The Conservative European Forum – Written Evidence (DAT0018)

House of Lords European Affairs Committee
UK-EU data adequacy Inquiry

Background

The Conservative European Forum (CEF) was launched in January 2021 under the leadership of the Rt Hon. Sir David Lidington KCB CBE as Chair and Stephen Hammond MP as Deputy Chair. The Forum is committed to strengthening political, economic, social, environmental, and security cooperation between the UK and European democracies.

In February 2023, CEF initiated a comprehensive year long inquiry into the Trade and Cooperation Agreement and the ongoing UK-EU relationship. During this inquiry, the Forum collected insights and heard evidence from various companies, trade and business organisations, and other experts with direct experience and knowledge of UK-EU relations. A theme that arose consistently, and across a range of sectors and industries, is the importance of maintaining data adequacy with the European Union, which was linked directly to both economic prosperity and national security. In March 2024, CEF published a report with its findings and a list of practical and industry-led recommendations. A key recommendation for the UK Government is to ensure that any forthcoming legislation avoids significant divergence from EU data protection standards. This could jeopardise the continuation or renewal of the EU's data adequacy decisions for the UK.

Representatives of the Conservative European Forum also met with a delegation from European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) to discuss data adequacy in November 2022.

What is your assessment of the existing adequacy arrangement underpinning data flows between the UK and the European Union? What is your assessment of the value of the EU's adequacy decisions to UK organisations?

The current data adequacy framework between the UK and the EU was established through two distinct data adequacy decisions — one under the

General Data Protection Regulation (GDPR) and the other under the Law Enforcement Directive (LED) — adopted by the European Commission on 28 June 2021.[1] The GDPR decision primarily addresses commercial activities, while the LED decision enables security-related data exchanges between law enforcement agencies.

These decisions are pivotal as they allow for smooth personal data transfers between the EU and the EEA and the UK, recognising the UK's data protection laws as providing 'essentially equivalent' protection compared to EU law. This equivalency is vital for fostering economic growth and enhancing security cooperation post-Brexit, enabling businesses to function internationally without additional data protection hurdles, which would otherwise bring considerable administrative and financial costs. According to statistics from the UK Government's Explanatory Framework for Adequacy Discussions, trade in data-enabled services between the UK and the EU was valued at £127 billion in 2018.[2]

The CEF Inquiry heard from a range of industries how the arrangements are especially critical in sectors heavily reliant on data, such as financial services and research collaboration. Financial institutions, for example, depend on uninterrupted real-time data flows for transaction processing, fraud prevention, and adherence to international regulatory standards. The significance of maintaining data adequacy has grown since the UK's reassociation with Horizon Europe and the increasing number of research collaborations with EU Member States.

The EU has granted data adequacy decisions to a number of other third countries, including Andorra, Argentina (only commercial organisations), the Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, the UK, and South Korea.

The UK is an outlier for two reasons. Firstly, it is the only third country whose data adequacy decisions included a sunset clause. This clause not only limits the duration of the agreement to four years but also signals the European Commission's intent to closely monitor the UK's progression in data policy and its potential divergence from EU standards. This is particularly relevant given the potential implications of the Data Protection and Digital Information Bill. The inclusion of a sunset clause

[1] The European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 whether a country outside the EU offers an adequate level of data protection.
[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872228/A_-_Cover_Note.pdf

possibly reflected the low levels of trust between the UK and the EU when the decision was granted and introduces an additional layer of uncertainty for businesses in both jurisdictions.

Secondly, the UK stands out as the sole third country granted an adequacy decision under the Law Enforcement Directive (LED) that facilitates law enforcement data exchanges. This decision recognises that the UK provides adequate protection for personal data transferred from EU entities involved in law enforcement activities such as the prevention, investigation, detection, or prosecution of criminal offenses, or the execution of criminal penalties.[3] The importance of this adequacy in law enforcement cannot be overstated, as it enables the UK to maintain access to essential databases. These include databases for criminal records, DNA, fingerprints, vehicle registration data (Prüm), and Passenger Name Record (PNR) data.

