EUROPEAN
COMMISSION

Brussels, 19.12.2025
C(2025) 8771 final

COMMISSION IMPLEMENTING DECISION

of 19.12.2025

amending Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (notified under document C(2021)4800)

(Text with EEA relevance)

COMMISSION IMPLEMENTING DECISION

of 19.12.2025

amending Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (notified under document C(2021)4800)

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) 2016/679 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 (General Data Protection Regulation) ([1]), and in particular Article 45(3) thereof,

Whereas:

1. INTRODUCTION

(1) Implementing Decision (EU) 2021/1772 ([2]) concludes that for the purposes of Article 45 of Regulation (EU) 2016/679, 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 Regulation ([3]).

(2) When adopting Implementing Decision (EU) 2021/1772, the Commission took into account that, after 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 ([4]) and after 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 ([5])

---

(1) OJ L 119, 4.5.2016, p. 1.

(2) Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 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. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).

(3) See Article 1(1) of Decision (EU) 2021/1772. Under Article 1(2) of that Decision, the Decision does not cover personal data transferred for the purposes of United Kingdom immigration control or otherwise falling under the scope of the exemption for certain data subject rights for the purposes of maintaining effective immigration control pursuant to paragraph 4(1) of Schedule 2 to the UK Data Protection Act 2018.

(4) OJ C 384I, 12.11.2019, p. 1.

(5) OJ L 149, 30.4.2021, p. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.

ceased to apply, the United Kingdom would 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) 2021/1772 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) 2021/1772 was therefore set to expire on 27 June 2025, unless extended in accordance with the procedure referred to in Article 93(2) of Regulation (EU) 2016/679.

(4) To decide on a possible extension of Implementing Decision (EU) 2021/1772, 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) 2021/1772 with respect to the elements listed in Article 45(2) of Regulation (EU) 2016/679.

(5) In particular, on 23 October 2024, the UK Government introduced the Data (Use and Access) Bill ([6]) into the UK Parliament, proposing amendments to the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) which are assessed in Implementing Decision (EU) 2021/1772. The Commission on 24 June 2025 adopted Implementing Decision (EU) 2025/, which extended the validity of Decision (EU) 2021/1772 for a period of six months until 27 December 2025 ([7]). 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 ([8]).

(6) Since the adoption of Implementing Decision (EU) 2021/1772, the Commission monitored, on an ongoing basis, relevant developments in the United Kingdom ([9]). In accordance with recital (281) of Implementing Decision (EU) 2021/1772, 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) 2021/1772, 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 (notably the one relating to the maintenance of effective immigration control), as well as compliance with the limitations and safeguards with respect to government access. 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 UK GDPR and the DPA 2018 introduced by the Data (Use and Access) Act, the Commission concludes that the United Kingdom continues to ensure an adequate level

---

([6]) Available at the following link: https://bills.parliament.uk/bills/3825/news.

([7]) Commission Implementing Decision (EU) 2025/1226 amending Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, OJ L 2025/1226 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj

([8]) The Data (Use and Access) Act received Royal Assent on 19 June 2025.

([9]) Article 45(4) of Regulation (EU) 2016/679.

of protection for personal data transferred within the scope of Regulation (EU) 2016/679 from the European Union to the United Kingdom.

(8) The Commission also concludes that, in light of amendments to the relevant provisions of United Kingdom law ([10]), the exclusion of personal data transferred for United Kingdom immigration control purposes or which otherwise falls within the scope of the exemption from certain data subject rights for purposes of the maintenance of effective immigration control (the "immigration exemption") pursuant to paragraph 4(1) of Schedule 2 to the UK Data Protection Act, from the scope of Implementing Decision (EU) 2021/1772 is no longer justified, as explained in recital (37) of this Decision.

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

2.1. The data protection framework of the United Kingdom

(9) When Implementing Decision (EU) 2021/1772 was adopted, the legal framework on the protection of personal data in the United Kingdom consisted of:

– The UK GDPR ([11]), as incorporated into the law of the United Kingdom under the European Union (Withdrawal) Act 2018 ([12]) and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations) ([13]),

---

(10) In May 2021, the England and Wales Court of Appel had found the immigration exemption as formulated at the time in paragraph 4(1) of Schedule 2 to the UK Data Protection Act incompatible with UK laws, as the legislative measure lacked specific provisions setting out the safeguards listed in Article 23(2) of the UK GDPR. In order to comply with the judgement, the UK Government revised the immigration exemption by passing The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022. However, the revised exemption was again challenged on the basis that it did not meet all the requirements of Article 23(2) of the UK GDPR. In a judgment of 11 December 2023, the Court of Appeal declared the revised immigration exemption again incompatible with Article 23(2) UK GDPR. To comply, the UK Government then passed the Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024, which entered into force on 8 March 2024.

(11) General Data Protection Regulation, available at the following link: https://www.legislation.gov.uk/eur/2016/679/contents.

(12) The European Union (Withdrawal) Act 2018, available at the following link: https://www.legislation.gov.uk/ukpga/2018/16/contents, incorporated Union legislation that was directly applicable in the United Kingdom at the end of the transition period into the law of the United Kingdom. This so-called "retained EU law" included Regulation (EU) 2016/679 in its entirety, including its recitals (see Explanatory Notes to the European Union (Withdrawal) Act 2018, paragraph 83, available at the following link: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). In accordance with that Act, the unmodified retained EU law had to be interpreted by the courts of the United Kingdom in accordance with the relevant case law of the European Court of Justice and general principles of Union law as they had effect immediately before the end of the transition period (called "retained EU case law" and "retained general principles of EU law" respectively).

(13) 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.

– the DPA 2018 ([14]), as amended by the DPPEC Regulations.

(10) While these two Acts that closely mirrored the corresponding rules applicable within the European Union continue to form the data protection legislation of the United Kingdom, they have since then been subject to limited amendments, reflecting that the United Kingdom is no longer subject to the law of the European Union.

(11) First, the Retained EU Law (Revocation and Reform) Act 2023 (REUL Act) ([15]) clarified that the general principles of EU law were no longer part of the United Kingdom's domestic law after the end of 2023 ([16]). In addition, United Kingdom courts are no longer required to interpret unmodified "assimilated law", which was previously referred to as "retained EU law", in accordance with the general principles of EU law, but such law must instead be read compatibly with domestic UK law ([17]). 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 ([18]), as also mentioned in recital (13) of Implementing Decision (EU) 2021/1772. The DPA 2018 has been amended by the Data (Use and Access) Act to clarify the effect of the REUL Act on the UK'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.

(12) Second, since the adoption of Implementing Decision (EU) 2021/1772, the data protection legislation of the United Kingdom has been amended through the Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023 ([19]). These Regulations define references to fundamental rights or fundamental freedoms in the UK GDPR and the DPA 2018 (which were previously defined to cover EU fundamental rights and fundamental freedoms ([20])), as references to rights under the

---

(14) 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.

(15) Available at the following link: https://www.legislation.gov.uk/ukpga/2023/28.

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

(17) Section 5(A2) of the European Union (Withdrawal) Act 2018, as amended by the REUL Act.

(18) Section 6(3) and (7) of the European Union Withdrawal Act 2018, as amended by the REUL Act.

(19) Available at the following link: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

(20) 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.

European Convention on Human Rights, which have been given effect in the United Kingdom's domestic law under the Human Rights Act 1998 ([21]). 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 ([22]).

(13) Finally, the UK GDPR and the DPA 2018 have 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 rules on data processing for purposes of scientific research, the legal bases for data processing, the rules relating to the purpose limitation principle, and the conditions for automated decision-making. 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 introduces new enforcement powers for the regulator.

(14) 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) 2021/1772. The assessment made in Implementing Decision (EU) 2021/1772 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) 2021/1772.

(15) 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 ([23]). As clarified by the Court of Justice of the European Union, this does not require finding an identical level of protection ([24]). 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 ([25]). 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 ([26]).

---

(21) Section 2(3) of the Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023.

(22) Articles 6, 8, 10 and 13 of the ECHR (see also Schedule 1 to the Human Rights Act 1998).

(23) Recital 104 of Regulation (EU) 2016/679.

(24) Case C-362/14, *Schrems* ("*Schrems I"*), ECLI:EU:C:2015:650, paragraph 73.

(25) *Schrems I*, paragraph 74.

(26) See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017)7 of 10.1.2017, section 3.1, pages 6-7,

2.1.1. Definitions

(16) Basic data protection concepts mirroring the terminology of Regulation (EU) 2016/67 continue to apply in the United Kingdom's data protection regime. These concepts have been assessed in recital (23) of Implementing Decision (EU) 2021/1772.

(17) While the Data (Use and Access) Act leaves the vast majority of definitions unchanged, it has introduced specific definitions related to the processing of personal data for scientific, historical, and statistical purposes in Article 4 paragraphs 2, 3, 4, and 5 of the UK GDPR. Paragraph 2 defines "processing for scientific purposes" as the processing of personal data conducted for purposes of any research that can reasonably be described as scientific. This research may be publicly or privately funded and may be conducted as either a commercial or non-commercial activity. Reflecting the content of recital (159) of Regulation (EU) 2016/679, Paragraph 3 provides a non-exhaustive list of examples of research activities that qualify as pursuing scientific purposes, including technical development, demonstration, fundamental research, and applied research. Paragraph 4 clarifies that "historical research" includes genealogical research, which is also recognised as a historical purpose in recital (160) of Regulation (EU) 2016/679. Lastly, paragraph 5 defines processing for statistical purposes as the processing of data for statistical surveys or to produce statistical results, where the data is aggregated to the extent that it no longer constitutes personal data. Moreover, the processed data or resulting information must not be used to make decisions or take actions directed at any individual. This definition aligns with the understanding of statistical purposes outlined in recital (162) of Regulation (EU) 2016/679.

(18) In conclusion, while the amendments to Article 4 of the UK GDPR add specific definitions of data processing for scientific, historical, and statistical purposes, such definitions are consistent with the letter and the spirit of Regulation (EU) 2016/679, as reflected in the above-mentioned recitals (159), (160), and (162).

(19) By adding paragraph 6 to Article 4 of the UK GDPR, the Data (Use and Access) Act has also established a specific framework for obtaining consent from the data subject for the processing of personal data for scientific purposes. In very similar terms as recital (33) of Regulation (EU) 2016/679, which recognises that in the area of scientific research, consent cannot always be obtained for a specific processing purpose, the new provision allows for broader forms of consent by allowing that data subjects can give valid consent even when the exact purposes of the research cannot be fully identified at the time of the data collection, provided that the seeking of consent is consistent with generally recognised ethical standards relevant to the specific research area. In any case, data subjects must have the opportunity to consent to the processing of personal data only for specific parts of the research, where possible.

