the controller is required to reconsider the decision as soon as reasonably practicable and there is meaningful human involvement in the reconsideration of the decision ([61]).

(49) In addition, the new Section 50A of the DPA 2018 clarifies the definition of a decision that is 'based solely on automated processing' by providing that such decision is one where there is no meaningful human involvement in the decision-making process. Importantly, controllers are required to assess the extent to which profiling contributes to a decision to determine if human involvement has been meaningful. Section 50A of the DPA 2018 also clarifies that a 'significant decision' is one that produces adverse legal effects or similarly significant adverse effects on a data subject ([62]). This limitation to decisions which have an adverse effect on the data subject reflects the fact that, unlike processing under the UK GDPR, competent authorities are unlikely to take any decisions that data subjects regard as positive.

(50) Finally, the newly introduced Section 50D of the DPA 2018 grants the Secretary of State the authority to make secondary legislation to describe what constitutes, and what does not constitute, meaningful human involvement, what decisions are, and are not to be considered as having a similarly significant adverse effect on data subjects. It also enables the Secretary of State to make secondary legislation to (i) add new safeguards; (ii) impose requirements supplementing the existing safeguards; and (iii) define measures that do not satisfy the safeguards ([63]). Importantly, before adopting regulations in accordance with Section 50D of the DPA 2018, the Secretary of State must consult the ICO ([64]), and regulations are subject to the affirmative resolution procedure ([65]), which means they must be approved by both Houses of the UK Parliament before they can be enacted.

(51) While the Data (Use and Access) Act has thus modified the framework for automated decision-making, it is important to note that under the United Kingdom legal framework automated decision-making continues to be subject to the key safeguard requiring the right to obtain human intervention in all cases of automated decision-making, i.e. on the basis of the processing of sensitive and non-sensitive personal data ([66]).

2.2.5. *Accountability*

(52) The United Kingdom's legal framework continues to uphold the accountability principle enshrined in Directive (EU) 2016/680, requiring public authorities to implement appropriate technical and organisational measures to ensure and demonstrate compliance with data protection obligations, as assessed in recitals 88 to 92 of Implementing Decision (EU) 2021/1773.

(53) One of the measures included in the DPA 2018 to ensure accountability and to allow controllers and processors to demonstrate compliance is a requirement for competent authorities to keep logs of their processing activities, including the collection, alteration, consultation, disclosure, combination, and erasure of personal data ([67]). The Data (Use and Access) Act modifies the specific obligations for controllers pursuant to that provision by only removing in Section 62 of the DPA 2018 the requirement for controllers to record a justification when personal data is consulted or disclosed ([68]). Importantly, the requirement for controllers to log the processing activities as such remains in place, meaning that the main mechanism for ensuring accountability is preserved.

([60]) Section 50C of the DPA 2018, as introduced by Section 80(3) of the Data (Use and Access) Act.
([61]) Section 50C(3) and (4) of the DPA 2018, as introduced by Section 80(3) of the Data (Use and Access) Act.
([62]) Section 50A of the DPA 2018, as introduced by Section 80(3) of the Data (Use and Access) Act.
([63]) Article 50D of the DPA 2018, as introduced by Section 80(3) of the Data (Use and Access) Act. Any regulations made under these powers are subject to the affirmative resolution procedure, ensuring parliamentary oversight. The regulations cannot amend the requirements provided by Section 50C.
([64]) Section 182(2) of the DPA 2018.
([65]) Section 50D(5) of the DPA 2018.
([66]) Section 50C(2)(c) of the DPA 2018.
([67]) Section 62 of the DPA 2018. See also recital 90 of Implementing Decision (EU) 2021/1773.
([68]) Section 82 of the Data (Use and Access) Act.

2.3. **Oversight and enforcement**

2.3.1. *Independent oversight*

(54) In the United Kingdom, the oversight and enforcement of compliance with the data protection framework continue to be carried out by an independent data protection supervisory authority, as analysed in recitals 93 to 99 of Implementing Decision (EU) 2021/1773. The Data (Use and Access) Act reforms the governance structure of this authority by establishing a body corporate, the Information Commission, which will replace the ICO that was structured as a corporation sole.

