European Parliament

# Navigating challenges to UK data adequacy

The United Kingdom (UK) adequacy decisions are set to expire on 27 June 2025, unless the European Commission reaffirms that the UK continues to ensure an 'essentially equivalent' level of data protection to the EU's. Critics raised concerns that recent and ongoing UK reforms could jeopardise the renewal of these decisions.

## Legal and economic background

According to the prevailing interpretation of the EU **General Data Protection Regulation** (GDPR), operators may only transfer personal data from the EU/European Economic Area (EEA) to a non-EU/EEA ('third') country if:

1. the Commission formally determined by way of an adequacy decision that the third country ensures an '**essentially equivalent**' level of data protection to that of the EU,
2. the exporter deploys alternative transfer mechanisms and, as appropriate, 'supplementary measures' to compensate for the third country's lacunae in protection, or
3. Article 49 derogations (of the GDPR) apply.

A sound **adequacy decision** enables companies to transfer personal data conveniently and cost-effectively to designated third countries with little administrative burden. Besides comprehensive adequacy decisions, the Commission can also adopt bespoke or partial adequacy decisions. Where no adequacy decision or superior international agreement is in place, operators would need to use **alternative transfer mechanisms**, conduct transfer risk assessments, and, as appropriate, deploy '**supplementary measures**' to ensure an 'essentially equivalent' level of data protection. Companies would face high costs and legal uncertainty in compensating for data protection deficits, not least given the UK's extensive intelligence powers. Additionally, some alternative instruments are inherently costly/cumbersome or still under development. While many companies resort to the standard contractual clauses (SCCs) as a precautionary measure if adequacy decisions expire or lose validity, a robust and reliable adequacy decision presents the commercially preferred option, as it provides welcome reassurance. **Article 49 derogations** are (arguably) narrow in scope and cannot serve as a cure-all. Under the Law Enforcement Directive, personal data may be transferred to third countries based on an adequacy decision, appropriate safeguards, or derogations.

If the Commission does not renew the decision, it will expire, and data transfers from the EU to the UK will become more complex and costly for businesses. A November 2020 study estimated the costs of 'inadequacy' conservatively at around GB£1 billion to GB£1.6 billion (€1.116 billion to €1.7856 billion based on the European Central Bank average reference rate in November 2020) for UK firms. These costs would stem from companies implementing SCCs as alternative transfer mechanisms if no follow-up adequacy decision had been reached after the expiration of the post-Brexit interim data bridge. In its March 2023 impact assessment accompanying the UK Data Protection and Digital Information Bill, the former Conservative government estimated an economic impact of GB£410 million (range between GB£190 million and GB£460 million) in one-off compliance costs, and an annual cost of GB£240 million (range between GB£210 million and GB£420 million) in lost export revenue. Once appraised over a 10-year period, the estimated Net Present Value (2019 prices, 2020 present value) of EU adequacy being continued is GB£2 billion (range between GB£1.6 billion and GB£3.4 billion). Both estimates are deemed conservative. Divergences result from different methodologies and assumptions, including regarding the necessary compliance action to set up SCCs, the costs and cost-structure for implementing SCCs, the assumption that many large businesses have already implemented SCCs, and the number of companies affected.

## Challenges to UK adequacy

Article 45(2)(a) GDPR requires the Commission to review relevant legislation and its implementation, including data protection rules, law enforcement acts and national security laws, to assess the UK's adequacy. There is disagreement on whether the Commission is required to assess the laws and practices


Author: Hendrik Mildebrath, Members' Research Service
PE 769.528 – March 2025

concerning direct government access to data for national security purposes even when authorities do not access data indirectly by placing obligations on private entities to retain and share data. In its *Schrems II* judgment, the Court of Justice of the European Union (CJEU) tested United States rules on direct surveillance measures (Executive Order 12333) against the EU data protection and privacy *acquis*. The CJEU did not follow suggestions by the Advocate General to apply the more lenient human rights standard instead of the EU fundamental rights standard. Academics counter the claim that the EU applies double standards to the review of direct access by third countries and Member States by emphasising that the Member States are bound by the European Convention on Human Rights.

**Pending Data (Use and Access) Bill:** The Data (Use and Access) Bill follows two bills introduced by previous Conservative governments. The reforms to parts of the UK's data protection and privacy framework are meant 'to support economic growth and modern digital government' and 'address a lack of clarity in existing legislation that impedes the safe development and deployment of some new technologies'. The provisions facilitating the flow and use of personal data for law enforcement and national security purposes seek to enhance the work of relevant agencies in the public interest, including by 'removing unnecessary complexity and processes, and reducing differences across the data processing regimes'. Digital rights advocates and groups identified a range of provisions that raise new or deepen existing adequacy concerns, including:

- the removal of protections in relation to automated decision-making;
- the reduction of transparency, notably in the area of artificial intelligence;
- the conferral of excessive powers on the Secretary of State to override safeguards (risk of function creep);
- the reduction of accountability over how data are shared and accessed for law enforcement and other public purposes.

**Investigatory Powers (Amendment) Act:** The key objective of the Investigatory Powers (Amendment) Act 2024 was a targeted reform of the Investigatory Powers Act 2016 (IPA 2016) in order 'to support the intelligence services in keeping pace with a range of threats against a backdrop of accelerating technological advancements, which provide new opportunities for criminals such as terrorists, hostile state actors, child abusers, and criminal gangs'. The IPA 2016 (dubbed the 'Snoopers' Charter' by critics) governs the interception of communications, the retention and acquisition of communications data, equipment interference, and the retention and examination of bulk personal datasets. The amendment bill of 2024 faced cross-sectoral concerns from digital rights organisations, academics and the tech industry. The House of Commons adopted few substantive amendments; much of the criticism submitted to the Public Bill Committee is therefore still relevant for the final act. Changes criticised include:

- the introduction of an ambiguously defined category of bulk personal data with 'low or no reasonable expectation of privacy', which intelligence services may retain with only categorical, not specific, judicial approval;
- the exculpation of civil servants from the offence of 'unlawfully obtaining communications data', on the basis that the civil servant obtained the data with 'lawful authority' where that data had previously been made available to the public or a section of the public;
- the conferral of power on the Secretary of State to require telecommunications operators to notify service and product changes, which may encourage greater use of technical capability notices, which, if approved, could hinder privacy and security improvements to facilitate surveillance operations;
- the requirement for recipients of data retention, national security, or technical capability notices to continue providing intelligence assistance even if the matter is referred back to the Secretary of State for review, provided that access was granted before the notice was issued.

The UK Home Office is holding a public consultation on updates to the codes of practice and notices regulations accompanying the amended IPA 2016. As with the 2024 reform, the envisaged operational details are facing criticism.

**Other pre-existing issues:** Criticism levelled at the IPA 2016 and other pre-existing data laws, agreements, and practices still applies. Reportedly, the UK Home Secretary has recently issued a technical capabilities notice to Apple, which then stopped offering advanced encrypted cloud storage in the UK.