(20) Finally, the Data (Use and Access) Act has further detailed the safeguards previously found in Article 89 of the UK GDPR and section 19 of the DPA 2018 for data processing for archiving in the public interest, scientific, historic and statistical research purposes in a new Chapter 8A of the UK GDPR ([27]). These safeguards are similar to those required by Article 89 of Regulation (EU) 2016/679 and include the

---

available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

[27] Articles 84A to 84D of the UK GDPR, as introduced by Section 86 of the Data (Use and Access) Act.

requirement to provide technical and organisational measures for the purpose of ensuring respect for the principle of data minimisation.

2.2. Safeguards, rights and obligations

2.2.1. Lawfulness and fairness of processing

(21) The data protection framework of the United Kingdom continues to require that data is processed in a lawful, fair and legitimate manner, as assessed in recitals (24) to (26) of Implementing Decision (EU) 2021/1772.

(22) The principles of lawfulness and fairness and the grounds for lawful processing continue to be guaranteed in the law of the United Kingdom through Articles 5(1)(a) and 6(1) of the UK GDPR, as assessed in Implementing Decision (EU) 2021/1772. While those provisions remain largely identical ([28]) to the respective provisions in Regulation (EU) 2016/679, the Data (Use and Access) Act first amends Article 6(1) of the UK GDPR by introducing an additional lawful ground for the processing of personal data under Article 6(1)(ea) ([29]). According to that provision, processing shall be lawful if and to the extent that it "is necessary for the purposes of a recognised legitimate interest". Unlike the legal ground of legitimate interest pursuant to Article 6(1)(f) of the UK GDPR, the newly introduced legal ground of recognised legitimate interest does not require a case-by-case balancing of the legitimate interests of the controller against the interests or fundamental rights and freedoms of the data subject, which is intended to give greater legal certainty to non-public body controllers. The newly introduced Article 6(5) of the UK GDPR specifies that processing is necessary for the purposes of a recognised legitimate interest only if it meets a condition in Annex 1 ([30]), which then lists situations in which processing is considered necessary for the purposes of a recognised legitimate interest, for example where it takes place in response to a request received by a public authority who needs the data for the purposes of the performance of a task carried out in the public interest that has a legal basis that satisfies Article 6(3) of the UK GDPR, where processing is necessary to safeguard national security, protect public security or for defence purposes, to respond to an emergency, to detect, investigate or prevent crime or to safeguard vulnerable individuals ([31]).

([28]) For purposes of clarification, the Data (Use and Access) Act also introduces in Article 6 of the UK GDPR a new paragraph which provides examples of types of processing that may be considered as necessary for the purpose of legitimate interest within the meaning of Article 6(1)(f) of the UK GDPR. These examples (direct marketing, intra-group transmission of data for administrative purposes, and the security of networks and information systems) are also mentioned in recitals 47 and 48 of Regulation (EU) 2016/679 as situations where processing would be considered in the legitimate interest of the controller.

([29]) Section 70(2)(b) of the Data (Use and Access) Act. Section 70(5) of the Data (Use and Access) Act has extended the right to object in Article 21 of the UK GDPR to the new Article 6(1)(ea) of the UK GDPR.

([30]) Section 70(4) of the Data (Use and Access) Act.

([31]) See Schedule 4 to the Data (Use and Access) Act. According to the UK authorities, examples of situations where non-public bodies may need to process personal data to prevent or detect crime include a company that becomes aware of attempts to unlawfully hack their computer systems, or a bank or financial institution that becomes aware of fraudulent attempts to open an account. Processing of personal data by a non-public body may for example be necessary to safeguard national security or defence where a commercial organisation suspects that a customer's online activity indicated involvement in terrorist activity. The ICO is working on specific guidance on this matter, including a definition of the relevant concepts. For example, it refers to 'national security' being likely to cover the security and well-being of the UK as whole, its population, its institutions and system of government.

(23) While the Data (Use and Access) Act thus extends the list of legal grounds for the processing of personal data that are available to the controller, the newly introduced legal ground of recognised legitimate interest is subject to several important limitations. First, the recognised legitimate interests are limited to specific situations which are listed exhaustively in the law. Second, this legal ground cannot be relied upon by public authorities in the performance of their tasks ([32]). Third, it only concerns areas where there is a clear public interest in the processing activity (according to the conditions set out in Annex 1), i.e. where the processing serves objectives listed in Article 23 UK GDPR (which corresponds to Article 23 of Regulation (EU) 2016/679) and can thus not be relied upon for commercial purposes. Fourth, while the Data (Use and Access) Act grants the Secretary of State the right to amend the list in Annex 1 by means of Regulation ([33]), the Secretary of State may only make such Regulation after having consulted the ICO ([34]) and add a recognised legitimate interest to that list only where that processing is again necessary to safeguard a public interest objective listed in Article 23(1)(c) to (j) of the UK GDPR ([35]). Finally, as also confirmed by the ICO's guidance ([36]), data controllers relying on a recognised legitimate interest as a legal basis are required to comply with all other requirements under the UK GDPR, including ensuring that the processing is necessary and proportionate to achieve the legitimate interest.

(24) Second, the Data (Use and Access) Act clarifies in Articles 6(3), 9(2)(g) and 10(1) of the UK GDPR, which correspond to the respective provisions of Regulation (EU) 2016/679, that the basis for the processing of personal data, special categories of personal data and personal data relating to criminal convictions and offences in compliance with a legal obligation or for the performance of a task in the public interest can have a basis not only in domestic law, but also in relevant international law ([37]). Relevant international law is then limited by the newly introduced Article 9A of the UK GDPR, in conjunction with Schedule A1, to one single agreement, namely 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, signed on 3 October 2019 (UK-US Agreement) ([38]). The safeguards provided by that Agreement have been

---

See draft ICO guidance on recognised legitimate interest, as published for public consultation, available at the following link: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

(32) Article 6(1) last subparagraph, as amended by Section 70(2)(c) of the Data (Use and Access) Act.

(33) Before laying Regulations, the Secretary of State must have regard to the effects of any changes on the interests and fundamental rights and freedoms of data subjects, and the fact that children (where relevant) merit specific protection with regard to their personal data. The regulations must be made by statutory instrument and are subject to the affirmative resolution procedure, which means that they must be actively approved by the United Kingdom Parliament. Section 70(4) subparagraph 8 of the Data (Use and Access) Act.

(34) Section 182(2) of the DPA 2018.

(35) Section 70(4) subparagraph 9 of the Data (Use and Access) Act.

(36) See ICO guidance on legitimate interests, available at the following link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy.

(37) Section 72 of the Data (Use and Access) Act.

(38) 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, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

assessed in recitals (153) to (155) of Implementing Decision (EU) 2021/1772 and their implementation is analysed in recitals (87) to (93) of this Decision.

2.2.2. Processing of special categories of personal data

(25) The United Kingdom's data protection framework continues to provide specific safeguards where special categories of data are involved, as assessed in Implementing Decision (EU) recitals (27) to (42) of Implementing Decision (EU) 2021/1772.

(26) Both the definition of special categories of personal data and the specific rules applying to the processing of these categories of data in the UK GDPR and in 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 special categories of data, to tailor the conditions applicable to their use, and to add new definitions, if necessary ([39]). Importantly, it does not allow the Secretary of State to remove or amend existing special categories of data, or to alter the conditions for the processing of these categories ([40]). The newly introduced regulation-making power thus only enables the Government to add new categories of sensitive data and to determine the conditions for the processing of these categories, which is intended to allow the Government to respond to future technological and societal developments where necessary.

(27) 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) 2021/1772.

2.2.3. Purpose limitation

(28) The United Kingdom's regime for the protection of personal data continues to require that data is processed for a specific purpose and subsequently used only insofar as this is not incompatible with the original purpose of the processing, as assessed in recitals (43) to (48) of Implementing Decision (EU) 2021/1772.

(29) First, the Data (Use and Access) Act makes few targeted amendments to the principle of purpose limitation set out in Article 5(1)(b) of the UK GDPR. These amendments clarify the application of this principle without changing the substance. Section 71(1), (2) and (3) of the Data (Use and Access) Act specify that the purpose limitation principle applies where data is collected from the data subject or otherwise, that it only applies where personal data is further processed by or on behalf of the same controller (i.e. that it does not apply where there is a change of controller), and that processing is not lawful by virtue only of being compatible with the purposes for which the personal data was collected.

(30) Second, the Data (Use and Access) Act clarifies the rules on further processing of personal data by regrouping them in the newly added Article 8A to the UK GDPR, which sets out the full regime for the further processing of personal data. Article 8A(2) of the UK GDPR lists the elements to be taken into account when determining whether a new processing purpose is compatible with the original purpose. These elements were previously listed in Article 6(4) of the UK GDPR, which corresponds to Article

[39] 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.

[40] See new Article 11A(1)(b) and (2) of the UK GDPR, as well as Explanatory Notes to the Data (Use and Access) Bill, paragraph 571, available at the following link: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf

6(4) of Regulation (EU) 2016/679 ([41]). Article 8A(3) of the UK GDPR regroups in one provision the situations in which the processing of personal data for a new purpose is to be treated as compatible with the original purpose. It covers situations where the data subject consents to the processing of personal data for the new purpose or where processing is necessary to safeguard an objective listed in Article 23(1) ([42]), where the processing is carried out for the purposes of scientific or historical research, archiving in the public interest or for statistical purposes ([43]). Finally, the Data (Use and Access) Act clarifies that any processing carried out to ensure that processing complies with the data protection principles set out in Article 5(1) of the UK GDPR or demonstrating that it does so is considered compatible with the original purpose. The abovementioned situations continue to correspond to what is considered compatible further processing also in Regulation (EU) 2016/679.

(31) Third, the Data (Use and Access) Act also introduces in Article 8A(3)(d) of the UK GDPR new additional situations in which the further processing of personal data for a new purpose is considered compatible with the original purpose. These situations are listed in Annex 2 to the UK GDPR ([44]) and include, for example, where processing takes place in response to a request received by a public authority who needs the data for the purposes of the performance of a task carried out in the public interest that has a legal basis that satisfies Article 6(3) of the UK GDPR, where processing is necessary to protect public security, to respond to an emergency, to detect, investigate or prevent crime, to protect the vital interests of the data subject and others, to safeguard vulnerable individuals, for tax purposes or if necessary for compliance with a legal obligation ([45]).

(32) While the Data (Use and Access) Act thus extends the list of situations where further processing for a different purpose is considered compatible with the original processing purpose, this extension is subject to important limitations. First, it is limited to specific situations that are listed exhaustively in the law. Second, it only concerns areas where there is a clear public interest in the processing activity, i.e. where the further processing serves objectives listed in Article 23 UK GDPR (which corresponds to Article 23 of Regulation (EU) 2016/679). It can thus not be relied upon for commercial purposes. Third, while the Data (Use and Access) Act grants the Secretary of State the right to amend the list in Annex 2 by means of Regulation ([46]), the Secretary of State may only add types of processing to that list where that processing is again necessary to safeguard a public interest objective listed in Article 23(1)(c) to (j) of the UK GDPR ([47]). Fourth, where the personal data collection by the controller is based on the data subject's consent, processing for a new purpose in the situations listed in Annex 2 is only considered compatible with the original purpose if the

---

([41]) Like in Regulation (EU) 2016/679, these elements include any link between the original and the new purpose, the context in which the personal data was collected, including the relationship between the data subject and the controller, the nature of the processing and whether it includes special categories of data, the possible consequences of the intended processing for the data subject, and the existence of appropriate safeguards.