In February 2020, the UK set out its negotiation aims to secure an agreement on law enforcement cooperation with the EU, seeking capabilities similar to SIS II. [4] However, the UK no longer has access to the SIS II and European Commission has expressed that it is legally unfeasible for a non-Schengen third country to engage with the EU through the SIS II database.[5]

SIS II is the largest EU-wide security database containing biometric data, as well as alerts on vulnerable or sought after people (including missing persons) and on certain property, including passports, vehicles, banknotes, and firearms. In a previous report by this committee, it was noted that in 2019, UK police forces had checked SIS II 603 million times.[6]

International partnerships represent the second phase of the International Law Enforcement Alerts Platform (ILEAP) rollout (the first phase concerned domestic implementation) allowing reciprocal access for exchanging international alert data with global partners. Originally, the program expected to achieve its objectives through bilateral agreements within a few years and TCA establishes a legal framework for the UK and EU to facilitate bilateral law enforcement data exchange, including alerts.

---

[3] Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (notified under document C(2021) 4801,

[4] https://assets.publishing.service.gov.uk/media/5e579695e90e07110306a2f5/The_Future_Relationship_with_the_EU.pdf

[5] Draft Agreement on Law Enforcement and Judicial Cooperation in Criminal Matters, HM Government, May 2020.

[6] https://committees.parliament.uk/publications/5298/documents/52902/default/

In 2022 the European Commission announced a new legislative proposal on a Framework for reciprocal access to security-related information for front-line officers between the EU and key third countries to counter shared security threats. A proposal from the European Commission was expected in Q4 2023 but this is now overdue.[7]

Following the proposal the Home Office shifted towards an EU-wide multilateral solution. This approach seeks to enable receipt of international alerts from all EU Member States through a unified system, offering "a substantially greater level of mutual benefit to both domestic and international law enforcement compared to individual bilateral agreements."[8] The target for an EU agreement on ILEAP to be concluded is 2027/28. [9]

Given the loss of access to the important SIS II database and the inadequacies of relying on Interpol's I-24/7 mechanism, the prompt establishment of an agreement on ILEAP with the EU should be given a high priority. This will significantly enhance the collective security of both the UK and the EU and is essential for maintaining effective law enforcement collaboration and ensuring timely information sharing between the regions.

What are the possible challenges to UK-EU data adequacy regime? What factors could influence the next European Commission when deciding whether to renew its data adequacy decisions for the UK in June 2025?

The factors that could influence the EU's decisions on data adequacy can be divided into four main categories:

1. Onward transfers/leakage: This category addresses the risk of data, especially data originating from within the EU, unintentionally reaching third countries. Such incidents could potentially lower privacy and security standards.
2. Issues of redress: This area focuses on the availability of judicial redress and oversight mechanisms in cases of data breaches. It highlights the importance of having robust legal frameworks that

[7] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13243-Security-related-information-sharing-%E2%88%92-reciprocal-access-for-frontline-officers-in-the-EU-and-key-partner-countries_en
[8] https://committees.parliament.uk/publications/41869/documents/207633/default/
[9] https://www.gov.uk/government/publications/home-office-major-programmes-accounting-officer-assessments/international-law-enforcement-alerts-platform-i-leap-programme

provide avenues for recourse and ensure accountability. The UK is noted for its strong performance in this domain.

3. Independence of the regulator: The focus here is on the independence of regulatory bodies responsible for monitoring and enforcing data protection laws. An independent regulator is crucial for maintaining impartiality and effectiveness in upholding data protection standards.
4. ECHR: Article 692 of the TCA triggers the termination of Part III if either the UK or an EU Member State "denounce" the ECHR (termination becomes effective on the date of such denunciation). It is difficult to envision a situation how the LED decision would remain in place if this were to occur.

What implications, if any, would a no or disrupted UK-EU data adequacy scenario have? Do you have any concerns about the direction of travel of the UK Government's data policies as set out in the Data Protection and Digital Information Bill, and about the potential for greater divergence from EU data standards?

