ANALYSIS OF THE DRAFT UK ADEQUACY DECISION

Analysis – September 2025

Author: Mariano delli Santi mariano@openrightsgroup.org

IN THIS ANALYSIS

0. EXECUTIVE SUMMARY

0.1 On July 22, the European Commission published their Draft Adequacy Renewal for the UK adequacy decisions adopted under the EU GDPR and LED. Their legal analysis presents key deficiencies, which underestimate both the immediate impact of recent changes affecting UK data protection law, and the potential for future divergence.

0.2 Open Rights Group has produced this analysis to fill these gaps, in the hope that this will help producing a more robust legal assessment underpinning the UK adequacy determination. In particular:

0.3 In Chapter 1, we address how Regulations 2023/1417 removed references to fundamental rights from UK data protection law. This narrows the applicability of "rights and freedoms of data subjects", thus affecting several key assessments such as with conditions to process special category data, Article 23 restrictions, legitimate interests and DPIAs.

0.4 In Chapter 2, we address how the REUL Act deleted the principle of supremacy of EU law from the UK GDPR. This removed the hierarchical supra-ordination over domestic enactments of the UK GDPR, thus undermining the safeguards introduced by Article 23 of the UK GDPR.

0.5 In Chapter 3, we address how the DUA Act introduces the new lawful ground of "Recognised Legitimate Interests", which legitimises data processing for an expansive list of purposes, even against an overriding right or interest of the data subjects.

0.6 In Chapter 4, we address how the DUA Act introduces a new rule-making power that can be used to restrict the definition of special category data and reduce legal safeguards.

0.7 In Chapter 5, we address how the DUA Act introduces a new, expansive exemption from the purpose limitation principle, which legitimises further processing without regard of the original purpose data was collected for.

0.8 In Chapter 6, we address how the DUA Act introduces several changes to the rules governing data processing for scientific purposes, leaving scope for abuse for commercial interests.

0.9 In Chapter 7, we address how the DUA Act gives the UK government the power to allow the onward transfer of personal data to third countries even in the absence of European Essential Guarantees

0.10 In Chapter 8, we address how the DUA Act allows the onward transfer of personal data to third countries on the basis of additional safeguards that do not ensure the availability of enforceable data subject rights and effective legal remedies.

0.11 In Chapter 9, we address how the DUA Act widens the scope for the UK government to interfere with the objective and impartial functioning of the UK supervisory authority, further eroding the independence of an already compromised regulatory authority.

0.12 In Chapter 10, we address how the DUA Act dilutes the role of the UK supervisory authority, shifting focus away from regulatory enforcement and data subjects rights toward data controllers and extra-legal considerations.

0.13 In Chapter 11, we address how the performance of the UK supervisory authority is already showing a severe downward trajectory

0.14 In Chapter 12, we explain why the review mechanisms envisioned by the draft UK adequacy decision will struggle to effectively monitor relevant developments in UK data protection law, exposing EU-UK cross-border data transfers to the risk of a judicial invalidation and heighten legal uncertainty.

1. REGULATIONS 2023/1417 AND IMPACT ON FUNDAMENTAL RIGHTS

1.1 Regulations 2023/1417 removed all references to an overarching right to data protection within the UK GDPR and the DPA 2018, and established that "fundamental rights or fundamental freedoms (however expressed)" refer only to rights set down in the European Convention of Human Rights, which have been given effect in the United Kingdom's domestic law under the Human Rights Act 1998.

1.2 This development is addressed by chapter 2.1 "The data protection framework of the United Kingdom" of the draft adequacy decision. In particular, Recital 12 thereof that:

1.2.1 *"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 [...] This includes the right to respect for private and family life (and the protection of personal data as part of that right)".*

1.3 However, the Commission severely underestimates the impact of these changes over UK data protection law.

1.4 The right to private life under Article 8 of European Convention of Human Rights (ECHR) is structurally different from the right to data protection under Article 8 of the Charter of Fundamental Rights of the EU (CFREU). In detail:

1.4.1 Although closely related, "*The right to respect for private life consists of a general prohibition on interference, subject to some public interest criteria*"[1] and "*the assessment of whether or not there is, or has been, an interference with private life depends on the context and facts of each case*".[2] On the contrary, the fundamental right to data protection concerns "*all kinds of personal data and data processing, irrespective of the relationship and impact on privacy*"[3] and, although "*processing of personal data may also infringe on the right to private life [...] it is not*

1 European Union Fundamental Rights Agency, Council of Europe, European Data Protection Supervisor, *Handbook on European data protection law - 2018 edition, p.19*, available at: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition#publication-tab-0

2 Ibid, p.20

3 Ibid, p.20

necessary to demonstrate an infringement on private life for data protection rules to be triggered".[4]

1.4.2 Furthermore, and although Von Hannover v Germany (2004) has clarified that the State does have *positive obligations* under Article 8 ECHR, it remains the case that "*the object of art 8 is essentially that of protecting the individual against arbitrary interference by the public authorities*".[5] This is in contrast with the right to data protection under Article 8 of CFREU, which establishes horizontal obligations which apply to relationships between private parties.

1.5 In the analysis of David Erdos, Co-Director of the Centre for Intellectual Property and Information Law (CIPIL) at the University of Cambridge, "*the narrowing of fundamental rights and freedoms within data protection to HRA Convention Rights means that this concept no longer recognises an overarching right to data protection, is no longer open-textured and so cannot encompass free-standing rights to such desiderata as privacy and non-discrimination and is no longer fully horizontal vis-à-vis the private sector*".

1.6 In turn, he concludes, "*previously overarching fundamental rights which do not fall within HRA Convention Rights will, at most, be considered interests of the data subject. It is, therefore, inevitable that they will be weighted more lightly than previously when reconciliation is necessary with other competing rights or, more often, purely economic or utilitarian interests*".D [6]

1.7 Thus, these changes affect a constitutional element of the UK GDPR, with the potential to lower the level of data protection afforded in a wide range of circumstances including:

1.7.1 Derogations from the prohibition on processing special category data (where article 9(2) letters g to j require that a Union or Member State law must "respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject");

---

4 Ibid, p.20

5 European Court of Human Rights, *Von Hannover v Germany [2004] 6 WLUK 538*, para. 57, at: https://hudoc.echr.coe.int/eng?i=001-61853

6 David Erdos, *Data Protection Reform via the Retained EU Law (Revocation and Repeal) Act and the Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023/1417: Arguably Partially Unlawful and Liable to Undercut the UK's Council of Europe Commitments*, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4212417

1.7.2 Restrictions to the exercise of data subjects rights or data protection principles (which, under Article 23, must respect “the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society”);