(55) More specifically, the governance measures set out in the Data (Use and Access) Act, once implemented, will abolish the office of the Information Commissioner and transfer the functions, staff and property, from the ICO to the new body, the Information Commission. The Information Commission consists of executive and non-executive members ([69]). The Act also makes provisions for the Information Commissioner to transition the role of Chair of the Information Commission, who is one of the non-executive members ([70]). The Data (Use and Access) Act further provides that in so far as is appropriate in consequence of the transfer of functions, references to the Information Commissioner in all enactments or other documents (whenever passed or made) are to be treated as references to the Information Commission. To carry out its functions, the Commission may establish committees and delegate functions to a member, an employee or a committee of the Commission ([71]), and may make arrangements for regulating its procedure and the procedure of the committees, including with respect to a quorum and the taking of decisions by majority. These procedures must be made public ([72]).

(56) Importantly, the independence of the Information Commission is subject to the same safeguards, including with respect to the rules on the appointment and dismissal of the Chair, as the ones assessed in recitals 95 to 98 of Implementing Decision (EU) 2021/1773 ([73]). Similar protections apply with respect to the other non-executive members of the Information Commission. In particular, the Chair of the Information Commission is appointed by His Majesty on recommendation from the Secretary of State. (S)he is selected on merit and on the basis of a fair and open competition ([74]). The other non-executive members are appointed by the Secretary of State following consultations with the Chair. Candidates can be recommended for appointment or appointed only if selected on the basis of merit pursuant to fair and open competition and if the Secretary of State is satisfied that they do not have a conflict of interest ([75]). The executive members are employees of the Information Commission employed on terms and conditions as determined by the non-executive members ([76]). The Chief Executive is appointed by the Chair and other non-executive members, following consultations with the Secretary of State. The executive appointments are also subject to a selection on merit on the basis of a fair and open competition ([77]).

(57) The Chair may only be removed from office by His Majesty on an Address from both Houses of Parliament and only if the Secretary of State has presented a report to that House stating that the Secretary of State is satisfied that the chair is guilty of serious misconduct, has a conflict of interest, has failed to comply with specific information requirements with respect to potential conflicts of interest, or is unable, unfit or unwilling to carry out the chair's functions ([78]). Non-executive members may only be removed from office by the Secretary of State if (s)he is satisfied that the specific conditions set out in the legislation are met. These include conflict of interest, serious misconduct or being unable, unwilling or unfit to carry out their duties. In terms of additional safeguards, the Secretary of State is required to make public the decision to do so and give the member a statement of reasons for the removal ([79]).

([69]) Paragraph 3(1) of Schedule 12A to the DPA 2018.
([70]) Sections 117, 118, 119 and 120 together with Schedule 14 of the Data (Use and Access).
([71]) Paragraphs 13 and 14 of Schedule 12A to the DPA 2018.
([72]) Paragraph 16 of Schedule 12A to the DPA 2018.
([73]) Article 52 of the UK GDPR, as well as Schedule 12A of the DPA 2018, as introduced by Section 117 of the Data (Use and Access) Act.
([74]) Paragraph 5(1) of Schedule 12A to the DPA 2018.
([75]) Paragraphs 3(2), 5 and 6 of Schedule 12A to the DPA 2018.
([76]) Paragraph 11 of Schedule 12A to the DPA 2018.
([77]) Paragraphs 5(2) of Schedule 12A to the DPA 2018.
([78]) Paragraph 7(6) and (7) of Schedule 12A to the DPA 2018.
([79]) Paragraph 9(6), (7), (8) and (9) of Schedule 12A to the DPA 2018.

(58) The Data (Use and Access) Act does not alter the core responsibilities of the Information Commission, which will continue to carry out the functions set out in Schedule 13 of the DPA 2018. These include monitoring and enforcing compliance with Part 3 of the DPA 2018, advising Parliament and the government, raising public awareness, supporting data controllers and processors in meeting their obligations, and informing individuals of their rights ([80]). The Data (Use and Access) Act clarifies that, in exercising the duty to ensure an appropriate level of protection for personal data, the Information Commission will have to take into account the interests of data subjects, controllers, and others, consider the wider public interest, and promote public trust and confidence in the processing of personal data ([81]).

