

## **Committee on Civil Liberties, Justice and Home Affairs (LIBE) – Written Evidence (DAT0001)**

### **The Right Honourable**

Lord Peter Ricketts  
Chair of the European Affairs  
Committee House of Lords  
UK Parliament

### **Subject: European Parliament Justice Committee's contribution to the inquiry into data adequacy**

Dear Lord Ricketts,

In response to the inquiry into data adequacy and its implications for the UK-EU relationship by the House of Lords European Affairs Committee, please find below the contribution of the Committee on Civil Liberties, Justice and Home Affairs (hereinafter: LIBE Committee) of the European Parliament.

The United Kingdom, while a Member State of the European Union (EU), aligned its national laws with the General Data Protection Regulation (GDPR) and the EU Law Enforcement Directive (LED). Following UK's withdrawal from the EU, the European Commission adopted two adequacy decisions on 21 June 2021, providing for the free flow of personal data between the UK and the EU, without requiring additional safeguards. The LIBE Committee is closely monitoring developments in the UK, as both adequacy decisions contain sunset clauses, and thus will automatically expire four years after their entry into force.

In this regard, the topic of UK adequacy findings was discussed during a LIBE Committee mission to London (2-4 November 2022), while an exchange of views with Mr John Edwards, the UK Information Commissioner, was held on 23 May 2023 during a meeting of the LIBE Committee in Brussels. There have also been recent exchanges between the LIBE Committee and Didier Reynders, European Commissioner for Justice, on the matter.

Before answering specific questions, let us mention three issues that we consider the most controversial and that regularly appear in discussions in the LIBE Committee on the UK data protection reforms:

**First**, the changes to the definition of "*personal data*".

The Bill modifies the concept of “personal data” that is at the heart of the EU data protection regime in the following ways:

- Under the Bill, “singling out” of individuals without using identifiers or person-specific factors will not be regarded as “identifying” the individual;

B-1047 Brussels - Tel. +32 2 28 40660

F-67070 Strasbourg - Tel. +33 3 88 1 74420

- Processors and “other persons” who process pseudonymised data are treated as if they do not process “personal data”, while in the EU, pseudonymised data are considered personal data;

**Second**, the role of the Information Commissioner’s Office (ICO) as the national data protection authority of the UK, including its independence.

Even under the current regime, several experts consider the ICO’s enforcement activities as weak. At the same time, the Bill appears to further undermine, not merely the effectiveness, but beyond that the independence of the ICO. In particular, there is a risk that the Commissioner will have a duty to consider factors outside its primary expertise when balancing between the protection of personal data and other interests such as the UK economy, public safety or the international agenda of the UK Government prior to exercising their powers, or, having to follow priorities set by the Secretary of State.

**Third**, onward transfers of personal data.

In line with the Bill, the UK can declare that other third countries or international organisations to provide adequate protection of personal data, irrespective of whether that third country or international organisation in question has been deemed to provide such essentially equivalent protection by the European Commission. The LIBE Committee is therefore strongly concerned that in such instances the UK adequacy status could lead to the bypassing of EU rules on international transfers to countries or international organisations not deemed adequate under EU law.

#### Answers to specific questions

1. **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?*

As highlighted in the European Parliament resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom (2021/2594(RSP)), the ability to transfer personal data across borders has the potential to be a key driver of innovation, productivity and economic competitiveness, and it is of crucial importance for effective cooperation in

the fight against crossborder serious crime, as well as in the fight against terrorism, that increasingly depends on the exchange of personal data.

- b. How are the General Data Protection Regulation and the Law Enforcement Directive working in practice? What extra costs do they impose on businesses?*

While extra costs for businesses may be expected in relation to compliance with these acts, the scope of this question is beyond the competence of the LIBE Committee.

- c. How would you assess the overall performance and effectiveness of the Information Commissioner's Office (ICO) as the UK's independent data regulator? Has its work been impacted by decisions on data adequacy?*

The UK data protection supervisory authority, the ICO, is one of the largest in Europe. However, according to experts with whom LIBE Members discussed this topic, despite having a lot of capacity and resources, ICO enforcement is currently rather weak. The LIBE Committee is concerned that such a lack of enforcement is a structural problem, as laid out in the ICO's regulatory action policy, which explicitly states that "in the majority of cases we will reserve our powers for the most serious cases, representing the most severe breaches of information rights obligations. These will typically involve wilful, deliberate or negligent acts or repeated breaches of information rights obligations, causing harm or damage to individuals". In practice, this has meant that a large number of breaches of data protection law in the UK have therefore not been remedied.