The proposed amendments to the UK's data protection framework have raised concerns, particularly regarding the independence of the Information Commissioner. An independent data protection authority is critical for the EU's adequacy decisions. However, the new Data Protection and Digital Information Bill could compromise this independence by allowing the Secretary of State to exert influence over the Commissioner's directives. This includes requiring the Commissioner to take government suggestions into account when developing Codes of Practice and to align with governmental strategic priorities, potentially diminishing the Commissioner's autonomy. Recent Government amendments, which limit the Secretary of State's role to offering feedback and recommendations on draft codes instead of possessing the authority to approve them, represent a positive step forward.

Additionally, the Bill modifies the criteria under which 'legitimate interests' can serve as a basis for data processing. Previously, the grounds for data processing were clearly defined, balancing individual rights with business needs. The Bill, however, proposes a looser interpretation that could shift this balance in favour of business interests, by enabling the Secretary of State to expand the grounds that qualify as legitimate interests, potentially to include commercial advantages.

The Bill suggests alterations in how data subjects' rights are handled, specifically regarding the rejection of their requests. It broadens the criteria for rejecting requests, allowing data controllers to consider their resource constraints and their relationship with the data subject. This expansion could restrict the exercise of data subjects' rights, weakening the existing protections.

How high is the risk of the European Commission withdrawing its UK data adequacy decisions?

The situation requires vigilant monitoring, and the United Kingdom must avoid any significant policy divergence that could jeopardise the European Union's decision to rescind or not renew its adequacy decisions. Nevertheless, there is strong support for the adequacy decisions within the European Commission, and it is anticipated that the arrangement will remain robust moving forward.

Although the European Parliament does not have a role in granting data adequacy decisions, it has been more vocal in raising concerns about the UK's direction of travel, particularly the Committee on Civil Liberties, Justice and Home Affairs (LIBE). Within the European Parliament, there is a split on the issue along the left-right axis. Right and centre-right parties view the UK's data protection framework more favourably than centrist, centre-left, and far-left parties.[10] It is important to note that this year will see the formation of a new European Commission and a new European Parliament. This change is likely to result in a different composition of political groupings.

What impact would that have and how prepared are businesses or the public sector for such a scenario?

Should data adequacy be revoked, firms would need to rely on alternative legal mechanisms, such as Standard Contractual Clauses (SCCs). Depending on SCCs could be cumbersome, unpredictable, and lead to notable economic impacts. It would also disproportionately affect small and medium-sized businesses.

According to the government's impact assessment, an estimated 14% of businesses trading with the EU already have SCCs in place, although, as

[10] The split is exemplified by the MOTION FOR A RESOLUTION on the adequate protection of personal data by the United Kingdom which passed (vote breakdown) and the alternative MOTION FOR A RESOLUTION on the adequate protection of personal data by the United Kingdom which was defeated (vote breakdown).

the impact assessment acknowledges, this figure may be an overestimate. The impact assessment further estimates the following costs associated with these changes:

> "The results of the updated modelling estimate an economic impact of £410m (range of £190-£460m) in one-off SCC costs and an annual cost of £240m (range of £210m and £420m) in lost export revenue. Once appraised over a 10-year period, the estimated NPV (2019 prices, 2020 present value) of EU Adequacy is £2 billion (range of £1.6 and £3.4 billion)."[11]

The government impact assessment focuses solely on direct UK-EU trade, which suggests that the actual costs could be higher when taking into account the broader implications on the entire supply chain.
The ability to share personal data is also fundamental for supporting medical safety as well as facilitating health and scientific research. Without EU data adequacy decisions, it would be difficult for these sectors to continue to function effectively.

What would be the implications for the continued operation of Part III of the TCA (law enforcement and judicial cooperation on criminal matters)?

Part III of the TCA, or any of its individual Titles, can be suspended if there is a "serious and systemic" lapse by one Party in either (i) "the protection of fundamental rights or the principles of the rule of law", or (ii) "the protection of personal data". This includes situations that result in the termination of a "relevant adequacy decision." For such a suspension to occur, a detailed written notification must be sent through diplomatic channels, specifying the exact deficiency that warrants the suspension. [12] The loss of access to these databases would have profound negative implications for future of policing and judicial cooperation and leave both sides less safe and less secure.