([42]) See also Article 6(4) of Regulation (EU) 2016/679.

([43]) Recital 50 of Regulation (EU) 2016/679.

([44]) Annex 2 is introduced in the UK GDPR through Schedule 5 of the Data (Use and Access) Act, see Section 71(6) of that Act.

([45]) See Schedule 5 of the Data (Use and Access) Act.

([46]) Article 8A(5) of the UK GDPR, as introduced by Section 71(1) of the Data (Use and Access) Act.

([47]) Article 8A(6) of the UK GDPR, as introduced by Section 71(1) of the Data (Use and Access) Act.

controller cannot reasonably be expected to obtain new consent from the data subject ([48]).

2.2.4. Individual rights

(33) Under the United Kingdom's framework for the protection of personal data, data subjects continue to benefit from the same individual rights as under Regulation (EU) 2016/679 without any significant modifications ([49]) 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 (51) to (54) of Implementing Decision (EU) 2021/1772.

(34) First, the Data (Use and Access) Act clarifies certain modalities under which those rights can be exercised. On the one hand, it specifies through an amendment of Article 12 and the introduction of a new Article 12A of the UK GDPR ([50]) the time limits within which controllers need to respond to data subject's requests. More specifically, Article 12 of the UK GDPR is amended in such a way that the controller is no longer required to provide information on the action taken (or on the reasons for not having taken any action) in response to a data subject request in accordance with Articles 15 to 22 of the UK GDPR "within one month of receipt of the request", but rather "before the end of the applicable time period". The applicable time period is further defined in the newly introduced Article 12A of the UK GDPR as a period of one month beginning with the relevant time, which is the time when the controller receives the request, when the controller receives any information requested in connection with a request under Article 12(6) of the UK GDPR, or when a fee that has been charged in connection with the request under Article 12(5) of the UK GDPR has been paid, whichever is the latest ([51]). Article 12A(3) further allows the controller to extend the applicable time period by two further months where that is necessary because of the complexity of requests made by the data subject, or by the number of such requests. On the other hand, with respect only to the right of access to information and personal data, the Data (Use and Access) Act amends Article 15 of the UK GDPR 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 ([52]). 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*

(48) Article 8A(4)(b) of the UK GDPR, as introduced by section 71(1) of the Data (Use and Access) Act.

(49) Section 31 of the Victims and Prisoners Act 2024 (VAP Act) inserted an additional ground in the right to erasure provided by Article 17 of the UK GDPR, providing data subjects with the right to request that data controllers erase their personal data when it had been processed as a result of an unfounded allegation about the data subject made by a malicious person. A person is considered 'malicious' if they have been convicted of an offence specified in section 31(3) of the VAP Act (such as harassment) or is subject to a stalking protection order. The VAP Act is available at the following link: https://www.legislation.gov.uk/ukpga/2024/21/contents. In addition, Section 77 of the Data (Use and Access) Act amends the right to information as provided by Article 13 of the UK GDPR in such a way that the controller is no longer required to inform the data subject about the further processing of his/her personal data for a new purpose if that purposes is scientific or historical research, archiving in the public interest or a statistical purpose, the processing is carried out in accordance with the specific safeguards set out in new Article 84B of the UK GDPR, and providing the information would be impossible or disproportionate.

(50) Section 76 of the Data (Use and Access) Act.

(51) Article 12A(1) and (2) of the UK GDPR, as introduced by Section 76 of the Data (Use and Access) Act.

(52) Article 15(1A) of the UK GDPR, as introduced by Section 78 of the Data (Use and Access) Act.

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" ([53]).

(35) Therefore, while the time limits for responding to requests from the data subjects and the specific obligations for data controllers with respect to the right of access 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 ([54]).

(36) The restrictions to these individual rights set out in the DPA 2018 and fitting within the framework of Article 23 of the UK GDPR, as well as the limitations and safeguards that frame the application of these restrictions, continue to be in place in the United Kingdom's framework ([55]) as described in detail in recitals (55) to (67) of Implementing Decision (EU) 2021/1772.

(37) With respect specifically to the restriction for personal data processed for the purposes of the maintenance of effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control, to the extent that the application of those provisions would be likely to prejudice any of those matters (the immigration exemption) ([56]), the United Kingdom Government has amended paragraph 4 of Schedule 2 to the DPA 2018 through the Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022 [57], and The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024 [58], which complement the Regulations of 2022 ([59]). The amendments integrate into

---

[53] *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74.

[54] 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/.

[55] Section 88(2) of the Data (Use and Access) Act makes a small modification to section 26(2)(f) of the DPA 2018 (national security and defence exemption), clarifying that the right to lodge a complaint with the Commissioner pursuant to Article 77 of the UK GDPR is not part of the provisions the application of which can be restricted for purposes of national security or defence.

[56] When Implementing Decision (EU) 2021/1772 was adopted, the validity and interpretation of the immigration exemption under United Kingdom law had not been settled, following a decision of the England and Wales Court of Appeal of 26 May 2021 which had found that the immigration exemption, as present in the DPA 2018 at the time, was incompatible with United Kingdom law, as it was lacking specific provisions setting out the safeguards listed in Article 23(2) of the UK GDPR, which reflects Article 23(2) of Regulation (EU) 2016/679. For that reason, personal data transferred for United Kingdom immigration control purposes, or which otherwise fall within the scope of the immigration exemption had been excluded from the scope of Implementing Decision (EU) 2021/1772.

[57] The Regulations entered into force on 31 January 2022 and are available at the following link: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

[58] The Regulations entered into force on 8 March 2024 and are available at the following link: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

[59] The immigration exemption as revised through the 2022 Regulations was challenged again by way of judicial review, on the basis that it did not yet meet all the requirements of Article 23(2) of the UK GDPR. The Court of Appeal in December 2023 found it incompatible with the requirements of Article

Paragraph 4A and 4B of Schedule 2 to the DPA 2018 the safeguards for the exercise of the immigration exemption that are required by Article 23(2) of the UK GDPR. In particular, they require (i) that the immigration exemption must only be invoked on a case by case basis, separately in respect of each of the relevant UK GDPR provisions and afresh on each occasion on which the Secretary of State considers disapplying or restricting the application of any of the relevant UK GDPR provision ([60]), (ii) that the data subject's rights and freedoms and potential vulnerabilities are taken into account when exercising the immigration exemption ([61]), (iii) the Secretary of State to keep a record on the use of the immigration exemption and to inform the data subject about its use (except in specific circumstances where the information would prejudice the objective of the exemption) ([62]), and (iv) clarify that the use of the immigration exemption is restricted to the processing of personal data by the Secretary of State ([63]), that is, in practice, by the Home Office for its functions relevant to paragraph 4(1) of Schedule 2 to the DPA 2018. In addition, they also explain the balancing exercise that must be undertaken when determining whether the exercise of data subject rights is likely to prejudice effective immigration control, and if it is necessary and proportionate to restrict such rights as a result.

(38) Furthermore, the UK ICO has issued detailed guidance on the use of this specific restriction ([64]). The guidance states in particular that "You should not apply the immigration exemption as a blanket exemption to restrict [….] rights for all the data you hold. The scope of the exemption is limited to those rights which, if exercised for the data held, would prejudice the identified immigration purposes. […]. Therefore, the default position of the controller should be to comply with the requirements of Regulation (EU) 2016/679 and the DPA as far as possible. […] The prejudice test has a high threshold, and you should not apply the exemption in a blanket fashion. […] You must consider whether the application of the exemption is a proportionate response to the individual's data protection request. You may consider that there is a pressing social need to apply the immigration exemption, but you must also take into account whether this outweighs your obligation to individuals under Regulation (EU) 2016/679. They have rights over their personal data which you must consider in all circumstances, in particular, the right of access. It is therefore important in every case that you consider whether the data protection rights of the individual override the identified risk of prejudice. Your application of the exemption must be proportionate to the circumstances and you must carefully consider and document each instance."

(39) Overall, the immigration restriction provided in Paragraph 4 of Schedule 2 to the DPA 2018 as revised by the United Kingdom Government in 2022 and 2024 and as

---

23(2) of the UK GDPR. As a result of that judgement, the 2024 Regulations supplement the 2022 Regulations and make further amendments to the immigration exemption.

(60) Paragraph 4A (2) of Schedule 2 to the DPA 2018.

(61) Paragraph 4AB (3) and (4) of Schedule 2 to the DPA 2018. The Information Commissioner's Office was consulted on the draft 2024 Regulations and publicly stated it was content with the regulation. The letter published in response to the consultation and confirming its view is available at the following link: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/.

(62) Paragraph 4B(1) and (2) of Schedule 2 to the DPA 2018.

(63) Paragraph 4(1) of Schedule 2 to the DPA 2018.

(64) Available at the following link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/.

interpreted by the case law([65]) and the ICO's guidance, is subject to a number of strict conditions that frame its application and are very similar to the conditions set in Union law, notably Article 23 of Regulation (EU) 2016/679, for the restriction of data protection rights and obligations for important public interest objectives, such as the control of immigration.

2.2.5. Restrictions on onward transfers

(40) The level of protection afforded to personal data transferred from the European Union to controllers or processors in the United Kingdom continues not to be undermined by the further transfer of such data to recipients in a third country. The regime on international transfers of personal data from the United Kingdom remains very close to the rules set out in Chapter V of Regulation (EU) 2016/679, as assessed in recitals (74) to (82) of Implementing Decision (EU) 2021/1772.

(41) While the Data (Use and Access) Act amended Chapter 5 of the UK GDPR on transfers of personal data to third countries or international organisations, it retains the core requirement that personal data may only be transferred to a third country or international organisation where the transfer is based on (i) regulations approving the transfer (new terminology for what was previously referred to as "adequacy regulations"), (ii) appropriate safeguards, or (iii) a derogation for specific situations. These general principles for data transfers are reflected in the new Article 44A, replacing Article 44 of the UK GDPR ([66]), 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 the UK GDPR.

(42) With respect specifically to the regulations approving a transfer, Article 45A(2) of the UK GDPR 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, introduced in Article 45A(3) of the UK GDPR, for the Secretary of State 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 legal standard for the data protection test to be met is set out in the new Article 45B(1) of the UK GDPR, which requires 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. Article 45B(2) of the UK GDPR provides for a non-exhaustive 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 Article 45 of the UK GDPR, the new Article 45B(2) retains the core elements of that list and therefore remains close to what is provided in Chapter V of Regulation (EU) 2016/679. Moreover, the United Kingdom authorities have confirmed that the Secretary of State will take into account elements not listed in Article 45B(2), such as

([65]) *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), paragraphs 40 and 41.