(59) In addition, the Data (Use and Access) Act specifies that the Information Commission shall consider, insofar as relevant in the circumstances, the promotion of innovation and competition, the importance of the prevention, investigation, detection and prosecution of criminal offences, the need to safeguard public security and national security, and the specific needs related to the protection of children when carrying out its function under the data protection legislation ([82]). EU data protection law also recognises the need to balance the protection of personal data with several other fundamental rights, and objectives, such as security and justice ([83]).

2.3.2. *Enforcement, including sanctions, and redress*

(60) The powers and tasks of the Information Commission continue to correspond to those of the data protection supervisory authorities of the Member States pursuant to the relevant articles of Directive (EU) 2016/680 ([84]), as assessed in recitals 100 to 109 of Implementing Decision (EU) 2021/1773.

(61) The Data (Use and Access) Act has introduced certain clarifications concerning the exercise of some of these powers.

(62) Section 97 of the Data (Use and Access) Act amends Section 142 of the DPA 2018 to expressly allow the Information Commission to require not only information but also specific documents, improving its ability to investigate and verify compliance.

(63) Section 98 of the Data (Use and Access) Act enhances the Information Commission's powers under Section 146 of the DPA 2018 by allowing the Information Commission to require a data controller or processor to commission an independent report on a specified matter. The report must be prepared by an 'approved person', with the Information Commission having final authority to approve the nominee or appoint someone if no suitable nominee is proposed or if the controller fails to act ([85]). The assessment notice can specify the report's format, content, and deadline ([86]). All related costs, including the approved person's fees, must be covered by the controller or processor ([87]).

(64) Section 100 of the Data (Use and Access) Act establishes interview notices as a new enforcement tool under Section 148A of the DPA 2018. The Information Commission may require an individual to attend interviews with safeguards in place such as protection against self-incrimination and legal privilege ([88]).

(65) Section 101 of the Data (Use and Access) Act amends Schedule 16 of the DPA 2018 to provide the Information Commission with greater flexibility in issuing penalty notices. While the current six-month deadline for issuing a final penalty notice following a notice of intent remains the general rule, the section permits the Information Commission to issue a penalty notice beyond this timeframe where it is not reasonably practicable to meet the deadline. In such cases, the notice must be issued as soon as reasonably practicable. Additionally, where the Information Commission decides not to issue a penalty notice, they must inform the concerned individual in writing within six months or as soon as reasonably practicable thereafter. The section also introduces a new requirement for the Information Commission to publish guidance on the circumstances in which more than six months may be needed to issue a penalty notice.

([80]) Schedule 13 to the DPA 2018.
([81]) Section 91 of the Data (Use and Access) Act, introducing Section 120A of the DPA 2018.
([82]) Section 91 of the Data (Use and Access) Act, introducing Section 120B of the DPA 2018.
([83]) See in particular recital 2 of Directive (EU) 2016/680.
([84]) Paragraph 2 of Schedule 13 to the DPA 2018.
([85]) Section 98 of the Data (Use and Access) Act, introducing Section 146A of the DPA 2018.
([86]) Section 98 of the Data (Use and Access) Act, introducing Section 146(3A) of the DPA 2018.
([87]) Section 98 of the Data (Use and Access) Act, introducing Section 146(11A) of the DPA 2018.
([88]) Section 98 of the Data (Use and Access) Act, introducing Section 146(8B) of the DPA 2018.

(66) Section 102 of the Data (Use and Access) Act introduces new reporting obligations for the Information Commission. It amends Section 139 and inserts a new Section 161A into the DPA 2018, requiring the Information Commission to publish an annual report on regulatory action. This report must detail how investigation and enforcement powers under the UK GDPR and Parts 3 and 4 of the DPA 2018 have been exercised. It must also disclose the number of penalty notices issued beyond the six-month window following a notice of intent and provide justifications for the delay. Furthermore, the report must explain how the Information Commission has followed their own guidance when taking regulatory decisions.