1.7.3 Legitimate interest (which must be balanced against “the rights and freedom of data subjects”);

1.7.4 Data Protection Impact Assessments (which must be carried out when processing “is likely to result in a high risk to the rights and freedoms of natural persons”);

2. REVOCATION OF EU LAW ACT AND IMPACT ON FUNDAMENTAL RIGHTS

2.1 **The Retained EU Law (Revocation and Reform) Act (REULA) 2024 deprives the UK GDPR of the supremacy it enjoyed under EU law. Section 106 of the Data (Use and Access) Act, which stipulates that UK law "does not override a requirement under the main data protection legislation", does not restore the supremacy of the UK GDPR, which can now be overridden by domestic data protection legislation.**

2.2 This development is addressed by chapter 2.1 "The data protection framework of the United Kingdom" of the draft adequacy decision. In particular, paragraph 11 thereof states that "section 106 ensures that the United Kingdom's data protection framework continues to operate as immediately before the REUL Act came into effect [...] This included ensuring that domestic laws continue to be interpreted compatibly with the data protection legislation.". However, the Commission misunderstand the impact of REULA and Section 106 of the DUAA 2025 on UK data protection law.

2.3 Eleonor Dhus, a UK data protection law expert, points out that REULA *"turns the relationship between the UK GDPR and the DPA on its head. If there is a conflict between the UK GDPR and the DPA 2018, the DPA will take precedence*".[7] While Section 106 of the DUAA 2025 restores hierarchical supremacy of "main data protection legislation" against other domestic enactments, it does not change the subordination of the UK GDPR to the DPA 2018. As pointed out by David Erdos, Co-Director, Centre for Intellectual Property and Information Law (CIPIL) at the University of Cambridge, "the UK GDPR would remain fully subject to the DPA 2018 and the new rule would also expressly not apply to an 'enactment forming part of the main data protection legislation'"[8]

2.4 Notably, **Schedules 2, 3 and 4 of the Data Protection Act 2018 implements a number of restrictions to data protection principles and the exercise of data subject rights.** Except for the Immigration Exemption, none of these

7 Eleonor Duhs, *The Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023 – a failure to contain damaging uncertainty*, at: https://bateswells.co.uk/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023/

8 David Erdos, *Data Protection Reform via the Retained EU Law (Revocation and Repeal) Act and the Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023/1417: Arguably Partially Unlawful and Liable to Undercut the UK's Council of Europe Commitments*, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4212417

exemptions enshrines adequate safeguards as required by the *Open Rights*[9] judgement. In particular, they do not include the requirement that such exemptions can only be relied upon on a case-by-case basis, only in relation to the right that would prejudice such interests, and that such exemption must be lifted once the exercise of such right would no longer constitute prejudice. As pointed out by Eleonor Dhus in her response to the Lords' Inquiry into Adequacy:

2.4.1 *"it is clear that none of the exemptions under Schedule 2-4 of the Data Protection Act 2018 were drafted in such a way as to comply with the requirements of Article 23(2) of the UK GDPR. […] The significant discrepancies in the level of safeguards under the immigration exemption as compared with those provided under any of the other exemptions set out in Schedule 2-4 of the Data Protection Act 2018 could also be cited in any challenge to UK data adequacy before the CJEU. The argument would be that only in the area of immigration are the protections for data subjects "essentially equivalent" to those under the EU regime and therefore that the UK's data adequacy decision is invalid".*[10]

2.5 However, and since REULA has undermined the principle, established in *Open Rights*, that the UK GDPR took precedence over the provisions of the DPA 2018, the unlawfulness of these exemptions cannot be remedied in Court any longer.

2.6 Finally, Section 16 of the DPA 2018 gives powers to the Secretary of State to "restricting the scope of the obligations and rights" under the GDPR. As these would constitute changes "forming part of the main data protection legislation", the legality of such new "exemptions" could not be judged against the standards provided by Article 23 of the UK GDPR.

9 UK High Court, *R (Open Rights Group & the3million) v Secretary of State for the Home Department & Secretary of State for Digital, Culture, Media and Sport ([2021] EWCA Civ 800)*, at: https://www.judiciary.uk/wp-content/uploads/2023/03/The3Million-v-Home-Secretary.pdf

10 Eleonor Duhs, *Written Evidence (DAT0005)*, Pp 5-6, at: https://committees.parliament.uk/writtenevidence/130147/pdf/

3. LAWFULNESS OF PROCESSING

5.1 **Schedule 4 of the Data (Use and Access) Act 2025 introduced a list of new legal bases for processing, i.e. recognised legitimate interests, which can be relied upon from private organisations to process personal data. These new "recognised legitimate interests" exclude the need to carry out a balancing test as provided under Article 6(1)f; thus, data processing under the lawful basis of "recognised legitimate interest" will always legitimate, even against overriding rights and interests of the individual involved.**

5.2 This list currently includes the purposes of:

5.2.1 Making a disclosure of personal data to a public authority;

5.2.2 Safeguarding national security, protecting public security or for defence purposes;

5.2.3 Detecting, investigating or preventing crime, as well as apprehending or prosecuting offenders;

5.2.4 Safeguarding a vulnerable individual.

5.3 **Furthermore, Section 70 of the Data (Use and Access) Act 2025 introduced a delegated legislative power that allow the Secretary of State to add further conditions to Schedule 4 (recognised legitimate interests).** In other words, the Secretary of State can introduce new legal bases that make data processing always legitimate even against an overriding interest of the individual.

5.4 This development is addressed by chapter 2.2.1 "*Lawfulness and fairness of processing*" of the draft adequacy decision. In particular, Recital 23 thereof reads that "the newly introduced legal ground of recognised legitimate interest is subject to several important limitations", which include the fact that processing must pursue "objectives listed in Article 23 UK GDPR (which corresponds to Article 23 of Regulation (EU) 2016/679)". Furthermore, the draft decision points out that "the Secretary of State may only add a recognised legitimate interest 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. Upon these bases, the draft adequacy decision reaches the conclusion that recognised legitimate interests "can thus not be relied upon for commercial purposes".