([66]) Section 85 and Schedule 7 to the Data (Use and Access) Act.

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 that relevant case law in the third country will be an essential component when considering the matters listed non-exhaustively in Article 45B(2) of the UK GDPR.

(43) 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 2021/1772. Under this procedure, the Secretary of State must consult the Information Commissioner when proposing to adopt UK adequacy regulations ([67]). 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 ([68]).

(44) With respect to appropriate safeguards, the new paragraph Article 46 (1A) of the UK GDPR sets out that such transfers may only proceed if relevant safeguards are provided in the instruments available pursuant to Article 46(2) and (3) ([69]) of the UK GDPR and the controller, processor, or applicable public bodies, acting reasonably and proportionately, consider that the data protection test is met. Newly inserted paragraphs 6 and 7 clarify 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, i.e. as it is the case under Regulation (EU) 2016/679, the same legal standards apply to both regulations approving a transfer and appropriate safeguards. According to the same paragraph, 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.

(45) Concerning derogations for specific situations, in Article 49 of the UK GDPR, on the conditions under which derogations for specific situations may be applied, a number of technical amendments are introduced which align the provision with changes in other provisions, but do not affect the level of protection for personal data in the United Kingdom. In addition, a new paragraph 4A is inserted to reproduce the effect of section 18(1) of the DPA 2018 which grants the Secretary of State the authority to specify, by regulations, the circumstances for data transfers deemed necessary for public interest reasons. Finally, a new Article 49A reproduces the effect of section 18(2) of the DPA 2018 which enables the Secretary of State, through regulations, to impose restrictions on data transfers where these are not approved under Article 45A

---

(67) 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.

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

(69) The transfer instrument available pursuant to Article 46(2) and (3) of the UK GDPR are legally binding and enforceable instruments between public authorities or bodies, binding corporate rules in accordance with Article 47 of the UK GDPR, standard data protection clauses specified in regulations made by the Secretary of State or specified in a document issued by Information Commission, an approved code of conduct and an approved certification mechanism.

(transfers approved by regulations) and when deemed necessary for important public interest reasons.

(46) In terms of implementation of the United Kingdom's international transfer rules, there have been several developments since the adoption of Implementing Decision (EU) 2021/1772.

(47) With respect to regulations approving transfers, two new regulations have been adopted so far, mirroring adequacy decisions that are in place also within the Union, i.e. for transfers to the Republic of Korea and for transfers to commercial entities that have adhered to the United Kingdom Extension to the EU-U.S. Data Privacy Framework. The adequacy regulations for the Republic of Korea ([70]) entered into force on 19 December 2022 and allow the transfer of personal data from the United Kingdom to the Republic of Korea. The United Kingdom Extension to the EU-U.S. Data Privacy Framework, for which the relevant regulations ([71]) entered into force on 12 October 2023, allows for the free flow of personal data to certified U.S. organisations.

(48) With respect to appropriate safeguards, the United Kingdom has published its own standard data protection contractual clauses, the International Data Transfer Agreement (IDTA) ([72]), and an Addendum to the EU Standard Contractual Clauses (SCCs), both of which came into effect in March 2022. The IDTA provides a mechanism specific for the United Kingdom for ensuring appropriate safeguards for the transfer of personal data and shares various similarities with the EU SCCs. The Addendum, issued by the ICO, enables data controllers and processors in the United Kingdom to rely on EU SCCs under the UK GDPR for international transfers. The ICO has also issued a Transfer Risk Assessment Tool to support UK organisations in evaluating the risks associated with international transfers.

(49) The United Kingdom has also streamlined the approval process for Binding Corporate Rules (BCRs) through new guidance and new options to approve BCRs. In July 2022, the ICO published guidance and referential tables to explain the United Kingdom's approach to BCRs post-Brexit, and, in December 2023, an Addendum to EU BCRs was published to ensure that BCRs approved under the Union framework are enforceable in the United Kingdom ([73]).

(50) Finally, in July 2023, the United Kingdom became an associate member of the Global Cross-Border Privacy Rules (CBPR) Forum ([74]). Importantly, this membership does not entail any facilitation of data transfers from the United Kingdom to other members of the CBPR Forum. The United Kingdom has clarified that any transfer of personal data from the United Kingdom to third countries or international organisations needs to meet the conditions set out in United Kingdom legislation, as described above, in

---

([70]) Available at the following link: https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) Available at the following link: https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) Available at the following link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/

([73]) The ICO received a significant number of UK BCR applications post-Brexit. Many approved BCRs could no longer be used, as only BCRs where the ICO had been involved with the BCR approval process could continue to be used post-Brexit but those BCR holders were required to submit to the ICO updated UK GDPR compliant BCR documentation.

([74]) The CBPR Forum consists of the United States of America, Canada, Japan, the Republic of Korea, the Philippines, Singapore, Taiwan and Australia, while Mauritius, the Dubai International Financial Centre and Bermuda are associate members like the United Kingdom.

particular the data protection test, which requires the standards of protection afforded to be "not materially lower" than those under the UK GDPR.

(51) As the Commission has already explained, CBPRs do not ensure a sufficient level of protection for personal data originating from the EU. In particular, they do not provide for enforceable individual rights ([75]). It is therefore particularly important that, even if the United Kingdom is an associate member to the Global CBPR Forum, CBPR cannot constitute a valid transfer mechanism under United Kingdom data protection law. If that were to change, this would undermine the level of protection currently guaranteed to personal data transferred from the EU to the United Kingdom. Therefore, the Commission will continue to closely monitor further developments in this regard.

2.2.6. Automated decision-making

(52) While keeping several elements of the rules on automated decision-making assessed in recital 54 of Implementing Decision (EU) 2021/1772, the Data (Use and Access) Act has amended some aspects of these rules.

(53) First, the newly introduced Article 22B of the UK GDPR establishes a general prohibition on the processing of special categories of personal data (defined by Article 9(1) of UK GDPR) for decisions based solely on automated processing that have legal or similarly significant effects for the data subject. However, it outlines three exceptions to this prohibition: the data subject has provided explicit consent for such processing; or the decision is necessary for entering into, or the performance of, a contract between the controller and the data subject; or the processing is required or authorised by law. For the last two exceptions, the automated processing must be necessary for reasons of substantial public interest ([76]). The general prohibition does not apply to significant decisions based on automated processing of non-special categories of data.

(54) In addition, the new Article 22A of the UK GDPR 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. Article 22A of the UK GDPR also clarifies that a "significant decision" is one that produces legal effects or similarly significant impacts on a data subject ([77]).

---

(75) See for instance, the comparative analysis conducted by the G7 Data Protection Authorities on the core elements of the GDPR certifications scheme and the CBPR system, which showed 'notable differences' between the systems including on 'enforceability and legal redress, rules regarding independent oversight and government access). Available at the following link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165
See recital (79) of Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC.
See also Article 29 Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents, 6 March 2014.

(76) Article 22B of the UK GDPR, as introduced by section 80(1) of the Data (Use and Access) Act.

(77) Article 22A of the UK GDPR, as introduced by section 80(1) of the Data (Use and Access) Act.

(55) Second, the newly introduced Article 22C of the UK GDPR mandates that controllers implement measures to provide the relevant safeguards for any significant decision based entirely or partly on personal data and based solely on automated processing (including of non-special categories of personal data). These safeguards must include providing information to the data subject about the decision-making process, allowing the data subject to contest the decision and make representations, and ensuring the data subject can obtain human intervention in the decision-making process ([78]).

(56) Finally, the newly introduced Article 22D of the UK GDPR grants the Secretary of State the authority to make secondary legislation to describe what constitutes, and what does not constitute, meaningful human involvement, and what decision is, and is not, to be considered as having a similarly significant effects 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 ([79]). Importantly, before adopting regulations in accordance with Article 22D of the UK GDPR, the Secretary of State must consult the ICO ([80]), regulations may not amend Article 22C of the UK GDPR ([81]), and regulations are subject to the affirmative resolution procedure ([82]), which means they must be approved by both Houses of the UK Parliament before they can be enacted.

(57) While the Data (Use and Access) Act has thus modified the framework for automated decision-making, it is important to note that under United Kingdom legal framework automated decision-making continues to be subject to the key safeguards requiring the right to obtain human intervention in all cases of significant decisions based solely on automated processing, i.e. on the basis of the processing of sensitive and non-sensitive personal data ([83]). In addition, as the Commission has noted in previous adequacy decisions ([84]), the specific rules on automated decision-making in the UK GDPR are unlikely to affect the level of protection for personal data transferred from the Union to the United Kingdom. As regards personal data that has been collected in the Union, any decision based on automated processing will typically be taken by the controller in the Union (which has a direct relationship with the concerned data subject) and is thus subject to the rules of Regulation (EU) 2016/679.

2.3. Oversight and enforcement

2.3.1. Independent Oversight

(58) 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

(78) Article 22C of the UK GDPR, as introduced by section 80(1) of the Data (Use and Access) Act.

(79) Article 22D of the UK GDPR, as introduced by section 80(1) 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 Article 22C.

(80) Section 182(2) of the DPA 2018.

(81) Article 22D(4) of the UK GDPR.

(82) Article 22D(5) of the UK GDPR.

(83) Article 22C(2) of the UK GDPR, as introduced by section 80(1) of the Data (Use and Access) Act.

(84) See for example recital (94) of Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information and recital (81) of Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act.

supervisory authority, as analysed in recitals (85) to (91) of Implementing Decision (EU) 2021/1772. 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.

(59) 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 ([85]). The Act also makes provisions for the Information Commissioner to transition to the role of Chair of the Information Commission, who is one of the non-executive members ([86]). 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 ([87]), 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 ([88]).

(60) 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 (87) to (90) of Implementing Decision (EU) 2021/1772 ([89]). 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 ([90]). 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 ([91]). The executive members are employees of the Information Commission employed on terms and conditions as determined by the non-executive members ([92]). The Chief Executive is appointed by the Chair and other non-executive members, following consultations with the Secretary of State. The executive members' appointments are also subject to a selection on merit on the basis of a fair and open competition ([93]).

(61) 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

---

(85) Paragraph 3(1) of Schedule 12A to the DPA 2018.

(86) Sections 117, 118, 119 and 120 together with Schedule 14 of the Data (Use and Access).

(87) Paragraphs 13 and 14 of Schedule 12A to the DPA 2018.

(88) Paragraph 16 of Schedule 12A to the DPA 2018.

(89) Article 52 of the UK GDPR, as well as Schedule 12A of the DPA 2018, as introduced by section 114A of the Data (Use and Access) Bill.

(90) Paragraphs 5(1) and 3(2) of Schedule 12A to the DPA 2018.