Under the draft Bill, the UK ICO will be entrusted with the promotion of innovation and competition. The draft Bill would make changes to the role of the Information Commissioner. Under the new **section 120A**, the principal objective of the Commissioner, when carrying out functions under data protection law, would be:

- 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.

At the same time, under new **section 120B**, the Commissioner would need to have regard to the following when carrying out data protection functions:

- The desirability of promoting innovation;
- The desirability of promoting competition.

Finally, **section 120E** would introduce a Statement of Strategic Priorities. This would set out the data protection priorities of the UK Government that the Commissioner would need to consider.

All of the aforementioned developments seem to constitute a significant departure from the EU data protection supervision model, where the

independence of the national supervision authorities is an important cornerstone.

## 2. **What are the possible challenges to the UK-EU data adequacy regime?**

- a. *What factors could influence the next European Commission when deciding whether to renew its data adequacy decisions for the UK in June 2025?*

One of the factors, as discussed by LIBE Members during the LIBE mission to London, 2-4

November 2022, is the topic of **onward transfers** (for more details, see the answer to question

4.c below). Furthermore, and as expressed above, the experts consulted by the LIBE Committee also pointed at the "**Henry VIII**" clauses in the new UK data protection Bill that gives the UK government a certain level of influence over the Information Commissioner's actions. Another factor with a possible influence on the adequacy findings is the **Retained EU Law Bill** that repealed or replaced all legal provisions adopted by the UK to comply with the EU law.

Finally, the LIBE Committee would like to stress that the United Kingdom is a signatory to the European Convention on Human Rights (ECHR) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and, therefore, bound by both the jurisprudence of the European Court of Human Rights (ECtHR) and the rules under the Convention. The latter applies both to processing carried out by private entities for commercial purposes and to processing carried out by public authorities for law enforcement purposes, as well as for national security purposes. Compliance with Strasbourg jurisprudence was an important factor when assessing UK adequacy. In this context, any possible changes to the UK's Human Rights Act or the UK's departure from ECHR jurisprudence would, in the opinion of the LIBE Committee, have a negative impact on the UK adequacy.

Furthermore, the LIBE Committee would like to stress the **ECHR Conditionality**: pursuant to Article 692 (termination clause) of the Trade and Cooperation Agreement (TCA) between the EU and the UK, should the UK [or one of the EU Member States] denounce its membership to the ECHR or Protocols 1, 6 or 13 thereto, Part III of the TCA on law enforcement and judicial cooperation in criminal matters shall cease to be in force as of the date that such denunciation becomes effective.

- b. *What factors could the Court of Justice of the EU (CJEU) consider if the legality of the EUUK adequacy decisions were challenged?*

The LIBE Committee would like to stress the importance of the following rulings of the Court of Justice of the European Union:

- Judgement of 6 October 2015 in Case C-362/14 Maximilian Schrems v Data Protection Commissioner ('*Schrems I*');

- Opinion 1/15 of 26 July 2017 on the Draft EU Canada PNR Agreement (*‘Opinion 1/15’*);
- Judgment of 16 July 2020 in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems (*‘Schrems II’*).

The core of these decisions underline the principle that an adequacy finding demands the “essential equivalence” in the level of protection of personal data from the third country, compared to the one awarded by the EU. Whenever this principle is breached, the Court will have to find that adequacy no longer exists. Furthermore and in particular, in *Schrems I*, the Court stated that indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the fundamental right to privacy provided for in Article 7 of the Charter of Fundamental Rights of the European Union; in *Schrems II*, the Court concluded that the EU-U.S. Privacy Shield mechanism did not provide sufficient legal remedies against mass surveillance for non-US nationals and that this violates the essence of the fundamental right to a legal remedy as provided for in Article 47 of the Charter.

In this context, the LIBE Committee is also concerned as to whether the processing of personal data by UK intelligence agencies, especially its bulk collection of communication data, is in line with the EU Charter of Fundamental Rights. The LIBE Committee is concerned that the indiscriminate bulk collection of communications metadata that is taking place in the UK could be contrary to principles established by the European Court of Human Rights and the CJEU.