5.5 However, the Commission fails to consider several important aspects in their assessment.

5.5.1 Firstly, Article 23(1)(e) of the UK GDPR include the objective to safeguard "an important economic or financial interest of the United Kingdom". In turn, **the Secretary of State can designate any commercial, economic or private interests as a recognised legitimate interest, insofar the Secretary of State considers it "an important economic or financial interest of the United Kingdom".**

5.5.2 Secondly, the Secretary of State only needs to "consider" that the an objective listed in Article 23(1)(c) to (j) is being met in order to introduce a new recognised legitimate interest. The wording *considers* clearly distinguishes these provisions from the restrictions imposed by Article 23 of the EU GDPR, where any restriction *must respect* "the essence of the fundamental rights and freedoms" and must be "a necessary and proportionate measure in a democratic society". **This makes the powers of the Secretary of State discretionary: it is not clear upon which basis a domestic Court could find the Secretary of State has failed to properly "consider" such limits when introducing a new recognised legitimate interest.**

5.5.3 Finally, the draft adequacy decision fails to consider that the recognised legitimate interests being introduced by Schedule 4 of the Data (Use and Access) Act 2025 already allow private organisations to pursue commercial purposes. For instance, a data broker could rely on the recognised legitimate interest of "Detecting, investigating or preventing crime" to sell data to law enforcement authorities. Notably, and because a recognised legitimate interest does not need a "balancing test" under Article 6(1)f, **selling data to law enforcement authorities would be lawful even if the interest of detecting, investigating or preventing crime was overridden by the interests or fundamental rights and freedoms of the data subject.**

4. PROHIBITION TO PROCESSING OF SPECIAL CATEGORY DATA

4.1 **Section 74 of the DUA Act 2025 introduces a new delegated legislative power which allows the Secretary of State to amend the definition of special category of data under Article 9(1) of the UK GDPR.** In particular, the provision allows the Secretary of State:

4.1.1 To designate a new category of data (i.e. "added processing") which is subject to the prohibition for special category data under article 9(1);

4.1.2 To make provision so that added processing "is not subject to the prohibition for special category data under article 9(1); or that "an exception in Article 9(2) may or may not be relied on in connection with added processing"; or to varying "such an exception as it applies in connection with added processing".

4.2 These developments are addressed by chapter 2.2.2 "*Processing of special categories of personal data*" of the draft adequacy decision. In particular, Recital 27 reads that "these amendments do not affect the level of protection for special categories of personal data". The Commission reaches this conclusion by noting that this power "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" and that "*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*".

4.3 **Contrary to the Commission's assessment, these conditions do not seem to negate the power of the Secretary of State to restrict the scope of the prohibition under article 9(1).** Indeed, the Secretary of State could use this power to add a new description of special category data which is a subgroup of the existing list under Article 9(1), and then make provisions so that this new, added processing is not subject to that prohibition. For instance:

4.3.1 The Secretary of State could, designate "membership to a political party" as an additional description of special category of data.

4.3.2 The Secretary of State could then make provisions that data related to the additional description "membership to a political party" would not be considered subject to the prohibition under Article 9(1).

4.3.3 In turn, data related to "membership to a political party" would be exempted from the prohibition from the prohibition to process data related to "political opinions, religious or philosophical beliefs" under article 9(1).

4.4 Likewise, the Secretary of State could also designate a new exemptions that apply to such "added" processing, thus allowing the processing of special category data under a new condition not listed in Article 9(2). For instance:

4.4.1 The Secretary of State could, under Schedule 74 letter a, designate "membership to a political party" as an additional description of special category of data.

4.4.2 The Secretary of State could then make provisions, under Schedule 74 letter d, that data related to the additional description "membership to a political party" can rely on a new condition for processing not included in the current list under Article 9(2).

4.4.3 In turn, data related to "membership to a political party", i.e. data which is related to "political opinions, religious or philosophical beliefs" could be processed even without relying on an exemption under article 9(2).

5. PURPOSE LIMITATION

5.6 **Schedule 5 of the Data (Use and Access) Act 2025 introduced a list of purposes according to which further processing of personal data is, always, "to be treated as compatible with original purpose", even if the conditions set out by the compatibility test as provided under Article 6(4) of the UK GDPR are not met.** This list can be relied upon by both private and public organisations, and it includes the purposes of:

- Making a disclosure of personal data to a public authority;
- Making a disclosure of personal data for Research, Archiving or Statistical Purposes;
- Protecting public security;
- Responding to an emergency;
- Detecting, investigating or preventing crime, as well as apprehending or prosecuting offenders;
- Protecting the vital interests of the data subject or another individual
- Safeguarding a vulnerable individual;
- The assessment or collection of a tax or duty or an imposition of a similar nature;
- Complying with an obligation of the controller under an enactment, a rule of law or an order of a court or tribunal.

5.7 **Furthermore, Section 71 of the Data (Use and Access) Act 2025 introduced a delegated legislative power that allow the Secretary of State to add further conditions to Schedule 5 (processing to be treated as compatible with the original purpose).** In other words, the Secretary of State can can designate new data processing which is exempted from the purpose limitation principle.

5.8 These developments are addressed by chapter 2.2.3 "*Purpose limitation*" of the draft adequacy decision. In particular, paragraph 32 thereof reads that the list *"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)"*. Furthermore, the draft decision points out that *"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"*. Upon these bases, the draft

adequacy decision reaches the conclusion that the list of compatible purposes "can thus not be relied upon for commercial purposes".

5.9 However, the Commission fails to consider several important aspects in their assessment:

5.9.1 Firstly, Article 23(1)(e) of the UK GDPR include the objective to safeguard "an important economic or financial interest of the United Kingdom". In turn, **the Secretary of State can designate any commercial, economic or private purpose as a compatible purpose, insofar the Secretary of State considers it "an important economic or financial interest of the United Kingdom".**

5.9.2 Secondly, the Secretary of State only needs to "consider" that the an objective listed in Article 23(1)(c) to (j) is being met in order to introduce a new compatible purpose. The wording *considers* clearly distinguishes these provisions from the restrictions imposed by Article 23 of the EU GDPR, where any restriction *must respect* "the essence of the fundamental rights and freedoms" and must be "a necessary and proportionate measure in a democratic society". **This makes the powers of the Secretary of State discretionary: it is not clear upon which basis a domestic Court could find the Secretary of State has failed to properly "consider" such limits when introducing a new recognised legitimate interest.**

5.9.3 Thirdly, the list of compatible purposes introduced by Schedule 5 DUAA 2025 qualifies as a restriction to the purpose limitation principle under Article 5 of the UK GDPR. However, Schedule 5 does not implement any of the safeguards required by Article 23(2) of the UK GDPR, nor there are restrictions that prevent the list of compatible purpose to be relied upon when doing so would violate "the essence of the fundamental rights and freedoms" and would not be "necessary and proportionate measure in a democratic society".

5.9.4 Finally, the draft adequacy decision fails to consider that the recognised legitimate interests being introduced by Schedule 5 of the Data (Use and Access) Act 2025 already allow private organisations to pursue commercial purposes. For instance, a data broker could rely on the compatible purpose of "Detecting, investigating or preventing crime" to repurpose and thus sell data to law enforcement authorities. Notably, and because a compatible purpose does not include a "compatibility test" under Article 6(4) nor any of the safeguards listed in Article 23(2), **such further**

processing risks being considered lawful even when it violates "the essence of the fundamental rights and freedoms" and cannot be considered necessary and proportionate in a democratic society.

