Subject: Urgent Concerns Regarding the EU-UK Adequacy Decisions and the Erosion of Data Protection Standards

Dear Commissioner McGrath,

We, the undersigned civil society organisations, write to express our deep concerns regarding the continued adequacy status granted to the United Kingdom (UK) despite its growing divergence from the standards required under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). These risks are heightened by reforms that would further regulatory divergence in the UK, and threaten the fundamental rights protections of people in the EU as mandated by the Charter of Fundamental Rights of the European Union and the EU-UK Withdrawal Agreement (the Withdrawal Agreement).

Since it was granted adequacy status under the EU GDPR and Law Enforcement Directive, the UK has seen a sustained and systemic erosion of privacy and data protection. This degradation would be furthered by the UK Data (Use and Access) Bill, pursued in the name of simplification, as repeatedly pointed out by the European Parliamentary research service[1], law firms[2], data protection specialists[3] and UK parliamentarians.[4] The Northern Ireland Human Rights Commission has raised serious concerns about the UK Data Bill's compatibility with the non-diminution commitment in Article 2 of the Windsor Framework, as well as the UK's commitments under the Rights, Safeguards, and Equality of Opportunity chapter of the Belfast (Good Friday) Agreement.[5]

There is a substantive risk that the UK adequacy decisions could be struck down by the Court of Justice of the European Union (CJEU) if the UK's current data protection framework continues to be degraded. **The Commission needs to act decisively, or risks leaving the UK adequacy decisions open to a judicial challenge.** A judicial invalidation of the UK adequacy decision would also disrupt key areas of EU-UK cooperation, including the Trade and Cooperation Agreement (TCA), the Windsor Framework, and the UK's participation in Horizon Europe. This would directly set back the Commission's and Member States' efforts to strengthen ties and pursue further collaboration with the UK.

We note that the 'sunset clause' in the EU's adequacy decisions for the UK, initially set to expire in June 2025, has been extended by six months. On 5 May 2025, the European Data Protection Board issued Opinion 06/2025, accepting the Commission's proposed six-month technical

1 https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769528/EPRS_ATA(2025)769528_EN.pdf
2 https://bateswells.co.uk/the-data-use-and-access-bill-areas-of-risk-to-the-continued-free-flow-of-data-from-the-eu-to-the-uk/
3 https://amberhawk.typepad.com/amberhawk/2025/02/index.html
4 https://hansard.parliament.uk/Lords/2024-11-19/debates/6B196F71-312C-4957-AF14-98B66C5DBEE4/Data(UseAndAccess)Bill(HL)
5 See 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

extension as a one-off exception to allow the UK's legislative process to conclude. Crucially, the EDPB emphasised that this extension should not be further prolonged, and called on the Commission to monitor the situation closely and take appropriate action if fundamental rights are endangered. We contend that **this extension must not be granted unless the UK's data protection framework ensures an equivalent level of protection to that guaranteed under EU law.** Doing otherwise would signal to third countries that adequacy decisions can be maintained regardless of genuine compliance with EU data protection standards. This would encourage regulatory competition at the expense of fundamental rights, undermining the integrity of the Single Market and putting EU businesses at a disadvantage.

The Annex to this letter provides detailed evidence of the UK's increasing divergence from EU data protection standards, illustrating why the UK risks no longer offering an equivalent level of protection as required by EU law.

Urgent Steps the Commission Must Take

Allowing third countries such as the UK to benefit from unrestricted personal data flows with the EU while simultaneously weakening legal safeguards at home does not only endanger the rights of people in the EU—it also undermines the credibility of the EU's data protection framework, exposes EU businesses to unfair competition, and devalues the Union's regulatory leadership on the global stage.

The UK Government's proposed reforms and recent actions threaten to imperil the UK's data and privacy protections. This status of affairs will fuel uncertainty and threaten individuals and businesses alike. **The European Commission cannot afford to wait for the CJEU to intervene**; it must act swiftly and decisively to protect fundamental rights and uphold its credibility as both the guardian of the EU's legal order and a global leader in digital rule-making. We urge the Commission to take immediate steps to:

1. Re-evaluate the UK's adequacy status in light of its recent and ongoing privacy and data protection-eroding measures.
2. Commit to a transparent process in which civil society concerns are meaningfully considered, in line with the concerns expressed by the EDPB in its letter to the European Commission regarding the review of the eleven adequacy decisions adopted under Directive 95/46/EC.
3. Ensure that adequacy decisions are rigorously enforced, suspended, or withdrawn where necessary to ensure respect of criteria emphasised by the CJEU.
4. **Reaffirm the EU's commitment to fundamental rights** by taking a consistent and principled approach to all adequacy decisions, including those concerning the UK, the US, and other third countries.