(91) Paragraphs 3(2), 5 and 6 of Schedule 12A to the DPA 2018.

(92) Paragraph 11 of Schedule 12A to the DPA 2018.

(93) Paragraphs 5(2) of Schedule 12A to the DPA 2018.

requirements with respect to potential conflicts of interest, or is unable, unfit or unwilling to carry out the Chair's functions ([94]). 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 ([95]).

(62) The main role of the Information Commission will continue to be the monitoring and enforcement of the data protection framework in the United Kingdom "in order to protect the fundamental rights and freedoms" of individuals ([96]). With respect to the Information Commission's function to secure an appropriate level of protection for personal data, the Data (Use and Access) Act specifically requires that the Information Commission will have regard to the interests of data subjects, controllers and others, to matters of general public interest, and to promote public trust and confidence in the processing of personal data ([97]). These objectives are also mentioned in recital 7 of Regulation (EU) 2016/679.

(63) In addition, the Data (Use and Access) Act specifies that the Information Commission shall consider 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 ([98]).EU data protection law also recognises the need to balance the protection of personal data with several other fundamental rights and objectives, such as economic and social progress, security and justice, and the freedom to conduct a business ([99]).

2.3.2. Enforcement, including sanctions

(64) 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 Regulation (EU) 2016/679 ([100]), as assessed in recitals (91) to (95) of Implementing Decision (EU) 2021/1772.

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

(66) On the one hand, the Data (Use and Access) Act clarifies that the Commission can require specific 'documents' and 'information' when using the information notice power ([101]). On the other hand, the Data (Use and Access) Act introduces two new

---

(94) Paragraph 7(6) and (7) of Schedule 12A to the DPA 2018.

(95) Paragraph 9(6), (7), (8) and (9) of Schedule 12A to the DPA 2018.

(96) Article 51 of the UK GDPR.

(97) Section 91 of the Data (Use and Access) Act, introducing Section 120A of the DPA 2018.

(98) Section 91 of the Data (Use and Access) Act, introducing Section 120B of the DPA 2018**.** The Data (Use and Access) Act further introduces a new section 120C in the DPA 2018 which requires the Information Commission to prepare and publish a strategy that, among others, reflects the way in which it will consider the abovementioned issues and the promotion of economic growth when exercising its regulatory functions.

(99) See in particular recitals 2 and 4 as well as Article 23 of Regulation (EU) 2016/679.

(100) Articles 57 and 58 of the UK GDPR.

(101) Section 97 of the Data (Use and Access) Act amending Section 142 of the DPA 2018. The considerations on the impact of technology and the role of data protection in creating trust in the digital

investigatory powers for the Information Commission: a new power to require a report ([102]) and a new power to issue 'interview notices' to controllers in case of suspected infringement of the UK GDPR or the DPA 2018 ([103]).

(67) With regard to the exercise of these powers by the Information Commission, since the entry into force of Implementing Decision (EU) 2021/1772, the Information Commissioner has handled about 40 000 complaints from data subjects per year, which is similar to the amount of complaints handled when the United Kingdom was still part of the Union and applying Regulation (EU) 2016/679 ([104]). The ICO also conducted ex officio investigations covering a broad range of sector and compliance issues, including data subjects' rights ([105]).

(68) In terms of enforcement measures, since the entry into force of the Implementing Decision (EU) 2021/1772, the Commissioner issued 120 reprimands, 32 information notices, 3 assessment notices, 12 enforcement notices, 2 warnings, and 12 fines ([106]). This includes several significant monetary penalties imposed under the UK GDPR and the DPA 2018. For example, the Information Commissioner issued in April 2023 a £12.7 million fine to a social media platform for misusing children's data ([107]). In March 2025, a software company was fined £3.07 million for security failings that put the personal information of more than 70,000 people at risk ([108]). Very recently, in June 2025, the Information Commissioner fined a genetic testing company £2.31 million for failing to implement appropriate security measures to protect the personal information of UK users, following a large-scale cyber-attack in 2023 ([109]).

(69) Since the adoption of Implementing Decision (EU) 2021/1772, the Information Commissioner's Office has also developed and published a significant number of guidelines, opinions and other guidance documents, which clarify the application of data protection rules in important areas, such as facial recognition, fairness in artificial intelligence, children's data, direct marketing, video surveillance, the right of access, transparency in health and social care etc., for different audiences, including small and medium-sized enterprises, specific entities like schools, nurseries or small public authorities, as well as for businesses in general, the general public or data subjects ([110]).

---

economy is part of the activities of data protection regulators both in the UK and in the EU. See for instance, European Data Protection Board annual report 2024, page 12: "The EDPB is a dynamic and collaborative body that plays a pivotal role in ensuring the consistent application of data protection laws across Europe. From my perspective as Deputy Chair, I see it as a guardian of individuals' privacy rights, skilfully balancing the needs of innovation and economic growth."

(102) Section 98 of the Data (Use and Access) Act amending Section 146 of the DPA 2018.

(103) Section 100 of the Data (Use and Access) Act introducing Section 148A of the DPA 2018.

(104) Information Commissioner's Annual Reports from 2021-2022, 2022-2023, and 2023-2024. See also Commission Implementing Decision (EU) 2021/1772, recital 96.

(105) Information Commissioner's Annual Report from 2023-2024, page 41.

(106) Information Commissioner's Annual Reports from 2021-2022, 2022-2023, and 2023-2024.

(107) For more information on these and more enforcement actions, see the ICO website, available at the following link: https://ico.org.uk/action-weve-taken/enforcement/

(108) More information is available at the following link: https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.

(109) More information is available at the following link: https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.

(110) Available at the following link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

3. RELEVANT DEVELOPMENTS REGARDING ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE UNITED KINGDOM

3.1. General legal framework

(70) The United Kingdom continues to be a member of the Council of Europe, to adhere to the European Convention of Human Rights, and to be submitted to the jurisdiction of the European Court of Human Rights. It therefore continues to be subject to the obligations enshrined in international law as described in recitals (116) to (119) of Implementing Decision (EU) 2021/1772, which frame its system of government access to personal data on the basis of principles, safeguards and individual rights identical to those that apply to the 27 Member States as party to the ECHR and that are, to a large extent, reflected in the relevant case law of the Court of Justice of the European Union.

(71) Specific data protection safeguards and rights continue to be guaranteed by the DPA 2018 when data is processed by the United Kingdom's public authorities, including by law enforcement and national security bodies, as analysed in recitals (121) to (132) of Implementing Decision (EU) 2021/1772. The Data (Use and Access) Act has made only limited and targeted amendments to those parts of the DPA 2018 that provide the rules for the processing of personal data in the context of criminal law enforcement (Part 3 of the DPA 2018) and national security (Part 4 of the DPA 2018).

(72) With respect 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, including the safeguarding against and the prevention of threats to public security, Part 3 of the DPA 2018 continues to provide for principles, rights and obligations similar to those set out by Directive (EU) 2016/680 ([111]).

(73) In particular, at the same date as this Decision, the Commission has adopted a Decision on the basis of Article 36(3) of Directive (EU) 2016/680, finding that the data protection regime applicable to processing by United Kingdom criminal law enforcement authorities for purposes of criminal law enforcement continues to ensure a level of protection essentially equivalent to the one guaranteed by Directive (EU) 2016/680.

(74) 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

([111]) Section 69 of the Data (Use and Access) Act inserts the definition of consent and the conditions for relying on consent as provided for by Article 4(11) and Article 7 of the UK GDPR (which mirror the corresponding provisions in Regulation (EU) 2016/679) as new sections 33(1A) and 40A into the DPA 2018, thus clarifying the concept of consent and the conditions for reliance on consent when used as a legal basis for the processing of personal data by competent authorities for the purposes of criminal law enforcement. In addition, section 71(7) and (8) of the Data (Use and Access) Act slightly clarifies the wording of section 36(1) of the DPA 2018. Finally, where relevant, amendments to the UK GDPR by the Data (Use and Access) Act as described in Section 2 are also reflected in Part 3 of the DPA 2018, see for instance section 74(2)-(5) on sensitive processing, section 76(4)-(6) with respect to the time limits for responding to data subject's requests, section 78(2) and (3) with respect to searches in response to data subjects' requests, and section 80(3)-(5) on automated decision-making.

required for the purposes of safeguarding national security [112]. 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).

(75) 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 [113]. 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 [114]. This is also confirmed in the ICO's guidance on the application of national security exemptions [115].

(76) Moreover, on the basis of the amendments introduced by the Data (Use and Access) Act ([116]), a specific processing activity by authorities competent for criminal law enforcement can also be governed by the provisions of part 4 of the DPA 2018, which normally applies only to the processing of data by national security authorities.

(77) While the data protection regime for national security processing is thus in certain situations extended also to data processing by criminal law enforcement authorities, this is the case only in specific circumstances and subject to strict conditions and safeguards, i.e. if (i) a competent authority is specified as "qualifying competent authority" in regulations made by the Secretary of State which require parliamentary approval ([117]), and (ii) the Secretary of State designates by way of notice a specific processing activity carried out by the qualifying competent authority. Importantly, such designation can only take place if the Secretary of State considers that the designation of the processing activity is required for the purposes of safeguarding national security, i.e. where a criminal law enforcement authority acts for national security purposes, and the processing activity is carried out by the qualifying competent authority as a joint controller with at least one intelligence service ([118]). As

---

(112) 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.

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

(114) 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.

(115) See ICO's guidance on the national security and defence exception, available at the following link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

(116) Sections 89 to 90 of the Data (Use and Access) Act.

(117) Section 82(A1), (2A) and (4) of the DPA 2018, as introduced by section 89(2) of the Data (Use and Access) Act.

(118) Section 82A(1) and (2), as introduced by section 89(3) of the Data (Use and Access) Act. As further safeguards, the Secretary of State must consult the Commissioner before giving a designation notice, see new section 82A(8) of the DPA 2018, the text of the notice must in principle be published, see new

further safeguards, the Secretary of State must consult the Commissioner before giving a designation notice ([119]), the text of the notice must in principle be published ([120]), and a person directly affected by a designation notice may request judicial review ([121]). Therefore, this amendment aims essentially at clarifying that when United Kingdom authorities have competences in the area of both law enforcement and national security and process data in the context of their latter responsibilities, the data protection regime for national security services may apply.

(78) Part 4 of the DPA 2018 regulates the data processing by United Kingdom intelligence services. It continues to set out the main data protection principles, to impose conditions on the processing of special categories of data, to provide for data subject rights, to require data protection by design, and to regulate transfers of personal data, as described in recitals (125) to (132) of Implementing Decision (EU) 2021/1772.