6. SCIENTIFIC RESEARCH PROVISIONS

6.1 **Section 67 of the Data (Use and Access) Act 2025 extends research exemptions to a new and broadly defined notion of "scientific research", which includes commercial technological development.** This includes research which is "privately or publicly funded" as well as "processing for the purposes of technological development or demonstration". Further, and according to the new definition of "scientific research", there is no need for such research to be carried out in the public interest unless it relates to "public health" purposes.

6.2 **Section 68 of the DUA Act 2025 introduces a new notion of purposeless consent, where data subjects can give broad consent to future research projects, even if those projects are not clearly defined at the point consent is given.**

6.3 **Section 77 introduces a new exemption from the requirement to inform data subjects about how their data will be used in research.** This exemption would apply when there would be a "disproportionate effort" to provide this information. New paragraph 6 of Article 13 provides a non-exhaustive list of factors for the controller to determine what constitutes a "disproportionate effort"—including the number of data subjects, the age of the personal data and any appropriate safeguards applied to the processing.

6.4 Notably, the draft adequacy decision does not address the new exemption to the to inform data subjects about how their data will be used in research. The draft decision does, however, address the changes introduced by Section 67 and 68 within chapter 2.2.1 "Definitions". In particular, Recital 18 states that *"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)"*, and Recital 19 states that the DUAA 2025 *"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"*.

6.5 Although its is true that the language of these changes mirrors those in the Recitals of the GDPR, the Commission does not seem to take into account the different legal weight that Recitals have compared to legal provisions,

and the heightened scope for abuse that these changes would introduce in UK data protection law.

6.6 In the UK, the scientific community has generally criticised these changes. The Royal Society has pointed out that, once given full legal status to broad definition contained in recitals, those could be "exploited by companies and individuals who do not follow ethical research practices".[11] The Ada Lovelace Institute mirrored these concerns, pointing out that these changes "must be read in the context of recent developments in artificial intelligence and the practice of AI developers", where *"The economic incentives for large technology companies to acquire as much data as possible [...] is driving compliance behaviour that deliberately pushes and exploits the boundaries of the law around legitimate interests, scientific research, and data reuse"*.[12]

6.7 With this in mind, the Ada Lovelace Institute laid out a number of areas where these changes to UK data protection law introduce a material risk for abuse, which are summarised below:

6.7.1 The proposed definition of scientific research is too broad and will permit abuse for commercial interests. Any AI development will likely be positioned by companies to reasonably be described as scientific and combined with the inclusion of commercial activities opens the door to data reuse for any data-driven product development under the auspices that this represents "scientific research"—even where their relationship to real scientific progress is unclear or tenuous.

6.7.2 Large tech companies could abuse the provisions to legitimise mass data scraping. Personal data scraped from the internet or collected via legitimate interest could potentially be legally re-used for training AI systems under the new provisions, if developers can claim that it constitutes "scientific research".

6.7.3 People may not even be told their data is being re-used. Section 77 will mean personal data collected through mass scraping or ingested during AI training would not be subject to normal notification requirements if it involved "disproportionate effort". AI developers to argue that contacting

11 The Royal Society, P*ost-Brexit divergence from GDPR: Implications for data access and scientific research in the UK*, at: https://royalsociety.org/-/media/policy/projects/post-brexit-data-protection/post-brexit-data-protection-workshop-note.pdf

12 Ada Lovelace Institute, *Policy briefing – Data (Use and Access) Bill: Committee Stage*, at: https://bills.parliament.uk/publications/59409/documents/6109

people whose data has been scraped or ingested by an AI model during training is impractical, as training datasets are very large and unstructured and retrieving personal data stored in a trained AI model is technically challenging. Data subjects cannot make use of their data rights if they do not even know their data is being processed.

6.8 Finally, it is worth mentioning that the changes introduced to definition, consent and notification requirements for scientific research processing would interact with the new list of compatible purposes, according to which "Making a disclosure of personal data for Research, Archiving or Statistical Purposes" is always to be considered compatible with the original purpose the data was collected for (See *supra*, §5). This further weights into the risks outlined above.

6.9 In his analysis of these provisions, Kings Counsel Stephen Cragg wrote that "*it is clear that these 'clarifications' in the Bill benefit data processors and controllers while providing no new protections for individual data subjects. In situations, especially where purposes will become automatically compatible, data subjects will lose important rights currently in play, such as the rights to be informed, to rectify, to restrict and to object to data processing*".[13]

13 Stephen Cragg KC, *IN THE MATTER OF THE DATA PROTECTION AND DIGITAL INFORMATION BILL*, paragraph 53, at: https://defenddigitalme.org/2023/11/28/new-legal-opinion-on-the-data-protection-and-digital-information-bill/

7. ESSENTIALLY EQUIVALENT LEVEL OF PROTECTION TO PERSONAL DATA FOR ONWARD DATA TRANSFERS

1.1 **Schedule 7 paragraph 4 of the Data (Use and Access) Act 2025 removes Article 45 of the UK GDPR, which mirrors provisions in the EU GDPR concerning adequacy determinations and the essentially equivalent level of protection.** This is replaced by a "Transfers approved by regulations" under new Article 45A, which stipulates that the Secretary of State may only approve international data transfer if the "data protection test" under new Article 45B is met.

1.2 The new "data protection test" reformulates—and omits some of—the standards set in Article 45 of the EU GDPR. Also, new Article 45A stipulates that "the Secretary of State may have regard to any matter which the Secretary of State considers relevant, including the desirability of facilitating transfers of personal data to and from the United Kingdom" when making such determinations.

1.3 These developments are addressed by chapter 2.2.5 "*Restrictions on onward transfers*" of the draft adequacy decision. In particular, paragraph 42 reads that *"While reformulating the list of relevant elements as provided under former the Article 45 of the UK GDPR, the new Article 45B retains the core elements of that list and therefore remains close to what is provided in Chapter V of Regulation (EU) 2016/679"*. This assessment does, however, overlooks key aspects of the new data protection test.

1.4 In comparison with the standards of Article 45 of the EU GDPR, the new "data protection test" defined by Article 45B requires, in order to be met, that the Secretary of State considers:

1.4.1 The "respect for the rule of law and for human rights" in the country of destination. Contrary to Article 45 of the EU GDPR, it omits the requirement to consider the impact that "public security, defence, national security and criminal law and the access of public authorities" to the level of protection of personal data.

1.4.2 The "existence, and powers, of an authority responsible for enforcing the protection". Contrary to Article 45 of the EU GDPR, it omits the requirement for such authority to be independent.

1.4.3 That "arrangements for judicial or non-judicial redress for data subjects in connection with such processing" are in place. Contrary to Article 45 of the EU GDPR, which requires "effective administrative and judicial

redress", the UK data protection test requires either one or the other—thus excluding the need of a judicial redress in the country of destination if an administrative redress is in place.