We remain at your disposal for further discussions and urge you to act with urgency to protect the integrity of the EU's legal framework.

Sincerely,

European Digital Rights (EDRi)
Statewatch
Electronic Frontier Norway
Access Now
Politiscope
Privacy International
IT-Pol Denmark
Deutsche Vereinigung für Datenschutz e.V. (DVD)

Annex: Key Developments Undermining Privacy and Data Protection in the UK

1. The Data (Use and Access) Bill

The UK Data Bill would represent a systematic weakening of privacy and data protection safeguards, introducing legislative changes that significantly reduce individuals' rights and the accountability of entities processing personal data. Among its most concerning aspects are:

- Broad exemptions from key data protection principles, which would grant government and law enforcement agencies expansive access to personal data;
- Diminishing the right to not be subject to automated decision-making under the UK GDPR so that solely automated decision-making involving the majority of personal data (with the exception of special category personal data) will no longer be subject to the same safeguards and restrictions that exist in EU law;
- Amending protections in the UK GDPR's data transfer provisions in a push to facilitate data transfers to jurisdictions lacking EU-equivalent protections, thus potentially making the UK a 'data laundering hub' that tech companies can use to bypass EU data protection law;
- Extensive delegated legislative powers allowing UK ministers to override legal provisions with minimal parliamentary scrutiny, including in relation to data transfers, special category data processing and the lawful bases for processing data;[6]
- Powers for the UK government to nominate, dismiss and set the salary of the non-executive members of the UK Data Protection Authority, who would then have the power to hire, fire, and determine terms and conditions of employment of the executive members. Since non-executive members are directly accountable to the Secretary of State, the government would have scope to interfere with the functioning of the UK data protection authority.

2. Other legislative initiatives

The UK Border Security, Asylum and Immigration Bill would compel the sharing of border control and custom data with UK intelligence services.[7] These provisions build upon the UK Data Bill's powers to exempt law enforcement and national security processing from UK GDPR and LED requirements. At the discretion of UK Ministers, EU individuals' personal data, would be subjected to UK intelligence services and counter-terrorism legislation. **Such developments are not only incompatible with the fundamental principles of the GDPR and the LED, but would also affect data shared under the EU-UK TCA and the Windsor Framework.**

Likewise, the UK's Public Authorities (Fraud, Error and Recovery) Bill would empower UK Ministers to compel banks, regardless of whether they are based in the UK, to provide information on the bank accounts of individuals. The Bill does not require Ministers to provide evidence of wrongdoing, and orders to disclose such information could be based on speculative discretion around those individuals' eligibility for social security. The Public Authorities Bill also builds on Data Bill's provisions that would remove safeguards around automated decision-making, with the effect of allowing the use of algorithmic scanning methods to process bank accounts' data and identify suspects to prosecute.[8]

---

6 See Open Rights Group, *Briefing: The Data Use and Access Bill (Second Reading House of Commons)*, at: https://www.openrightsgroup.org/publications/briefing-the-data-use-and-access-bill-second-reading/

7 See See House of Commons, *Border Security, Asylum and Immigration Bill*, at: https://bills.parliament.uk/bills/3929

8 See Big Brother Watch, Briefing on the Public Authorities (Fraud, Error and Recovery) Bill for Committee Stage in the House of Commons, at: https://bigbrotherwatch.org.uk/wp-content/uploads/2025/02/Big-Brother-Watch-Committee-Stage-Briefing-on-PAFER-Bill.pdf

3. Concerns over the Independence of the ICO

Provisions in the UK Data Bill would give new powers to the UK government to appoint, dismiss and set the salary of all the members of the Board of the UK data protection authority. Further, the Bill seeks to create a statutory duty on the ICO to consider innovation while performing its regulatory functions.[9] This would provide the UK government with a statutory footing to impose its deregulatory agenda[10] in the technology sector, thus placing inappropriate pressure on the ICO and arguably undermining its ability to act independently.[11] Indeed, **the UK government's politicisation of regulatory bodies has already raised alarm domestically**, with the dismissal of the Chair of the Competition and Markets Authority for his failing to align with the government's political priorities.[12]