(79) The amendments to this regime introduced by the Data (Use and Access) Act are limited. With respect to the data subjects' right of access provided in section 94 of the DPA 2018, the Data (Use and Access) Act introduces a new subsection (2A), clarifying that the data subject is only entitled to the relevant information as far as the controller is able to provide it based on a reasonable and proportionate search ([122]). As explained in recital (35), this amendment frames the right of access on the basis of established legal standards, which take into account also the interests of the data subject. While in the area of automated decision-making, controllers continue to be prohibited from taking a decision significantly affecting a data subject that is based entirely on automated processing of personal data relating to the data subject, unless such decision is required or authorised by law, the data subject has given consent to the decision being made on that basis, or the decision is taken in the context of a contract ([123]); the Data (Use and Access) Act introduces in Part 4 of the DPA 2018 ([124]) the same definition of the notion of "decisions based entirely on automated processing" as included in Article 22A of the UK GDPR and analysed in recital (53) of this Decision.

3.2. Relevant developments regarding access and use by United Kingdom public authorities for criminal law enforcement purposes

(80) The law of the United Kingdom continues to impose important limitations on the access and use of personal data for criminal law enforcement purposes, and provides oversight and redress mechanisms in this area, as analysed in recitals (134) to (174) of Implementing Decision (EU) 2021/1772.

3.2.1. Legal bases and applicable limitations/safeguards

(81) The collection of personal data from business operators in the United Kingdom for purposes of criminal law enforcement continues to be permissible in the United

---

section 82D(1), subject to the exemptions set out in new section 82D(3) of the DPA 2018, and a person directly affected by a designation notice may request judicial review, see new section 82E of the DPA 2018.

([119]) Section 82A(8) of the DPA 2018

([120]) Section 82D(1), subject to the exemptions set out in new section 82D(3), of the DPA 2018.

([121]) Section 82E of the DPA 2018.

([122]) Section 78(4) of the Data (Use and Access) Act.

([123]) Section 96 of the DPA 2018.

([124]) Pursuant to new section 96(4) of the DPA 2018, a decision is based on entirely automated processing if the decision-making process does not include an opportunity for a human being to accept, reject or influence the decision. See section 80(4)(c) of the Data (Use and Access) Act.

Kingdom legal order on the basis of search warrants and productions orders, subject to the conditions and safeguards described in recitals (135) to (138) of Implementing Decision (EU) 2021/1772.

(82) In addition, the National Security Act 2023 ([125]), which aims at addressing threats to national security through espionage, sabotage and persons acting for foreign powers, has introduced new powers of entry, search and seizure for the United Kingdom police, including the possibility to obtain personal data, where there are reasonable grounds for suspecting that material will be obtained which is likely to be evidence that one of the more serious offences or foreign power threat activities under the National Security Act 2023 has been or is about to be committed ([126]). These powers are subject to similar conditions and safeguards to those analysed in Implementing Decision (EU) 2021/1772 for the powers existing at the time. In particular, their use must be authorised by means of a warrant, production order or explanation order issued by an independent judicial authority, on application of the constable/investigating officer ([127]). Specific protections exist for confidential material, such as journalistic material and items subject to legal privilege ([128]). Similarly, the issuing of disclosure orders ([129]), customer information orders ([130]) and account monitoring orders ([131]) also created by the National Security Act 2023, must be authorized by a judge on application by an appropriate officer, and is subject to specific conditions and safeguards, including that the order is sought with respect to a specific person, for the purposes of an investigation into foreign power threat activity, that the order will enhance the effectiveness of the investigation, and that it is not used to obtain information that is legally privileged or otherwise excluded, such as journalistic material and certain health records ([132]).

(83) As described in recitals (139) to (141) of Implementing Decision (EU) 2021/1772, in the United Kingdom legal framework specific law enforcement authorities, for example the National Crime Agency or the Metropolitan Police Service can also use targeted investigatory powers under the Investigatory Powers Act 2016 (IPA 2016)

---

(125) Available at the following link: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

(126) Schedule 2 to the National Security Act 2023. Relevant offenses under the National Security Act 2023 are for example obtaining or disclosing protected information (section 1), obtaining or disclosing trade secrets (section 3), assisting a foreign intelligence service (section 4), carrying out sabotage (section 12), or carrying out specific prohibited conduct for a foreign power with the intention to create an interfering effect (section 13).

(127) See paragraphs 2(1), 3(1), 4(1) and 10(1) of Schedule 2 to the National Security Act 2023.

(128) See paragraphs 2(4)(b), 3(4)5(b) and (c), 4(4)(b) and (c), and 10(1) of Schedule 2 to the National Security Act 2023.

(129) Through disclosure orders under Schedule 3 to the National Security Act 2023, an officer may give notice to a person compelling them to provide information, produce documents, and/or answer questions relevant to an investigation to identify property related to foreign power threat activity, including the property's movement or use.

(130) Through customer information orders under Schedule 4 to the National Security Act 2023, an officer may give notice to a financial institution to require that it provides any customer information relating to a specified person.

(131) Through account monitoring orders under Schedule 5, a financial institution may be required to provide information specified in the order to an officer for the period and in the manner specified in the order, which may not exceed 90 days.

(132) Schedule 3 paragraph 2(1), Schedule 4 paragraph 1, Schedule 5 paragraph 1 to the National Security Act 2023.

([133]) for the purposes of preventing or detecting serious crimes. The specific investigatory powers that those law enforcement authorities can rely upon are targeted interceptions (Part 2 of the IPA 2016), acquisition of communications data (Part 3 of the IPA 2016), and targeted equipment interference (Part 5 of the IPA 2016). Where retention notices are given by the Secretary of State under Part 4 of the IPA 2016, law enforcement can also benefit by accessing the retained communications data through communications data acquisition powers under Part 3 of the IPA 2016.

(84) Since the adoption of Implementing Decision (EU) 2021/1772, the IPA 2016, together with the Regulation of Investigatory Powers Act 2000 (RIPA) for England, Wales and Northern Ireland and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) for Scotland, continues to provide for the legal basis and to set out the applicable limitations and safeguards for the use of such powers, as described in Implementing Decision (EU) 2021/1772. Importantly, the legal framework continues to require that in order to exercise these powers, the authorities need to obtain a warrant ([134]) issued by a competent authority ([135]) and approved by an independent Judicial Commissioner ([136]) (so-called "double-lock" procedure). The obtaining of such a warrant continues to be subject to a necessity and proportionality test ([137]).

(85) At the same time, since the adoption of Implementing Decision (EU) 2021/1772, the Investigatory Powers (Amendment) Act 2024, which received Royal Assent in April 2024, amended certain specific elements of the IPA 2016 ([138]). To the extent these amendments and other relevant developments relate to the conditions, limitations and safeguards around the use of the abovementioned specific investigatory powers by public authorities in the United Kingdom for criminal law enforcement purposes, as assessed in recitals (177) to (215) of Implementing Decision (EU) 2021/1772, they are analysed in the following paragraphs. With respect to elements of the United Kingdom's framework that have not been amended by the abovementioned Act or affected by other relevant developments, the analysis carried out in Implementing Decision (EU) 2021/1772 continues to be valid.

([133]) The Investigatory Powers Act 2016 (see: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) replaced a different laws concerning the interception of communications, equipment interference and the acquisition of communication data, in particular Part I of the RIPA 2000 that provided the previous general legislative framework for the use of investigatory powers by law enforcement and national security authorities.

([134]) Chapter 2 of Part 2 of the IPA 2016 provides for a limited number of cases where interceptions can be performed without a warrant. This includes: interception with the consent of the sender or the recipient, interception for administrative or enforcement purposes, interception taking place in certain institutions (prisons, psychiatric hospitals and immigration detention facilities) as well as interception carried out in accordance with a relevant international agreement.

([135]) In most of the cases, the Secretary of State is the authority that issues the warrants under the IPA 2016, while Scottish Ministers are empowered to issue targeted interception warrants, mutual assistance warrant and targeted equipment interference warrants when the persons or premises to be intercepted and the equipment to be interfered are located in Scotland (see Sections 22 and 103 of the IPA 2016). In case of targeted equipment interference, a law enforcement chief (described in Part 1 and Part 2 of Schedule 6 to the IPA 2016) can issue the warrant under the conditions of Section 106 of the IPA 2016.

([136]) Judicial Commissioners assist the Investigatory Powers Commissioner (IPC), an independent body which exercises oversight functions over the use of investigative powers by intelligence agencies.

([137]) See in particular Section 19 and 23 of the IPA 2016.

([138]) Available at the following link: https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

(86) Concerning the targeted acquisition and retention of communications data ([139]), the conditions and safeguards governing these powers, as assessed in Implementing Decision (EU) 2021/1772, remain in place. Investigatory Powers (Amendment) Act 2024 clarified the existing safeguards by introducing into section 11 of the IPA 2016 (which creates an offence for unlawfully obtaining communications data from a telecommunications operator) a list of examples of what is understood as being covered by "lawful authority" in that provision ([140]). In addition, the Investigatory Powers (Amendment) Act 2024 further clarified the definition of communications data in section 261 of the IPA 2016 by explicitly specifying that subscriber details qualify as communications data ([141]).

(87) The issuing of notices requiring the retention of communications data ([142]) continues to be subject to limitations and safeguards, as described in recitals (208) and (209) of Implementing Decision (EU) 2021/1772, in particular requirements of necessity and proportionality and approval by an independent Judicial Commissioner. While the Investigatory Powers (Amendment) Act 2024 introduced the possibility to renew such notices, any renewal is subject to the same conditions of necessity and proportionality and approval by the Judicial Commissioner ([143]).

(88) With respect to communications data, the Investigatory Powers (Amendment) Act 2024 also amended the definition of a telecommunications operator, i.e. the possible addressees of a retention notice. This 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" ([144]). Importantly, the amended definition continues to always require a close link with the United Kingdom market. The amendment thus clarifies that large companies with complex corporate structures are covered in their totality by the IPA 2016 without

---

(139) The term "communications data" covers the "who", "when", "where" and "how" of a communication, but not the content, i.e. what was said or written. Communications data could include the time and duration of communication, the number or email address of the originator and recipient and sometimes the location of the devices from which the telecommunication was made, see section 261(5) of the IPA 2016 The IPA 2016 permits the Secretary of State to require telecommunications operators to retain communications data for the purpose of targeted access by a range of public authorities, including law enforcement and intelligence agencies. Part 4 of the IPA 2016 provides for the retention of communications data, while Part 3 provides for targeted acquisition of communications data. Part 3 and Part 4 of the IPA 2016 also set out specific limitations on the use of these powers and provide for specific safeguards.

(140) For example, where the relevant person obtains the communications data in the exercise of a statutory power of the relevant public authority or where the communications data is obtained in accordance with a court order or other judicial authorisation. Section 11(3A) of the IPA 2016, as introduced by section 12(3) of the Investigatory Powers (Amendment) Act 2024.

(141) Section 261(5A) and (5B), as introduced by section 13(3) of the Investigatory Powers (Amendment) Act 2024.