1.5 Furthermore, new Article 45A also allow the Secretary of State to "*have regard to any matter which the Secretary of State considers relevant, including the desirability of facilitating transfers of personal data to and from the United Kingdom"* when considering if adopting the decision to authorise an international data transfer. This give discretion to the Secretary of State to authorise transfers for reasons that do not account for the level of protection for personal data.

1.6 Notably, the Information Commissioner's Office, the UK supervisory authority, raised this same concern as follows:

> "*It would be helpful to clarify that the matters the Secretary of State may consider do not outweigh or take precedence over the need to meet the data protection test. We would welcome explicit clarification in the legislation that there is a distinction between the decision making about which countries to make adequacy regulations for, and the decision about whether the data protection test is met for any such country*".[14]

1.7 This opinion concerned the previous proposal known as Data Protection and Digital Information Bill. Such clarification, however, has never been enshrined in the Data (Use and Access) Bill; thus, the issue has been carried over to the new Act.

14 Information Commissioner's Office, *Information Commissioner's Response to the Data Protection and Digital Information (No 2) Bill (DPDI No 2 Bill)*, at: https://ico.org.uk/media2/migrated/4025316/response-to-dpdi-bill-20230530.pdf

8. APPROPRIATE SAFEGUARDS FOR ONWARD DATA TRANSFERS

8.1 **Schedule 7 paragraph 6 of the DUA Act 2025 removes Article 46(1) of the UK GDPR, which stipulates that international data transfers in the absence of an adequacy determination are allowed "only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available".** This is replaced by new Article 46(1A), which stipulates that:

8.1.1 "*1A. A transfer of personal data to a third country or an international organisation by a controller or processor is made subject to appropriate safeguards only—*

(a) in a case in which—

(I) safeguards are provided in connection with the transfer as described in paragraph 2 or 3 or regulations made under Article 47A(4), and

(ii) the controller or processor, acting reasonably and proportionately, considers that the data protection test is met in relation to the transfer or that type of transfer […]".

8.2 These developments are addressed by chapter 2.2.5 "*Restrictions on onward transfers*" of the draft adequacy decision. In particular, paragraph 43 reads that Schedule 7(4) of the DUAA *"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"*. Further, the commission points out that *"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"*.

8.3 This assessment does, however, overlooks key aspects of the UK new regime for transfers subject to appropriate safeguards.

8.3.1 Firstly, we have seen how the new UK standards—i.e. the "data protection test" and the "not materially lower" threshold—lack reference to key requirements for adequacy established by the Court of Justice of the European Union's case law, also known as European Essential Guarantees. Thus, it is unlikely that UK standards will match the requirement for an "essentially equivalent level of protection of personal data" under the GDPR.

8.3.2 Secondly, reliance on additional safeguards to conduct a data transfer under UK law is considered appropriate if "the controller or processor, acting reasonably and proportionately, considers that the data protection test is met". The new standard of reasonableness and proportionality replaces the requirement to ensure the availability of "enforceable data subject rights and effective legal remedies" under Article 46 of the EU GDPR.

8.4 Thus, new Article 46(1A) of the UK GDPR shifts the focus away from the level of protection afforded to the data, and toward the conduct of the data exporter. In turn, data transfers that do not provide enforceable rights and effective remedies, as required by the EU GDPR, could still be considered legal and subject to appropriate safeguards, insofar the data exporter can demonstrate that they acted "reasonably and proportionately".

8.5 Furthermore, it is worth mentioning that the draft adequacy decision points out, at paragraph 50, that:

> *"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. 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".*

8.6 However, the requirement for the controller to act "reasonably and proportionately" established by new Article 46(1A) of the UK GDPR seems to mirror provisions in the Asia-Pacific Privacy Framework, according to which *"in cases where disclosures are required by domestic law [i.e of the country of destination], the personal information controller [i.e the data exporter] would be relieved of any due diligence or consent obligations."*[15]

15 APEC PRIVACY FRAMEWORK (2015), available at: https://www.apec.org/docs/default-source/publications/2016/11/2016-cti-report-to-ministers/toc/appendix-17-updates-to-the-apec-privacy-framework.pdf

9. INDEPENDENCE OF THE SUPERVISORY AUTHORITY

9.1 **Schedule 14 of the Data (Use and Access) Act 2025 abolishes the Information Commissioner's Office (the ICO, i.e. the UK supervisory authority) and re-establishes it as a corporate body (the Information Commission) composed of a Chair, a Chief Executive Officer, and non-executive and executive members.**

9.2 The draft adequacy decision addresses the changes introduced by Schedule 14 of the DUAA 2025 at Recital 59 of the draft decision, which states that *"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"* the UK adequacy decision adopted in 2021. The same Recital continues with a summary analysis of the appointment process for the members of the Information Commission.

9.3 The assessment made by the Commission fails to understand the reality and the real-world dynamics which have engaged with the ICO and its functioning, as well as the significance of the changes introduced by the DUAA 2025 in this regard.

9.4 Firstly, and although Schedule 14 of the DUAA 2025 establishes formal safeguards against the removal of the Chair of the Information Commission, the Secretary of State would retain the power to amend the salary, allowances, and the tenure of the Chair, thus retaining the ability to interfere with their independence through economic coercion.

9.5 Secondly, the Chair of the Information Commission is a member of a the "Management board", a corporate body which works and adopts collegial decisions. None of the other members would enjoy significant guarantees against their dismissal or against financial coercion, and in particular:

9.5.1 Non-executive members other than the Chair are not appointed "by His Majesty by Letter Patent" and, thus, can be dismissed by the Secretary of State without addressing both Houses of Parliament. Furthermore, the Secretary of State maintains the power to amend their salary, allowances, and the conditions of their tenure.

9.5.2 Executive-members, including the Chief Executive Officer, do not have voting rights within the management board and are *"employed by the Commission on such terms and conditions, including those as to remuneration, as the non-executive members of the Commission may determine"*.

9.6 Thirdly, the UK government has already proven their ability to overcome formal guarantees against the political dismissal of members of independent authorities in the UK. For instance, the Labour government

has removed the Chair of the Competition and Market Authority (CMA) for political reasons—i.e. for his failure to align with the government mission to "support growth".[16] The provisions regulating the dismissal of the members of the CMA mirror those of the non-executive members of the Information Commission, who would thus be exposed to an equivalent risk of political interference.

9.7 Fourthly, the threat of political dismissal has already allowed the Labour government to influence the functioning of the ICO. Following the dismissal of the Chair of the CMA, the UK government has obtained formal commitments from other UK regulators "to ensure regulators and regulation support growth",[17] in line with the government agenda. This includes the ICO, which has adopted five formal commitments toward the government, including the promise to relax enforcement of cookie consent requirements and updating *"their transfer risk assessment tools to underpin the Data (Use and Access) Bill reforms to create a more proportionate and risk-based regime"*.