(67) Section 103 of the Data (Use and Access) Act strengthens the complaints procedure available to data subjects. It inserts new Sections 164A and 164B into the DPA 2018. Section 164A provides that data subjects have the right to lodge complaints directly with data controllers if they believe their rights under the UK GDPR or Part 3 of the DPA 2018 have been infringed. Controllers must facilitate this process, acknowledge complaints within 30 days, and respond without undue delay. They must also keep complainants informed about the progress and outcome. Section 164B gives the Secretary of State the power to make regulations requiring controllers to report the number of complaints received.

(68) Section 104 of the Data (Use and Access) Act inserts a new Section 180A into the DPA 2018 to clarify the court's powers in data subjects' access request proceedings. Under this provision, courts may require data controllers to provide the disputed information for the court's inspection when deciding whether a data subject is entitled to it. However, the information cannot be disclosed to the data subject unless the court determines they have a right to access it. This section clarifies courts can examine disputed material without prematurely disclosing it to the claimant, restoring a safeguard that previously existed under the Data Protection Act 1998.

(69) In terms of the implementation of these powers, since the adoption of Implementing Decision (EU) 2021/1773 the Information Commissioner has handled numerous complaints ([89]) and conducted several investigations and taken enforcement measures with respect to the processing of data by law enforcement authorities. Between 2021 and 2025, the Information Commissioner conducted investigations and issued reprimands against various police bodies for different failures to comply with their data protection obligations, for instance when responding to requests for access to data, when putting in place security measures for video surveillance data, when dealing with sensitive criminal records, when merging the data of different individuals, or when disclosing personal data to third parties ([90]). The Information Commissioner also issued and updated guidelines, opinions and guidance documents, for example on the right of access or on how to handle manifestly unfounded or excessive requests under Part 3 of the DPA 2018 ([91]), or updated existing guidelines, such as its Guide on Law Enforcement Processing ([92]).

3. **CONCLUSION**

(70) The Commission considers that Part 3 of the DPA 2018 continues to ensure a level of protection for personal data transferred for criminal law enforcement purposes from competent authorities in the European Union to United Kingdom competent authorities which is essentially equivalent to the one guaranteed by Directive (EU) 2016/680.

([89]) For example, the Information Commission in 2023-2024 received 1 890 complaints on the basis of the GDPR and/or the DPA 2018 about organisations within the subsectors 'Police Authority', 'Police Forces' and 'Police Commissioners'. See also Information Commissioner's Annual Report and Financial Statements 2023/24, available at the following link: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([90]) Additional information is available at the following link: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([91]) Available at the following link: https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ and https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([92]) Available at the following link: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/.

(71) Moreover, the Commission considers that, taken as a whole, the oversight mechanisms and redress avenues in United Kingdom law continue to enable infringements to be identified and sanctioned in practice and offer legal remedies to the data subject to obtain access to personal data relating to him/her and, eventually, the rectification or erasure of such data.

(72) Therefore, it should be decided that the United Kingdom continues to ensure an adequate level of protection within the meaning of Article 36(2) of Directive (EU) 2016/680, interpreted in light of the Charter of Fundamental Rights.

4. EFFECTS OF THIS DECISION AND ACTION OF DATA PROTECTION AUTHORITIES

(73) Member States and their organs are required to take the measures necessary to comply with acts of the Union institutions, as the latter are presumed to be lawful and accordingly produce legal effects until such time as they expire, are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality.

(74) Consequently, a Commission adequacy decision adopted pursuant to Article 36(3) of Directive (EU) 2016/680 is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities. In particular, during the period of application of Implementing Decision (EU) 2021/1773, as amended by this Decision, transfers from a controller or processor in the Union to controllers or processors in the United Kingdom may take place without the need to obtain any further authorisation.