(142) The issuance of such retention notices pursuant to sections 87 to 89 of the IPA 2016 aims at securing that telecommunication operators retain, for a maximum period of 12 months, relevant communications data that would otherwise be deleted once no longer required for business purpose. The data retained are to remain available for the period required should it subsequently be necessary for a public authority to acquire it under an authorisation for a targeted acquisition of communication data provided by Part 3 of the IPA 2016.

(143) Section 94A of the IPA 2016, as introduced by section 20(4) of the Investigatory Powers (Amendment) Act 2024.

(144) Section 261(10)(c) of the IPA 2016, as introduced by section 19 of the Investigatory Powers (Amendment) Act 2024.

extending the scope of the definition to the providers of telecommunication services not directed at persons in the United Kingdom. . This is also confirmed by the Explanatory Notes on the Investigatory Powers (Amendment) Act 2024, which set out that the amendment is not intended to bring additional companies within the scope of the relevant powers under the IPA 2016 ([145]) but has essentially a clarification function.

(89) Finally, the Investigatory Powers (Amendment) Act 2024 introduced some targeted modifications to the procedure for the issuing of warrants, including with respect to targeted interception and targeted equipment interference, i.e. powers which can also be used by specific law enforcement authorities in the United Kingdom for purposes of preventing or detecting serious crimes. The modifications concern only the specific situation where these powers are used to obtain communications of, or private information about a person who is Member of a relevant legislature ([146]). While warrants in relation to targeted interception and equipment interference can normally be issued by the Secretary of State and are approved by a Judicial Commissioner (see recitals (186) to (196) and (210) to (215) of Implementing Decision (EU) 2021/1772), sections 26 and 111 of the IPA require in addition approval by the Prime Minister when the warrant concerns a Member of Parliament or another relevant legislature (so-called "triple-lock" procedure). The Investigatory Powers (Amendment) Act 2024 now allows the Prime Minister to nominate five Secretaries of State who will be empowered to exercise the Prime Minister's power to authorise these warrants, provided that the need for authorisation is urgent and the Prime Minister is unable to authorise it because of medical incapacity or lack of access to secure communications. Importantly, the limitations and safeguards with respect to the issuing of these warrants, as described in the abovementioned recitals of Implementing Decision 2021/1772, remain in place.

3.2.2. Further use of the information collected

(90) The sharing of data by a law enforcement authority with a different authority for purposes other than the ones for which it was originally collected (so-called "onward sharing"), continues to be subject to the conditions analysed in recitals (142) to (156) of Implementing Decision (EU) 2021/1772.

(91) As regards the specific situation of onward transfers from the United Kingdom to the United States, 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 (the UK-US Agreement) ([147]), which was concluded in October 2019, has entered into force and been implemented since October 2022. Under the UK-US Agreement, data transferred from the EU to service providers in the United Kingdom could be subject

(145) Explanatory Notes on the Investigatory Powers (Amendment) Act 2024, paragraph 359, available at the following link: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

(146) See sections 26 and 111 of the IPA 2016.

(147) 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, available at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

to orders for the production of evidence issued by competent US law enforcement authorities and made applicable in the United Kingdom.

(92) Importantly, the conditions and safeguards under which such orders can be issued and executed, as assessed in recital (154) of Implementing Decision (EU) 2021/1772, continue to apply. In particular, data obtained under the Agreement benefits from equivalent protections to the specific safeguards provided by the so-called "EU-US Umbrella Agreement" ([148]) which are all incorporated into the UK-US Agreement by reference on a *mutatis mutandis* basis ([149]).

(93) Since the adoption of Implementing Decision (EU) 2021/1772, the United Kingdom has explained that it has clarified, including via engagement with the relevant parties in the context of the implementation of the UK-US Agreement, how the specific safeguards of the Umbrella Agreement that were designed for a law enforcement-to-law enforcement cooperation context are adapted and applied to the specific transfers covered by the UK-US Agreement. In particular, the United Kingdom has explained that the provisions of the Umbrella Agreement that foresee a role for the relevant Competent Authority (which does not exist in a situation of direct cooperation between a United Kingdom service provider and a law enforcement authority in the US) are interpreted mutatis mutandis to refer to the Designated Authority (as defined under the UK-US Agreement) ([150]) of the relevant Party.

(94) For example, on the notification of an Information Security Incident pursuant to Article 10 of the EU-US Umbrella Agreement, which requires a notification to the transferring Competent Authority, the United Kingdom has explained that this provision is applied mutatis mutandis to mean that the notification should be made to the Designated Authority of that Party from which the data was transferred.

(95) On the authorisation from the transferring Competent Authority prior to any onward transfer of personal information pursuant to Article 7 of the Umbrella Agreement, the United Kingdom has clarified that it will apply that provision mutatis mutandis to mean that the Designated Authority of the Party from which the data was transferred will need to authorise any onward transfer.

(96) With respect to the obligations under Article 8 of the Umbrella Agreement on maintaining the quality and integrity of information, a mutatis mutandis interpretation of the provision would make the Designated Authority of the Party who receives the data responsible for liaising with the provider who has transferred the data in case of any issues with respect to the data quality and integrity.

(97) On judicial redress, the United Kingdom has highlighted that transfers under the UK-US Agreement will always involve the Designated Authority of each Party. Where the US is the Party that receives data from service providers in the United Kingdom, the US Department of Justice will act as the Designated Authority. Therefore, according to the United Kingdom's interpretation, in each request issued on the basis of the UK-

---

(148) 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, available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN

(149) Article 9(1) of the Agreement.

(150) Pursuant to Article 1(8) of the UK-US Agreement, "Designated Authority" means the governmental entity designated, for the United Kingdom, by the Secretary of State for the Home Department, and for the United States, by the Attorney General.

US Agreement, the Department of Justice as a federal authority designated under the US Judicial Redress Act will be involved, and judicial redress can thus be exercised against the Department of Justice in accordance with Article 19 of the Umbrella Agreement. In addition, the United Kingdom has confirmed to the Commission services that the Judicial Redress Act is not the only mechanism for seeking redress. Depending upon the circumstances and context of the specific case, other applicable US laws provide alternative routes by which judicial redress might be sought.

3.2.3. Oversight and redress

(98) Depending on the powers used by the competent authorities when processing personal data for a law enforcement purpose (whether under the DPA 2018 or the IPA 2016), different bodies continue to ensure the oversight over the use of these powers, as assessed in recitals (158) to (174) of Implementing Decision (EU) 2021/1772, and redress mechanisms continue to be available under Part 3 of the DPA 2018, under the IPA 2016 and under the Human Rights Act 1998, as analysed in recitals (250) to (269) of Implementing Decision (EU) 2021/1772.

(99) With respect to oversight over Part 3 of the DPA 2018, the functions and powers of the Information Commission are analysed in recitals (158) to (160) and (162) of Implementing Decision (EU) 2021/1772, subject to the amendments introduced by the Data (Use and Access) Act described in section 2.3.1 and 2.3.2 of this Decision.

(100) In terms of the implementation of these powers, since the adoption of Implementing Decision (EU) 2021/1772 the Information Commissioner has handled numerous complaints ([151]) 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 ([152]). The Information Commissioner also issued 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 ([153]).

(101) With respect to the use of investigatory powers under the IPA 2016, independent and judicial oversight continues to be ensured by the Investigatory Powers Commissioner (IPC), assisted by other Judicial Commissioners, which are collectively referred to as Judicial Commissioners ([154]). In this area, the Investigatory Powers (Amendments) Act 2024 has made only limited and targeted modifications, which do not affect the

---

(151) For example, the Information Commission in 2023-24 received 1890 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.

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

(153) 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/.

(154) See recital (250) of Implementing Decision (EU) 2021/1772.

independence, tasks and powers of the Judicial Commissioners, but are aimed at strengthening the functioning in practice of the existing oversight regime, 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 ([155]).

3.3. Relevant developments regarding access and use by United Kingdom public authorities for national security purposes

(102) With respect to investigatory powers exercised in the context of national security, the IPA 2016 continues to provide the legal framework for the use of these powers. In addition to the amendments concerning targeted investigatory powers which can, subject to specific conditions, be relied upon also by certain law enforcement authorities, as described in recitals (77) to (85) of this Decision, the Investigatory Powers (Amendment) Act 2024 has also made modifications to one of the powers provided by the IPA 2016 that can be exercised in bulk.

(103) More specifically, the Investigatory Powers (Amendment) Act 2024 has introduced in the new Part 7A of the IPA 2016 a specific regime for the retention and examination of a specific subset of bulk personal datasets ([156]), i.e. for those datasets for which the individuals to whom the personal data relates could have no, or only a low, reasonable expectation of privacy in relation to the data ([157]). Whether or not a bulk personal dataset is part of this specific subset of datasets is determined by the head of an intelligence service on the basis of all circumstances, in particular (i) the nature of the data, (ii) the extent to which data has been made public by the individuals, or the individuals have consented to the data being made public, (iii) if the data has been published, the extent to which it was published subject to editorial control or by a person acting in accordance with professional standards, (iv) if the data has been published or is otherwise in the public domain, the extent to which the data is widely known about, and (v) the extent to which the data has already been used in the public domain ([158]).

(104) Importantly, for the retention and examination of bulk personal datasets that do not fall within this category, i.e. those that are more sensitive and therefore entail a reasonable expectation of privacy, 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 ([159]).

([155]) Section 227 of the IPA 2016, as introduced by section 7 of the Investigatory Powers (Amendment) Act.

([156]) Bulk Personal Dataset warrants issued pursuant to section 200 of the IPA 2016 authorise intelligence agencies to retain and examine sets of data that contain personal data relating to a number of individuals and 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, and that is retained electronically by an intelligence service and held for analysis in the exercise of its statutory functions, see also section 199 of the IPA 2016.

([157]) Section 226A(1) of the IPA 2016 , as introduced by section 2 of the Investigatory Powers (Amendment) Act 2024.

([158]) Section 226A(3) of the IPA 2016, as introduced by section 2 of the Investigatory Powers (Amendment) Act 2024.

([159]) The Investigatory Powers (Amendment) Act 2024 has amended section 213 of the IPA 2016 to the effect that bulk personal dataset warrants cease to have effect 12 months after they were issued.

(105) Part 7A of the he IPA 2016 provides for two types of authorisation: individual authorisation and category authorisation. The retention, or the retention and examination, of every bulk personal dataset held under Part 7A must be authorised under one of these authorisations. Both authorisations require in principle ([160]) an authorisation by the head of the intelligence service (or a person acting on their behalf) and approval by an independent Judicial Commissioner ([161]). An individual authorisation is granted by the head of an intelligence service subject to the conditions set out section 226B(4) of the IPA 2016, and subject to prior approval by the Judicial Commissioners. The Judicial Commissioner must review the conclusions of the person who granted the authorisation in relation to whether section 226A, i.e. the low or no reasonable expectation of privacy requirement, applies to the bulk personal dataset described in the authorisation ([162]).