9.8 Finally, the UK Government has already demonstrated that the appointment process of the UK supervisory authority can be leveraged to achieve political goals. In 2021, the UK government published a vacancy notice[18] to seek a new Information Commissioner, tasked with delivering on the National Data Strategy (a policy adopted by the government the year before). This notice came alongside an opinion piece by the Minister for Digital, which described the appointment of the new Commissioner as "the first stage" in the process of implementing the UK data protection reform.[19] As a result, a cross-party group of Members of Parliament denounced that the UK government was seeking *"an Information Commissioner whose policy views match its own, rather than a regulator that will seek to enforce the law as Parliament has written it"*.[20]

16 Sky News, *Chair of UK's competition regulator removed by government*, at: https://news.sky.com/story/chair-of-uks-competition-regulator-removed-by-government-over-growth-concerns-13293755

17 HM Treasury, *New approach to ensure regulators and regulation support growth (HTML)*, at: https://www.gov.uk/government/publications/a-new-approach-to-ensure-regulators-and-regulation-support-growth/new-approach-to-ensure-regulators-and-regulation-support-growth-html

18 *Announcements (Archive): Information Commissioner*, at: https://publicappointments.cabinetoffice.gov.uk/appointment/information-commissioner-2/

19 Financial Times, *New approach to data is a great opportunity for the UK post-Brexit*, at: https://www.ft.com/content/ac1cbaef-d8bf-49b4-b11d-1fcc96dde0e1

20 Open Rights Group, *Cross-party group of MPs warn Govt about unduly influencing Regulator's appointment*, at: https://www.openrightsgroup.org/press-releases/cross-party-group-of-mps-warn-govt-about-unduly-influencing-regulators-appointment/

9.9 Following his appointment under these terms, John Edwards gave full support to the UK Government plans to reform data protection.[21] This came against the opinions of other UK independent authorities such as the National Data Guardian,[22] the Biometrics and Surveillance Camera Commissioner,[23] the Scottish Biometrics and Surveillance Camera Commissioner,[24] the Equality and Human Rights Commission,[25] and the Norther Ireland Human Rights Commission,[26] who have all expressed serious concerns throughout the years as the UK data protection reform was progressing.

9.10 Further to that, the former Conservative Government fell before being able to pass the UK data protection reform, then known as Data Protection and Digital Information Bill (DPDI Bill). A response to a Freedom of Information Request has revealed that, reacting to this development, John Edwards had sent an internal communication to ICO staff, expressing regret for the falling of the DPDI Bill and announcing that he would have used his discretion to implement in practice the reform.[27] The reform was, eventually, retabled by the new Labour government with the Data (Use and Access) Bill.

---

21 Politico, *UK data chief rejects claims country is ditching privacy rights as 'bullshit'*, at: https://www.politico.eu/article/uk-data-chief-reject-country-ditch-privacy-right-bullshit/

22 National Data Guardian, *Written Evidence by the National Data Guardian (DPDI0008)*, at: https://committees.parliament.uk/writtenevidence/121615/pdf/

23 Office of the Biometrics and Surveillance Camera Commissioner, *The Data Protection and Digital Information (No. 2) Bill Committee*, at: https://bills.parliament.uk/publications/51173/documents/3425

24 Scottish Biometrics Commissioner, *Commissioner reiterates concerns about Data Protection and Digital Information (No 2) Bill to Scottish MP on Westminster Committee*, at: https://www.biometricscommissioner.scot/news/commissioner-reiterates-concerns-about-data-protection-and-digital-information-no-2-bill-to-scottish-mp-on-westminster-committee/

25 Equality and Human Rights Commission, *Written evidence submitted by the Equality and Human Rights Commission (DPDIB38)*, at: https://publications.parliament.uk/pa/cm5803/cmpublic/DataProtectionDigitalInformation/memo/DPDIB38.htm

26 Northern Ireland Human Rights Commission, *Briefing on the Data (Use and Access) Bill [HL]*, at: https://nihrc.org/publication/detail/nihrc-briefing-on-the-data-use-and-access-bill-hl

27

10. ROLE OF THE SUPERVISORY AUTHORITY

10.1 **Section 90 of the Data (Use and Access) Act 2025 introduced a new principal objective, and a number of secondary duties, that the UK supervisory authority must have regard to when carrying out functions under the data protection legislation.** In particular:

10.1.1 The new, principal objective is defined as *"to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest"* and "to promote public trust and confidence in the processing of personal data".

10.1.2 The new, secondary duties are defined as "the desirability of promoting innovation"; "the desirability of promoting competition", "the importance of the prevention, investigation, detection and prosecution of criminal offences", "the need to safeguard public security and national security", and "the fact that children merit specific protection with regard to their personal data"

10.2 These developments are addressed by chapter 2.3.1 "Independent Oversight" of the draft adequacy decision.

10.3 Concerning the new, principal objective, Recital 60 reads that:

"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. 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. These objectives are also mentioned in recital 7 of Regulation (EU) 2016/679".

10.4 Furthermore, and concerning the new secondary duties, Recital 61 reads that:

"Similarly, EU data protection law also balances 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".

10.5 However, the assessment made by the Commission severely underestimates the breadth and scope of these changes.

10.6 Firstly, Section 90 introduces the principal objective and new duties outlined above in the Data Protection Act 2018. Provisions in the DPA 2018 prevail over those of the UK GDPR due to its degradation to "assimilated EU law" (more *supra*, §2). Thus, the role enshrined by Article 51 of the UK GDPR becomes hierarchically subordinated to the new principal objective and statutory duties introduced by Section 90 of the DUAA 2018. This is an intended consequence of the reform, as the UK government stated their intention to introduce an overarching "new statutory framework for [the ICO] objectives and duties", which the ICO "must aim to fulfil when exercising its data protection functions".[28]

10.7 Secondly, the Court of Justice of the European Union has clarified the meaning of the EU GDPR by stating that the main role of a supervisory authority is "ensuring that the GDPR is fully enforced with all due diligence".[29] Contrary to this interpretation, the new "principal objective" introduced by Section 90 of the DUAA 2025 dilutes this responsibility: the objective of securing "appropriate level of protection for personal data" is given equal weight to that of promoting "confidence in the processing of personal data". Further, and because provisions in the Data Protection Act 2018 prevail over those in the UK GDPR, this dilution has the potential to override legally binding case-law established in Schrems II.