(75) At the same time, it should be recalled that, pursuant to Article 47(5) of Directive (EU) 2016/680, and as explained by the Court of Justice in the *Schrems I* judgment, where a national data protection authority questions, including upon a complaint, the compatibility of a Commission adequacy decision with the fundamental rights of the individual to privacy and data protection, national law must provide it with a legal remedy to put those objections before a national court, which may be required to make a reference for a preliminary ruling to the Court of Justice ([93]).

5. MONITORING

(76) Pursuant to Article 36(4) of Directive (EU) 2016/680, the Commission is to monitor, on an ongoing basis, relevant developments in the United Kingdom, in order to assess whether it still ensures an essentially equivalent level of protection. Such monitoring is particularly important because the United Kingdom will apply and enforce a modified data protection regime. Moreover, the United Kingdom's modified data protection framework provides the Secretary of State with the power to further specify this framework through secondary legislation. In that respect, special attention should be paid to such additional specifications, as well as to the application in practice of the United Kingdom's modified rules on transfers of personal data to third countries; to the effectiveness of the exercise of individual rights, including any relevant developments in law and practice concerning the newly introduced exceptions to or restrictions of such rights, and to the functioning of the restructured ICO, including with respect to complaint handling and the application of corrective powers. Amongst other elements, case law developments and oversight by the ICO and other independent bodies should inform the Commission's monitoring.

(77) In order to facilitate this monitoring, the United Kingdom authorities should promptly and regularly inform the Commission of any material change to the United Kingdom legal order that has an impact on the legal framework that is the object of the Implementing Decision (EU) 2021/1773, as amended by this Decision, as well as any evolution in practices related to the processing of the personal data assessed in Implementing Decision (EU) 2021/1773, as amended by this Decision, as amended by this Decision, in particular with respect to the elements mentioned in recital 39.

(78) Moreover, in order to allow the Commission to effectively carry out its monitoring function, the Member States should inform the Commission about any relevant action undertaken by the national data protection authorities, in particular regarding queries or complaints by EU data subjects concerning the transfer of personal data from the Union to competent authorities in the United Kingdom. The Commission should also be informed about any indications that the actions of United Kingdom public authorities responsible for the prevention, investigation, detection or prosecution of criminal offences, including any oversight bodies, do not ensure the required level of protection.

([93]) *Schrems I*, paragraph 65.

(79) Where available information, in particular information resulting from the monitoring of this Decision or provided by United Kingdom or Member States' authorities, reveals that the level of protection afforded by the United Kingdom may no longer be adequate, the Commission should promptly inform the competent United Kingdom authorities thereof and request that appropriate measures be taken within a specified timeframe, which may not exceed three months. Where necessary, this period may be extended for a specified period of time, taking into account the nature of the issue at stake and/or of the measures to be taken.

(80) If, at the expiry of that specified timeframe, the competent United Kingdom authorities fail to take those measure or otherwise demonstrate satisfactorily that this Decision continues to be based on an adequate level of protection, the Commission will initiate the procedure referred to in Article 58(2) of the Directive (EU) 2016/680 with a view to partially or completely suspend or repeal this Decision.

(81) Alternatively, the Commission will initiate this procedure with a view to amend Implementing Decision (EU) 2021/1773, as amended by this Decision, in particular by subjecting data transfers to additional conditions or by limiting the scope of the adequacy finding only to data transfers for which an adequate level of protection continues to be ensured.

(82) On duly justified imperative grounds of urgency, the Commission will make use of the possibility to adopt, in accordance with the procedure referred to in Article 58(3) of the Directive (EU) 2016/680, immediately applicable implementing acts suspending, repealing or amending the Decision.

6. REVIEW, DURATION AND RENEWAL OF THIS DECISION

(83) In application of Article 36(3) of Directive (EU) 2016/680 and in the light of the fact that the level of protection afforded by the UK's legal framework may be liable to change, the Commission, following the adoption of this Decision, should periodically review whether the findings relating to the adequacy of the level of protection ensured by the UK are still factually and legally justified. Such evaluations should take place at least every four years and should cover all aspects of the functioning of this Decision, including the functioning of the relevant oversight and enforcement mechanisms.