(106) A category authorisation authorises the retention, or retention and examination, of a category of bulk personal datasets described in the authorisation.

(107) The decision to grant the category authorisation is taken by the head of the intelligence service where they consider that section 226A applies to any dataset within the category and where the decision to grant the authorisation is approved by an independent Judicial Commissioner ([163]). The latter must review whether section 226A, i.e. the low or no reasonable expectation of privacy requirement, applies to any dataset that falls within the category of datasets described in the authorisation ([164]).

(108) Importantly, when approving a decision to grant an individual or category authorisation, the Judicial Commissioner must "apply the same principles as would be applied by a court on an application for judicial review" ([165]) and consider these matters with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 of the IPA 2016 (general duties in relation to privacy) ([166]). Moreover, the issuing of authorisations is subject to strict ex-

---

Previously, such warrants needed to be renewed every 6 months. See section 3 of the Investigatory Powers (Amendment) Act 2024.

(160) An individual authorisation may be granted without prior judicial approval only (i) if the person granting the individual authorisation considers that the bulk personal dataset in question falls within an existing category authorisation, or (ii) in case of urgency, see section 226B(6) of the IPA 2016. In the latter case, the decision to grant an urgent individual authorisation must be reviewed by a Judicial Commissioner within three working days following the day of issue, see section 226BC of the IPA 2016.

(161) Section 226B(1) of the IPA 2016, as introduced by section 2 of the Investigatory Powers (Amendment) Act.

(162) Section 226BB(1)(a) of the IPA 2016, as introduced by section 2 of the Investigatory Powers (Amendment) Act 2024.

(163) Section 226BA of the IPA 2016, as introduced by section 2 of the Investigatory Powers (Amendment) Act.

(164) Section 226BB(1)(b) of the IPA 2016, as introduced by section 2 of the Investigatory Powers (Amendment) Act.

(165) Section 226BB(2)(a) of the IPA 2016, as introduced by section 2 of the Investigatory Powers (Amendment) Act 2024.

(166) Section 226BB(2)(b) of the IPA 2016, as introduced by section 2 of the Investigatory Powers (Amendment) Act 2024. In accordance with the general duties in relation to privacy as set out in section 2 of the IPA 2016, a public authority must have regard to (a) whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means, (b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information, (c) the public interest in the integrity and security of telecommunication systems and postal services, and (d) any other aspects of the public interest in the protection of privacy.

post oversight, in particular through annual reporting to the Secretary of State and the Intelligence and Security Committee of Parliament ([167]) and through regular inspections of the Office of the IPC ([168]).

(109) In terms of relevant developments in the area of oversight, the Office of the IPC has published annual reports for the years 2021, 2022 and 2023, which provide detailed statistics and information about the use of investigatory powers by intelligence agencies and law enforcement authorities in the United Kingdom ([169]). The reports also describe the Office's audits and investigations, as well as their findings, confirming that the IPC continues to ensure its very important oversight function under the United Kingdom's investigatory powers regime. For example, in 2023, it reviewed the necessity and proportionality justifications for the use of bulk interception powers (as assessed in recitals (218) to (225) of implementing Decision (EU) 2021/1772) by the Government Communications Headquarters (GCHQ), concluding that a significant majority of the statements were articulated with a sound rationale, while in some cases proportionality was not well expressed. These findings were discussed with the GCHQ Compliance Team, who undertook to commission additional internal awareness training to address this issue ([170]).

(110) In addition, the Investigatory Powers Tribunal issued a public report of its activities and case law for the period 2021 to 2023 ([171]). The report shows that the number of cases received by the Tribunal has more than doubled since 2017, with more than 400 cases received in 2023 ([172]). Most complaints were against law enforcement agencies, closely followed by security and intelligence authorities ([173]). Importantly, in 2022 and 2023, the Tribunal handed down judgments in cases it had received prior to 2021 in which it found that United Kingdom public authorities (respectively Police Scotland ([174]), Greater Manchester Police ([175]), Surrey Police ([176]), and MI5 and the Home Secretary ([177]) had acted unlawfully. In terms of remedies, the Investigatory Powers Tribunal among other ordered the destruction of any material unlawfully obtained, and in one case also the payment of £12,000 by way of just satisfaction for the breaches identified. The annual report thus confirms that the Investigatory Powers Tribunal effectively fulfils its important role in guaranteeing oversight and redress in the area of criminal law enforcement and national security access to personal data.

---

(167) Sections 226DA and 226DB of the IPA 2016, as introduced by section 2 of the Investigatory Powers (Amendment) Act 2024.

(168) 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, p.3.

(169) The annual reports are available at the following link: https://www.ipco.org.uk/publications/annual-reports/.

(170) See paras. 6.39 to 6.43 of the Annual Report 2023, 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 .

(171) The Investigatory Powers Tribunal Report 2021-2023, available at the following link: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

(172) The Investigatory Powers Tribunal Report 2021-2023, p. 5.

(173) The Investigatory Powers Tribunal Report 2021-2023, p. 12.

(174) Wilson v Police Scotland [2022] UKIPTrib 5.

(175) Pendlebury v Greater Manchester Police [2023] UKIPTrib 2.

(176) Hill v Metropolitan Police Service & Independent Office For Police Conduct [2022] UKIPTrib 6.

(177) Liberty & Privacy International v Security Service and Secretary of State for the Home Department [2023] UKIPTrib 1.

(111) Moreover, the report also highlights important developments, such as a judgment by the European Court of Human Rights in which the Court held that individuals anywhere in the world can make a claim before the Investigatory Powers Tribunal concerning the operation of the UK's bulk interception regime if the conduct in question was carried out by a United Kingdom public body and occurred in the United Kingdom ([178]).

4. CONCLUSION

(112) The Commission considers that the UK GDPR and the DPA 2018, as amended by the Data (Use and Access) Act, continue to ensure a level of protection for personal data transferred from the European Union that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679.

(113) 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 punished 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.

(114) Finally, on the basis of the available information about the United Kingdom legal order, the Commission considers that any interference with the fundamental rights of the individuals whose personal data are transferred from the European Union to the United Kingdom by United Kingdom public authorities for public interest purposes, in particular law enforcement and national security purposes, continues to be limited to what is strictly necessary to achieve the legitimate objective in question and that effective legal protection against such interferences exists.

(115) Therefore, in light of the findings of this Decision, it should be decided that the United Kingdom continues to ensure an adequate level of protection within the meaning of Article 45 of Regulation (EU) 2016/679, interpreted in light of the Charter of Fundamental Rights of the European Union.

(116) This conclusion is based on both the relevant United Kingdom domestic regime, as it has evolved since the adoption of Implementing Decision (EU) 2021/1772, and its international commitments, in particular the United Kingdom's continued adherence to the European Convention of Human Rights and continued submission to the jurisdiction of the European Court of Human Rights. Continued adherence to such international obligations is therefore a particular important element of the assessment on which this Decision is based.

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

(117) 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.

([178]) *Wieder and Guarnieri v UK*, [2023] ECHR 668, see also Investigatory Powers Tribunal Report 2021-2023, p. 6.

(118) Consequently, a Commission adequacy decision adopted pursuant to Article 45(3) of Regulation (EU) 2016/679 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) 2021/1772, as amended by this Decision, transfers from a controller or processor in the European Union to controllers or processors in the United Kingdom may take place without the need to obtain any further authorisation.

(119) It should be recalled that, pursuant to Article 58(5) of Regulation (EU) 2016/679 and as explained by the Court of Justice in the *Schrems I* judgment ([179]), 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 ([180]).

6. MONITORING

(120) Pursuant to Article 45(4) of Regulation (EU) 2016/679, 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, to the functioning of the restructured ICO, including with respect to complaint handling and the application of corrective powers, as well as to compliance with the limitations and safeguards with respect to government access, in particular with respect to the newly introduced Part 7A of the IPA 2016. Amongst other elements, case law developments and oversight by the ICO and other independent bodies should inform the Commission's monitoring.

(121) To facilitate this monitoring, the United Kingdom authorities should promptly inform the Commission of any material change to the UK legal order that has an impact on the legal framework that is the object of Implementing Decision (EU) 2021/1772, 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) 2021/1772, as amended by this Decision, both as regards the processing of personal data by controllers and processors under the UK GDPR and the limitations and safeguards applicable to access to personal data by public authorities. This should include developments regarding the elements mentioned in recital (120).

---

(179) *Schrems I*, paragraph 65.

(180) *Schrems I*, paragraph 65: "It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity".

(122) 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 controllers or processors 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, or for national security including any oversight bodies, do not ensure the required level of protection.

(123) Where available information, in particular information resulting from the monitoring of Implementing Decision (EU) 2021/1772, as amended by 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. For example, such a procedure would be triggered in cases where onward transfers, including on the basis of new adequacy regulations adopted by the Secretary of State or international agreements concluded by the United Kingdom, would no longer be carried out under safeguards ensuring the continuity of protection within the meaning of Article 44 of Regulation (EU) 2016/679.

(124) 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 93(2) of Regulation (EU) 2016/679 with a view to partially or completely suspend or repeal this Decision.

(125) Alternatively, the Commission will initiate this procedure with a view to amend the 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.

(126) 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 93(3) of Regulation (EU) 2016/679, immediately applicable implementing acts suspending, repealing or amending the Decision.

7. REVIEW, DURATION AND RENEWAL OF THIS DECISION

(127) In application of Article 45(3) of Regulation (EU) 2016/679, 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, taking into account the elements listed in Article 45(2) of Regulation (EU) 2016/679. 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.

(128) 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.

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

(130) The Commission must also take into account that the data protection framework assessed in this Decision and in Implementing Decision (EU) 2021/1772 may further evolve.

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

(132) 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 93(2) of Regulation (EU) 2016/679.

8. FINAL CONSIDERATIONS

(133) The European Data Protection Board published an opinion ([181]) which has been taken into consideration in the preparation of this Decision.

(134) The measure provided for in this Decision is in accordance with the opinion of the Committee established under Article 93 of Regulation (EU) 2016/679,

(135) Implementing Decision (EU) 2021/1772 should therefore be amended accordingly.

HAS ADOPTED THIS DECISION:

Article 1

Article 1(2) of Implementing Decision (EU) 2021/1772 is repealed.

Article 2

Article 4 of Implementing Decision (EU) 2021/1772 is replaced by the following:

(181) Opinion 26/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, available at the following link https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.

‘Article 4

This Decision shall expire on 27 December 2031, unless extended in accordance with the procedure referred to in Article 93(2) of Regulation (EU) 2016/679.’

Article 3

This Decision is addressed to the Member States.

Done at Brussels, 19.12.2025

For the Commission
Michael McGRATH
Member of the Commission

CERTIFIED COPY
For the Secretary-General

Martine DEPREZ
Director
Decision-making & Collegiality
EUROPEAN COMMISSION