10.8 Thirdly, the definition of "appropriate level of protection for personal data" with regard to "the interests of data subjects, controllers and others and matters of general public interest" substantially differs from the formulation of Recital 7 of the EU GDPR, according to which "Natural persons should have control of their own personal data". In his analysis concerning the same subject, Kings Counsel Stephen Cragg wrote that "*it can be seen that the rights of data subjects are given no particular primacy in this formulation and could get lost amongst the range of other issues and interests that must be taken into account*".[30]

---

28 Department of Digital, Culture, Media and Sport, *Data: a new direction - government response to consultation, Chapter 5.2*, at: https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#ch5

29 Court of Justice of the European Union, *Case C-311/18*, at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155

30 Stephen Cragg KC, *IN THE MATTER OF THE DATA PROTECTION AND DIGITAL*

10.9 Finally, the secondary duties established by Section 90 of the DUAA 2025 introduce extra-legal considerations, such as “the desirability of promoting innovation”. This goes beyond the notion, mentioned by the Commission in Recital 61, of balancing “the protection of personal data with several other fundamental rights and objectives”.

INFORMATION BILL, paragraph 56, at: https://defenddigitalme.org/2023/11/28/new-legal-opinion-on-the-data-protection-and-digital-information-bill/

11. PERFORMANCE OF THE SUPERVISORY AUTHORITY

11.1 The draft adequacy decision addresses the performance of the Information Commissioner's Office at Chapter 2.3.2 "Enforcement, including sanctions". In particular:

11.2 In Recital 65, the Commission reports that "the Information Commissioner has handled about 40 000 complaints from data subjects per year".

11.3 In Recital 66 the Commission reports that *"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"*.

11.4 While the numbers are, at least formally, correct, the Commission's assessment fails to meaningfully interpret these findings.

11.5 Commenting on the latest ICO Annual Report (2024/2025),[31] David Erdos, Co-Director of the Centre for Intellectual Property and Information Law (CIPIL) at the University of Cambridge found that:

11.5.1 On the ICO use of enforcement powers, *"there were just 2 UK GDPR fines during the year (which compares to >200 in both Germany and Spain) and that even the number of outcomes resulting in reprimands fell from 31 to just 9 (a 70% reduction)", and "the Report also reveals that the number of reported data breaches which even resulted in a GDPR investigation [...] dropped from a mere 6% to just 3%".*

11.5.2 Furthermore, "*there were only 43 UK GDPR investigations in this year compared to 285 in 2023-24 (in other words, less than 1/5 of the previous year's total), that not a single UK GDPR enforcement notice (the main "appropriate measure" in the UK regime) was issued at all and that even the number of reprimand outcomes (which have no direct legal effect) declined from 31 to just 9 (less than 1/3 of the previous year's total). Meanwhile, just 2 UK GDPR fines were issued totalling £3.8M (compared to 3 fines totalling £13M in 2023/24). Criminal enforcement also decreased by 20% in the case of prosecutions (down from 5 to 4) and by 57% as regards cautions (down from 7 to 3). Similar trends were apparent in the area of e-*

31 David Erdos, *The UK Information Commissioner's Annual Report 2024/25: Surveying a Systematic Trend Away from Adequate Enforcement*, at: https://ukconstitutionallaw.org/2025/07/22/david-erdos-the-uk-information-commissioners-annual-report-2024-25-surveying-a-systematic-trend-away-from-adequate-enforcement/

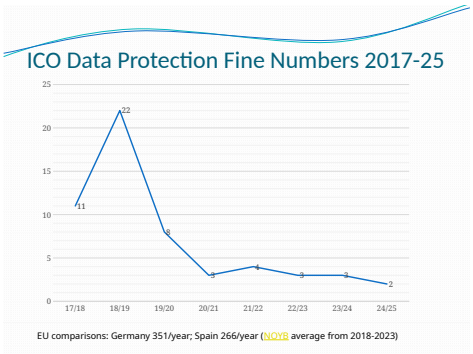
Privacy with fines (and related notices) here down to just 9 and £890K compared to 26 and £2.59M in 2023/24 which again represents an approximate 65% decrease".

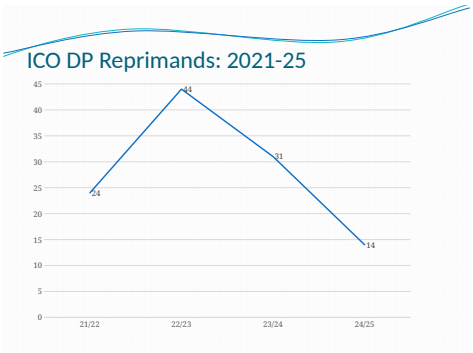
11.5.3 Also, "*the Report revealed that the percentage of breach reports which even prompted an investigation (let alone enforcement action) halved from just 6% to a mere 3%*".

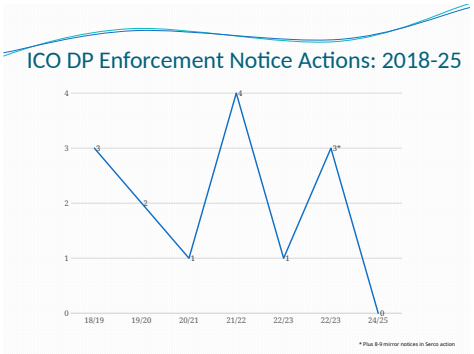
11.6 Finally, and moving to the ICO track record in handling data protection complaints, his analysis points out that *"the number of data protection complaints which received no response during the expected 90 day timeframe sky-rocketed from just 15.2% in 2023/24 to 70% in 2024/25 (a 360% increase)"*. Further, he continues:

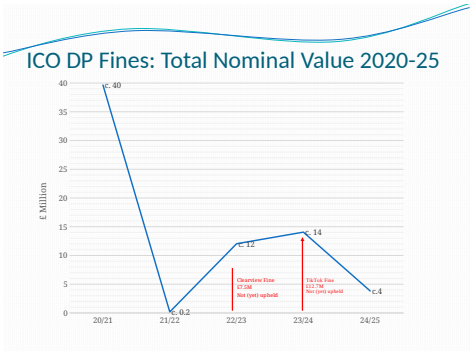
11.6.1 "*Over the same period, the ICO has clearly deprioritised the handling of data protection complaints with the percentage of individuals receiving no response within the three months expected (see UK GDPR, art. 78(2)) ballooning from approximately 15% in 2023-24 to a massive 70% in 2024-25 (a 360% increase). The number of complaints which remained open also increased by over 70% from 9,168 and 15,810. Contrary to what is stated in the Report, this can hardly be explained by "a rising increase in cases" as the complaints received only increased by 6.5%, a figure which is clearly dwarfed by both these other numbers*".