*c. How would you assess the possible impact of proposed UK rules on automated decisionmaking and the use of Artificial Intelligence on data adequacy?*

The LIBE Committee was one of the two European Parliament Committees responsible for the AI Act negotiations. The AI Act maintains the level of protection as set out in the GDPR, in particular in Article 22 (“Automated individual decision-making, including profiling”) thereof.

According to the expert consulted by the LIBE Committee, the draft Bill reverses the logic of Article 22 GDPR and the right not to be subject to automated decision making or profiling. Instead of few exceptions as to when automated decisions can be taken (e.g. authorised by law), the draft Bill permits automated decision making in general, subject to limited exceptions. The LIBE Committee also considers as controversial the provisions of the draft Bill permitting large databases of personal data to be used, disclosed and transferred (including outside the United Kingdom) for AI training and development without informing the data subjects or asking for their consent.

Likewise, the use of automated decision-making in the context of law enforcement under the Bill seems to follow a different approach than the one taken in the EU, providing more flexibility and fewer safeguards. Furthermore, pursuant to Article 2(4) of the AI Act, the use of AI systems in the framework of law enforcement or judicial cooperation may only take place if the third country in question provides adequate safeguards regarding

the protection of fundamental rights and freedoms. Since the AI Act is without prejudice to the relevant EU instruments covering the protection of personal data, should the UK LED adequacy decision be affected by the changes under the UK data protection Bill, an EU competent authority would have to apply Article 37(1)(b) LED for any transfers to the UK competent authorities. In addition, that competent authority would have to take into account the EDPB Guidelines 1/2023 on that matter. The assessment required under that provision could lead to the conclusion that an adequate level of protection cannot be ensured in light of the UK rules on automated decision-making under the data protection Bill or the use of AI without the provision of adequate safeguards in the context of law enforcement and judicial cooperation.

**3. What implications, if any, would a no or disrupted UK-EU data adequacy scenario have?**

- a. *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 LIBE Committee is concerned about the overall direction of the data policies of the UK Government. The current actions of the Government appear to be aimed at (i) eliminating constraints arising from European or international law, and (ii) limiting the impact of European court jurisdiction and European court interpretations on UK law. Finally, the LIBE Committee also observes a switch towards using executive legislative powers in these policies with limited oversight from the UK Parliament. In the opinion of the LIBE Committee, these factors, as well as other issues mentioned in this contribution, may increase UK divergence from EU data standards, putting the validity of the adequacy findings into question.

- b. *How high is the risk of the European Commission withdrawing its UK data adequacy decisions? What impact would that have and how prepared are businesses or the public sector for such a scenario?*

From the perspective of the LIBE Committee, both EU and UK businesses need and deserve legal certainty. Therefore, governments should avoid creating situations where businesses constantly need to adapt to new legal solutions. Possible invalidation of the UK adequacy findings would result in a lack of legal certainty, increase costs and cause disruption for European and UK businesses, as well as individuals. This might be particularly burdensome for micro, small and medium-sized enterprises. For example, if there is no adequacy finding, transfers of personal data will require the use of specific safeguards, adding another layer of burdensome compliance requirements for businesses.

- c. *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 on law enforcement and judicial cooperation in criminal matters is based on the assumption that an adequacy decisions between the

UK and the EU exists. While the GDPR adequacy decision is relevant in the context of personal data exchanges related to anti-money laundering (AML) or Passenger Name Records (PNR) by air carriers, a withdrawal by the European Commission of its UK LED related data adequacy decision could jeopardise additional channels of cooperation that currently takes place between UK and EU competent authorities.

The LIBE Committee would like to reiterate its concerns expressed in the resolution of February 2021 on the TCA regarding the special use and longer retention of personal data granted to the UK under the PNR titles of the TCA, which are not in line with the use and retention by the Member States and the requirements set out in the CJEU judgment of 21 June 2022 in Case C-817/19 on the PNR Directive.

Furthermore, the possibilities to engage in joint processing operations by intelligence services and competent authorities under **Section 29** of the draft Bill could lead to the circumvention of important data protection safeguards that apply to law enforcement processing and not to processing carried out by intelligence services. For instance, intelligence agencies may be more flexible to exchange information, including personal data, with other intelligence services in third countries, than the law enforcement.