(84) To perform the review, the Commission should meet with relevant representatives from the UK authorities, including the Information Commission. Participation in that meeting should be open to representatives of the members of the European Data Protection Board. In the framework of the review, the Commission should request the UK to provide comprehensive information on all aspects relevant for the adequacy finding. The Commission should also seek explanations on any information relevant for this Decision that it has received, including from the EDPB, individual data protection authorities, civil society groups, public or media reports, or any other available source of information.

(85) On the basis of the review, the Commission should prepare a public report to be submitted to the European Parliament and the Council.

(86) The Commission must also take into account that the data protection framework assessed in this Decision and in Implementing Decision (EU) 2021/1773 may further evolve.

(87) It is therefore appropriate to provide that this Decision will apply for a period of six years as of its entry into force.

(88) Where in particular information resulting from the monitoring of this Decision reveals that the findings relating to the adequacy of the level of protection ensured in the United Kingdom are still factually and legally justified, the Commission should, at the latest six months before this Decision cease to apply, initiate the procedure to amend this Decision by extending its temporal scope, in principle, for an additional period of four years. Any such implementing act amending this Decision is to be adopted in accordance with the procedure referred to in Article 58(2) of Directive (EU) 2016/680.

7. FINAL CONSIDERATIONS

(89) The European Data Protection Board published an opinion ([94]) which has been taken into consideration in the preparation of this Decision.

(90) The measure provided for in this Decision is in accordance with the opinion of the Committee established under Article 58 of Directive (EU) 2016/680.

(91) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Directive (EU) 2016/680, and hence this implementing decision, which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU. Nevertheless, by virtue of Council Implementing Decision (EU) 2020/1745 ([95]), Directive (EU) 2016/680 is to be put into effect and applied on a provisional basis in Ireland as of 1 January 2021. Ireland is therefore bound by this Decision, under the same conditions as apply to the application of Directive (EU) 2016/680 in Ireland as set out in Implementing Decision (EU) 2020/1745, as regards the part of the Schengen *acquis* in which it participates.

(92) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not bound by the rules laid down in Directive (EU) 2016/680, and hence this Implementing Decision, or subject to their application which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU. However, given that Directive (EU) 2016/680 builds upon the Schengen *acquis*, Denmark, in accordance with Article 4 of that Protocol, notified on 26 October 2016 its decision to implement Directive (EU) 2016/680. Denmark is therefore bound under international law to implement this Decision.

(93) As regards Iceland and Norway, this Decision constitutes a development of provisions of the Schengen *acquis*, within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* ([96]).

(94) As regards Switzerland, this Decision constitutes a development of provisions of the Schengen *acquis*, within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis* ([97]).

(95) As regards Liechtenstein, this Decision constitutes a development of provisions of the Schengen *acquis*, within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([98]).

(96) Implementing Decision (EU) 2021/1773 should therefore be amended accordingly,

([94]) Opinion 27/2025 regarding the European Commission Draft Implementing Decision amending on the adequate protection of personal data by the United Kingdom, available at the following link https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-272025-regarding-european-commission-draft_en.

([95]) Council Implementing Decision (EU) 2020/1745 of 18 November 2020 on the putting into effect of the provisions of the Schengen *acquis* on data protection and on the provisional putting into effect of certain provisions of the Schengen *acquis* in Ireland (OJ L 393, 23.11.2020, p. 3, ELI: http://data.europa.eu/eli/dec_impl/2020/1745/oj).

([96]) Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen acquis (OJ L 176, 10.7.1999, p. 36, ELI: http://data.europa.eu/eli/agree_internation/1999/439(1)/oj).

([97]) OJ L 53, 27.2.2008, p. 52.

([98]) OJ L 160, 18.6.2011, p. 21.

HAS ADOPTED THIS DECISION:

Article 1

Article 4 of Implementing Decision (EU) 2021/1773 is replaced by the following:

'*Article 4*

This Decision shall expire on 27 December 2031, unless extended in accordance with the procedure referred to in Article 58(2) of Directive (EU) 2016/680.'

Article 2

This Decision is addressed to the Member States.

Done at Brussels, 19 December 2025.

For the Commission
Michael MCGRATH
Member of the Commission