11.7 The severe downward trajectory of the use of Enforcement powers by the ICO post-Brexit can, perhaps, be better appreciated in the graphics below:









11.8 Furthermore, the ICO has formalised a new regulatory approach against public sector that prioritises the use of performative actions such as reprimands over legally-binding enforcement measures. As Open Rights Group Alternative Annual Report on the ICO shows,[32] evidence proves that over-reliance on reprimands lacks deterrence for law-breaker. For instance, The Home Office was issued three consecutive reprimands in 2022 for a number of data protection breaches,[33] recording and publishing conversations with Windrush victims without consent,[34] and a systemic failure to answer to SARs within statutory limits, with over 22,000 requests handled late.[35] Against this background, the ICO issued yet another reprimand to the Home Office in 2024.[36]

11.9 Finally, it must be noted that the ICO has recently refused to use their enforcement powers to take any actions against a data breach that involved the personal details of 19,000 Afghan applicants for relocation to the UK following the Taliban takeover in 2021. This breach is estimated to have put more than 100.000 lives (the applicants and their family members) at risk of harms, and the Defence secretary was "unable to say" if the breach resulted in anyone's death.[37]

32 Open Rights Group, *ICO Alternative Annual Report 2023-24*, at: https://www.openrightsgroup.org/publications/ico-alternative-annual-report-2023-24/

33 Information Commissioner's Office, *Action we have taken: Enforcement action: Secretary of State for the Home Department*, at: https://ico.org.uk/action-weve-taken/enforcement/2022/10/secretary-of-state-for-the-home-department/

34 Information Commissioner's Office, *Action we've taken: Enforcement action: Secretary of State for the Home Department (Home Office)*, at: https://ico.org.uk/action-weve-taken/enforcement/2022/08/secretary-of-state-for-the-home-department-home-office/

35 Information Commissioner's Office, *Action we've taken: Enforcement action: Secretary of State for the Home Department (Home Office)*, at: https://ico.org.uk/action-weve-taken/enforcement/2022/09/secretary-of-state-for-the-home-department-home-office-1/

36 Information Commissioner's Office, *Action we've taken: Enforcement action: Home Office*, at: https://ico.org.uk/action-weve-taken/enforcement/2024/03/home-office/

37 BBC, *Defence secretary 'unable to say' if anyone killed after Afghan data breach*, at: https://www.bbc.co.uk/news/articles/c1k8yvj89kyo

12. MONITORING AND REVIEW OF THE LEVEL OF PROTECTION AFFORDED BY UK DATA PROTECTION LAW

12.1 If adopted as it is, the draft UK adequacy decision would "apply for a period of six years as of its entry into force"[38] and, within that period, *"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"*.[39] To this purpose, the Commission also commits to meet "with relevant representatives from the UK authorities, including the Information Commission", and expects "the UK to provide comprehensive information on all aspects relevant for the adequacy finding". Further, the Commission clarifies that they will *"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"*.

12.2 The commission reaches this decision by noting, in their conclusions, 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 [...] that is essentially equivalent"*, that "the oversight mechanisms and redress avenues in United Kingdom law continue to enable infringements to be identified and punished in practice"; and 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"*.

12.3 As this analysis has demonstrated, these conclusions are moving from the wrong premises. In turn, the review and monitoring mechanism established by the draft adequacy determination appears underwhelming and ill-suited to ensure an effective monitoring and timely reaction to relevant developments.

12.4 The Retained EU law (Revocation and Reform) Act (REUL) 2024, Regulations 2023/1417 and the Data (Use and Access) Act (DUA) 2025 have all introduced changes with the potential to significantly reduce the level of protection afforded to personal data in the UK. Oversight mechanisms and redress avenues in the UK are showing manifest signs of deterioration and paralysis, and it is at least dubious that UK data protection law still provide an "essentially equivalent level of protection" to the EU. Lacking

38 Regulation (EU) 679/2016, Recital 112

39 Ibid

case-law or updated guidance that reflects these changes, the impact of these developments has yet to be fully measured.

12.5 Furthermore, The DUA Act has give the UK government wide and discretionary powers that they could use to further divergence from EU data protection law and lowering protection in key areas such as: restrictions under Article 23 and in particular exemptions from the purpose limitation principle; lawful grounds for processing; prohibition to the processing of special category data; and restrictions to onward transfers of personal data. The potential impact of these powers is magnified by the removal of fundamental rights and the principle of supremacy of EU law from the UK statute book, and the expansive interference with the rights of individuals that this allows.

12.6 Finally, it is worth mentioning that the nature of delegated legislative powers allows for sudden and radical changes to UK data protection law. Also known as "Henry VIII" powers, these clauses are considered "constitutionally anomalous"[40] in the United Kingdom as they allow the government to override primary legislation (i.e. the law as enacted by Parliament) via secondary legislation (i.e. Statutory Instruments written by the government). Contrary to most delegated powers in continental Europe, there is no formal hierarchy that requires secondary law to be compatible with primary law: insofar the government does not exercise legislative power beyond the mandate given by the Henry VIII clause (i.e. unless the statutory instrument is *ultra-vires*), secondary legislation can amend primary legislation and will prevail in case of incompatibility.

12.7 Despite the breadth of these powers, scrutiny and procedural safeguards are minimal, and secondary legislation becomes law within a period of 28 to 40 days.

12.8 In particular, secondary legislation subject to the affirmative procedure is debated in Delegated Legislation Committees (DLCs). According to the Institute for Government:

12.8.1 "Debates in DLCs can last up to 90 minutes (or 150 minutes if the piece of secondary legislation relates only to Northern Ireland), but are usually much shorter. DLCs typically debate and agree a motion that they have 'considered' a piece of secondary legislation without holding a formal vote. Once this has happened, a motion to approve a piece of secondary legislation is put 'forthwith' to the House of Commons. This means MPs will vote on whether to approve the instrument(s) on a different day to the DLC, and without debate."[41]

40 Delegated Powers and Regulatory Reform Committee, *Democracy Denied? The urgent need to rebalance power between Parliament and the Executive*, at: https://publications.parliament.uk/pa/ld5802/ldselect/lddelreg/106/10602.htm

12.9 Secondary legislation subject to the "negative resolution procedure", instead, is signed off by the relevant minister and they becomes law unless it is actively voted down by Parliament within a set period, usually 40 days.

12.10 The absence of substantive scrutiny is reflected by data: according to the Institute for Government, the House of Commons has not rejected a single Statutory Instrument since 1978 under the affirmative resolution procedure, and since 1979 for the negative resolution procedure. These figures are confirmed by the Hansard Society.[42]

41 Institute for Government, *Secondary legislation: How is it scrutinised?*, at: https://www.instituteforgovernment.org.uk/explainer/secondary-legislation-scrutiny

42 Hansard Society, *Delegated legislation: the problems with the process*, at: https://www.hansardsociety.org.uk/publications/reports/delegated-legislation-the-problems-with-the-process