**Section 131** of the Bill on retention of pseudonymised biometric data seems to be in contradiction with established case law of the ECtHR (*S and Marper v UK*). In addition, the continuous storage of (pseudonymised) personal data potentially increases the severity of data breaches in terms of the number of and repercussions for concerned data subjects, in particular where the personal data in question are of sensitive nature, such as biometric data. Likewise, the weakening of oversight and use of biometric material, under **Section 147** of the proposed Bill, contributes to such concerns.

Due to the requirement that an adequacy decision must be in place as prerequisite to allow for exchanges of personal data within the scope of Part III of the TCA, the watering down of some of the data protection safeguards under the Bill may lead to the partial or even full suspension of law enforcement and criminal justice cooperation provisions.

Finally, in accordance with Article 693(2) of the TCA (suspension clause), in the event of serious and systemic deficiencies within one Party as regards to the protection of personal data, including where those deficiencies have led to a relevant adequacy decision ceasing to apply, the other Party may suspend Part III of the TCA or Titles thereof. Consequently, a suspension of [parts] of Title III of the TCA may occur already before an adequacy decision is withdrawn. Such a suspension or termination of [parts of] Title III of the TCA could affect relevant provisions on data exchanges such as PNR or DNA and vehicle registration data, the sharing of personal data for AML and counter terrorist financing purposes as well as the surrender mechanism superseding the European arrest warrant (EAW), or cooperation with Europol and Eurojust.

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

- a. *What conclusions do you draw from the European Commission's recent adequacy review of 11 countries and territories?*

The LIBE Committee has taken note of the review, but will not analyse it before the end of the current parliamentary term.

- b. *Are there examples of best practice which the UK could learn from in the way other countries approach their data transfer arrangements with the EU?*

The LIBE Committee is not in a position to comment on this question, in particular because there is no comparable case where a third country was previously an EU Member State and carried over the relevant Union legislation when leaving.

- c. *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?*

In line with the Bill, the UK can declare that other third countries or international organisations provide adequate data protection, irrespective of whether the third country or international organisation in question has been considered to provide such protection by the European Commission. The LIBE Committee is therefore strongly concerned that the UK adequacy status could lead to the bypassing of the EU rules on international transfers to countries or international organisations not deemed adequate under EU law.

For example, the UK has already held that Gibraltar provides "adequate" protection in terms of the UK GDPR, while there is no similar finding on this territory by the EU. Similar problems as those mentioned with regard to the commercial processing of personal data may arise concerning the processing of personal data by the law enforcement, as well as the onward transfers from the UK to third countries not subject to an EU adequacy decision. While the LED requires prior authorisation from the Member State that carried out the original transfer, which should take due account of all relevant factors surrounding the transfer, including the level of personal data protection in the third country or international organisation to which the onward transfer takes place, this system of checks and balances could be undermined where the UK grants its own adequacy decision to other third countries.

In addition, **Section 126** of the proposed Bill on law enforcement information-sharing could lead to the onward transfer of information obtained by UK competent authorities from EU competent authorities based on obligations under international agreements that the UK is subject to. This could, for instance, be the case with regard to the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

Finally, as we have already mentioned above, the European Parliament is concerned that the UK could become a transit country for data that cannot be sent from the EU/EEA to "inadequate" third countries. In particular, the LIBE Committee is concerned about countries where the overall human



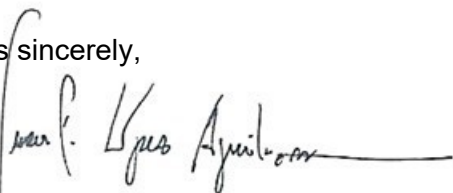
rights situation is satisfactory, but where there are massive concerns regarding the surveillance and risks to personal data from the EU.

*d. If the UK joined the Global Cross Border Privacy Rules system, what impact if any could that have on the UK's EU adequacy status?*

The LIBE Committee has not assessed the Global Cross Border Privacy Rules system in detail. However, we understand it is only a declaration and does not constitute binding obligations. Therefore, the effect on EU adequacy ratings would appear to be minimal, if any, as EU rules on adequacy would still apply.

We hope you can take these comments into consideration. Please do not hesitate to contact the LIBE Secretariat ([libe-secretariat@europarl.europa.eu](mailto:libe-secretariat@europarl.europa.eu)) should you require further information or clarifications.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Juan F. López Aguilar", with a long horizontal line extending to the right.

Juan Fernando LÓPEZ AGUILAR

**Received 22 April 2024**