These threats to the independence and effectiveness of the UK's Information Commissioner's Office (ICO) have been highlighted in the UK parliament during the scrutiny of the bill,[13] but the UK government opposed any attempts to address them. We are concerned that, following the implementation of the UK's Data Bill, the ICO will not meet the standards set in the UK's 2021 adequacy decisions, including that they must act: '*with complete independence [...], remain free from external influence, whether direct or indirect, in relation to those tasks and powers, and neither seek nor take instructions from anyone.*'[14]

In 2024, the ICO published statistics which revealed that they had only taken regulatory action on 1 complaint out of the 25,582 which they had received[15], favouring actions that lack the force of law when they did respond. We are concerned that the ICO's overreliance on actions lacking legal force when responding to complaints is a symptom of the political pressure the ICO is receiving to not obstruct innovation or growth for UK businesses at the expense of UK data subjects' effective right of redress.

Another example of how competing political pressures the ICO is under can affect its independence and effectiveness can be found in a case involving the UK's police cloud infrastructure, particularly in light of the Commission's 2021 adequacy decisions, which stated that particular attention would be paid to the UK's implementation of the UK-US Cloud Act.[16].. An independent investigation carried out by the Scottish Biometric Commissioner revealed that the sovereignty of UK policing data hosted on the Microsoft Azure public cloud was not being guaranteed.[17] However, the ICO refused to intervene despite calls from the Scottish

9 See Data Use and Access Bill, at s.90(3): https://publications.parliament.uk/pa/bills/cbill/59-01/0199/240199.pdf

10 See Department of Science Innovation and Technology press release: https://www.gov.uk/government/news/technology-secretary-kickstarts-plan-to-bin-barriers-and-back-innovators-to-reap-rewards-of-new-tech-over-next-decade-and-drive-plan-for-change

11 See House of Lords, Data Use and Access Bill [HL], Volume 843 per Lord Holmes's comments at column 141 at: https://hansard.parliament.uk/lords/2025-01-28/debates/9BEB4E59-CAB1-4AD3-BF66-FE32173F971D/Data(UseAndAccess)Bill(HL)

12 See 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

13 See House of Lords, *Data Use and Access Bill [HL]*, Volume 841 per Lord Freyberg's comments at column 183 at: https://hansard.parliament.uk/lords/2024-11-19/debates/6B196F71-312C-4957-AF14-98B66C5DBEE4/Data(UseAndAccess)Bill(HL)

14 See Commission Implementing Decision (EU) 2021/1772of 28 June 2021 at recital (87): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D1772#ntr20-L_2021360EN.01000101-E0020

15 See Information Commissioner's Office, response to FOIA IC-353505-C3D8, at: https://www.whatdotheyknow.com/request/proportion_of_complaints_you_rec/response/2895145/attach/3/IC%20353505%20C3D8%20Response%20Letter.pdf?cookie_passthrough=1

16 See Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 at recitals (153) – (156): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D1772

17 See ComputerWeekly, ICO prompts confusion over police cloud legality, at: https://www.computerweekly.com/news/366566869/ICO-prompts-confusion-over-its-position-on-police-cloud-legality

Commissioner to investigate,[18] citing concerns that ruling on the legality of the police cloud infrastructure would frustrate the operation of the UK-US Cloud Act Agreement.[19] In a related development, the ICO was recently summoned by the UK government to a roundtable, where the Information Commissioner reportedly 'set out a raft of new measures that support the Government's growth agenda'.[20] These examples raise serious concerns about the extent to which political pressures may be affecting the ICO's regulatory independence and decision-making.

A regulatory authority that fails to act independently, does not ensure meaningful enforcement, and does not provide meaningful access to redress cannot offer the necessary guarantees that individuals' rights will be upheld, nor can it satisfy the requirement of 'independent oversight' under Article 45(2)(b) of the GDPR.