What can be learned from other countries' experience with the adequacy system and engagement with the European Commission's process?

[11] https://publications.parliament.uk/pa/bills/cbill/58-03/0265/DataProtectionandDigitalInformationBillImpactAssessment.pdf
[12] UK-EU Trade and Cooperation Agreement, Article 692, December 2020.

The UK started from a unique position compared to other countries that have been granted EU data adequacy. As a former member of the EU, the UK originally shared the same GDPR regulations. In contrast, other countries have had to negotiate and reform their domestic laws to align with EU standards and achieve adequacy status. For example, Japan and South Korea both recognised the significant advantages of facilitating free data flows with the EU.

South Korea undertook comprehensive reforms of its data protection laws by amending the Personal Information Protection Act in 2020 to meet the EU's standards for data adequacy. The amendments were designed to address the European Commission's concerns regarding access by public authorities to personal data and to establish effective redress mechanisms for data subjects within the EEA. These changes culminated in the integration of data protection services within the Personal Information Protection Commission (PIPC), helping South Korea to align with the EU GDPR and supporting its Free Trade Agreement with the EU, which is valued at approximately €90 billion annually.[13]

Similarly, Japan enhanced its data protection framework to secure an adequacy decision from the EU in January 2019, creating the world's largest area of free data transfer, covering over 127 million citizens. This decision was announced concurrently with a statement by Prime Minister Abe at the World Economic Forum, advocating for 'data free flow with trust'. Japan's efforts included the introduction of Supplementary Rules by the Personal Information Protection Commission of Japan (PPC) under the Act on the Protection of Personal Information. These rules bolstered individual rights and introduced stringent safeguards for data transfers to third countries and sensitive data. Japan also established a complaint handling mechanism akin to those in South Korea and the UK.[14]

The first review of the EU-Japan mutual adequacy arrangement occurred in October 2021. During this review, Didier Reynders, European Commissioner for Justice, and Shuhei Ohshima, remarked on the success of the partnership in enhancing data protection and facilitating data transfers. They noted that the convergence between the data protection systems of the EU and Japan had increased, further solidifying their strategic partnership. This review highlighted how aligning data protection laws can extend beyond economic benefits, fostering deeper cooperation

[13] https://edpb.europa.eu/news/news/2021/edpb-adopts-opinion-draft-south-korea-adequacy-decision_en
[14] https://ec.europa.eu/info/sites/info/files/annex_i_supplementary_rules_en.pdf

and trust between the EU and third countries, as evidenced by Japan's example.

These examples illustrate that third countries have progressively aligned their data protection frameworks with the EU's standards, demonstrating further convergence since the initial adoption of the adequacy decisions.

What are the implications for the UK's EU adequacy status if the UK grants its own adequacy decisions to other third countries currently not subject to EU adequacy?

The UK will use different criteria to assess data protection regulations in third countries to the EU and is looking to grant data adequacy to several countries that the EU does not recognise as having comparable GDPR standards.

The Bill introduces a "data protection test" which will be met provided that data protection in a given third country is "not materially lower" than in the UK. This test will apply when the Secretary of State is assessing potential country-level adequacy decisions (the test is also applicable when data controllers are assessing transfer mechanisms for day-to-day international data transfers).

This new outcomes-based approach, taking into account the overall standards of protection for data subjects, differs from the point by point comparison used by the EU. The wording is slightly different than under the GDPR, which requires the standard to be "essentially equivalent" rather than "not materially lower".

The Data Protection and Digital Information Bill impact assessment clearly states an ambition to establish transborder data flow partnerships with Australia, Colombia, the Dubai International Financial Centre, South Korea, Singapore, and the United States as top tier priority countries with longer term priority partners including Brazil, India, Indonesia and Kenya.

The lists have raised concerns, as countries like Australia, Singapore and the U.S. are still far from privacy standards comparable to the level of the GDPR and that the UK might become a loophole for transferring the personal data of EU data subjects to jurisdictions where adequate safeguards are not in place.

Received 24 May 2024