4. Retained EU Law (Revocation and Reform) Act 2023

Case-law in the UK suggests that all the exemptions to the right to exercise data protection rights provided by the Data Protection Act 2018 may be illegal—with the sole exclusion of the Immigration Exemption, whose illegality was remedied by a Court order. However, following enactment of the Retained EU Law Act, the UK GDPR has lost its primacy under EU law. As pointed out by prominent legal practitioners in the UK,[21] **this undermines the applicability of Article 23 of the UK GDPR, allowing key principles and data protection rights to be overridden or disproportionately restricted**. This issue was raised during the UK Parliamentary debate, but the UK government has obstructed Lords' attempts to remedy this state of affairs.

5. Reforms to the UK's Investigatory Powers Act 2016

The UK's Investigatory Powers Act 2016 (IPA) permits and facilitates the interception of, and access to, data by law enforcement and intelligence agencies. This regime has known shortcomings in respect of its compatibility with international human rights law (a relevant consideration for adequacy decisions), including a failure to properly allow for people to exercise their rights.[22] Similar concerns were raised by both the European Data Protection Board[23] and the European Parliament[24] ahead of the 2021 adequacy decisions.

In the UK's 2021 adequacy decisions, the Commission relied on the UN Special Rapporteur on the right to privacy's 2018 report which observed that the UK's law enforcement and national security agency representatives understood that privacy needs to be a primary consideration for

18 See ComputerWeekly, UK data regulator should investigate police cloud deployments, at: https://www.computerweekly.com/news/366592229/UK-data-regulator-should-investigate-police-cloud-deployments

19 See Scottish Biometrics Commissioner, at: https://www.biometricscommissioner.scot/media/2wtnw1ro/letter-to-andrew-hendry-police-scotland-re-desc-december-2023.pdf

20 See ICO, Package of measures unveiled to drive economic growth, at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/package-of-measures-unveiled-to-drive-economic-growth/ See also ICO, How our approach to regulation is supporting economic growth, at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/how-our-approach-to-regulation-is-supporting-economic-growth/

21 See E. Duhs, "The Data (Use and Access) Bill – areas of risk to the continued free flow of data from the EU to the UK", Bates Wells (2nd December 2024) (available at: https://bateswells.co.uk/the-data-use-and-access-bill-areas-of-risk-to-the-continued-free-flow-of-data-from-the-eu-to-the-uk/)

22 See Privacy International's submission to the Human Rights Committee ahead of the eighth periodic report on the United Kingdom (140th session, March 2024), https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2FCCPR%2FCSS%2FGBR%2F57465&Lang=en

23 EDPB, 'Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom', 13 April 2021, https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf, 166.

24 European Parliament, Resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom, 2021/2594(RSP), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0262

surveillance measures.[25] However, **recent amendments to the IPA have indicated that this position has now been overridden by a desire for more intrusive, privacy-effacing surveillance powers**. Rather than mitigating the risks arising from the IPA, the UK has has instead introduced, with the Investigatory Powers (Amendment) Act 2024,[26] new powers to secretly compel telecommunications operators to undermine data security and impinge people's rights (e.g. by requiring the removal of encryption).[27] The 2021 position therefore reflected a high water-mark in terms of the UK's approach to surveillance powers, which has since been eroded, threatening the UK's adequacy. For example, the UK regime now includes the concept of bulk personal datasets with 'low or no reasonable expectation of privacy' which are vaguely defined and subject to lower thresholds for agency access, including an insufficient form of authorisation.[28] This is most probably not in accordance with the definition and requirements established by the European Court of Human Rights (ECtHR).[29]

6. The use of Technical Capability Notices to Undermine Encryption

In February 2025, it was reported[30] that the UK government had issued a Technical Capability Notice (TCN) to Apple, believed to have been instructing the company to facilitate access to encrypted user data stored on iCloud. **TCNs compel companies to provide the ability to remove encryption at the government's request, which not only creates systemic vulnerabilities but also poses a direct threat to the integrity and confidentiality of digital communications.** These notices are issued in secrecy, with little to no transparency, oversight, or independent redress mechanisms, effectively enabling the UK government to implement de facto backdoors while circumventing established legal safeguards. The recent push to force encrypted messaging services to comply with scanning obligations, despite strong warnings from the industry about the potential security risks, underscores the growing divergence between UK policy and the core principles of necessity and proportionality enshrined in EU law.[31]

The absence of meaningful judicial oversight for TCNs, alongside the UK's increasingly hostile stance towards encryption, exacerbates concerns about the ongoing adequacy of UK data protection standards. Not only does this jeopardise the rights of individuals, but it also exposes EU businesses and institutions to heightened cybersecurity risks, including vulnerability to hacking, fraud, and state-sponsored cyber threats. Moreover, the ECtHR has already ruled that the mandating of backdoors to encryption is incompatible with the right to private life under Article 8 of the European Convention on Human Rights (ECHR).[32]

25 See Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 at recital (184): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D1772

26 See 'Joint Briefing on the Investigatory Powers (Amendment) Bill' (January 2024), https://www.openrightsgroup.org/publications/joint-briefing-on-the-investigatory-powers-amendment-bill/ and Privacy International's response to Home Office consultation on codes of practice under the Investigatory Powers (Amendment) Act 2024 (January 2025), https://www.privacyinternational.org/advocacy/5512/pi-response-home-office-consultatation-codes-practice-under-investigatory-powers

27 Both the ECtHR and several UN bodies have recognised that end-to-end encryption is fundamental to a number of human rights, see pp24-26 of Privacy International's response to Home Office consultation (supra) for a summary.

28 https://www.gov.uk/government/consultations/investigatory-powers-amendment-act-2024-codes-of-practice-and-notices-regulations

29 In *Benedik v Slovenia*, the ECtHR reiterates that "private life is a broad term not susceptible to exhaustive definition" which includes "a zone of interaction of a person with others, even in a public context" (para. 100) and thus, supports a wide scope of the reasonable expectation of privacy in the digital age, which the UK concept of bulk personal datasets with no or low expectation of privacy is likely contradicting. See https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-182455%22]}

30 "U.K. orders Apple to let it spy on users' encrypted accounts" (Washington Post, 7 February 2025), https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/

31 "UK amends encrypted message scanning plans" (BBC, 19 July 2023), https://www.bbc.co.uk/news/technology-66240006

32 See Podchasov v Russia (App. No. 33696/19) (13 February 2024) (European Court of Human Rights) at para. 80

This case illustrates the extraterritorial nature of TCNs, as the UK Government has reportedly sought to undermine encryption not just for UK users, but for all iCloud users worldwide. This could have **far-reaching consequences for the privacy and security of individuals outside the UK, raising serious questions about the compatibility of such measures with EU data protection law**.[33]

7. Unregulated use of live facial recognition technology in the UK

Police forces across the UK are trialling or using live FRT despite the lack of clear lawful authorisation for doing so.[34] In May 2023, the UK Biometrics and Surveillance Camera Commissioner critiqued the very limited rules that apply to public space surveillance by the police and noted that oversight and regulation in this area is incomplete, inconsistent and incoherent.[35]

Not only does UK practice appears to be in conflict with EU standards as contained in the AI Act, but there is also evidence of biometric data collected for passport or immigration databases (including by facial recognition technologies) being re-purposed for law enforcement[36] without effective oversight, transparency, or mechanism to assess necessity and proportionality.[37] **This directly affects EU individuals whose data is found in UK immigration databases.**

33 Including suggestions that it may precipitate a Schrems-II like decision, see: I. Kouvakas, 'You Can't Have Your Apple and Eat It Too: Decryption Orders and the Perilous Future of U.K. Data Adequacy', U.K. Const. L. Blog (13th March 2025) (available at https://ukconstitutionallaw.org/))

34 "First permanent facial recognition cameras to go up in London despite 'dystopian' warning" (Metro, 26 March 2025), https://metro.co.uk/2025/03/26/new-big-brother-cameras-announced-london-despite-dystopian-warning-22790959/

35 "The Commissioner discusses the new era for live facial recognition after the Coronation" (17 May 2023), https://videosurveillance.blog.gov.uk/2023/05/17/the-commissioner-discusses-the-new-era-for-live-facial-recognition-after-the-coronation/

36 "Police Secretly Conducting Facial Recognition Searches of Passport Database" (Liberty Investigates, 8 January 2024) https://libertyinvestigates.org.uk/articles/police-secretly-conducting-facial-recognition-searches-of-passport-database/

37 As is required: see *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II)*, CJEU case C-311/18 (July 2020), para 184.