The UK Government's assessment of adequacy for the UK Extension to the EU-US Data Privacy Framework for the general processing of personal data

Introduction

The UK Government can assess whether another country, territory or an international organisation provides an adequate level of data protection compared to the UK. Some countries may have a substantially similar level of data protection to the UK. In these cases, the Government can make UK adequacy regulations. This allows organisations to send personal data to that country, territory or international organisation if they wish.

An adequacy assessment may cover either general processing, or law enforcement processing, or both. The Government must consider a range of factors, including that sending personal data to that country, territory or international organisation does not undermine people's protections.

We support the Government undertaking adequacy assessments and making regulations. This enables personal data to flow freely in our global digital economy to trusted partners. We do this by providing independent assurance on the process followed and the factors that government officials take into consideration. This allows the Secretary of State to make an informed and reasonable decision. By doing this work once for everyone, the Government and the ICO are reducing the burden of compliance on organisations that would otherwise have to put alternative measures in place.

One of our priorities for this year, as set out in our ICO25 strategic plan[1], is to "enable international data flows through regulatory certainty". This includes our work on adequacy assessments. We provided advice to the Government during its assessment of the UK Extension to the EU-US Data Privacy Framework (UK Extension). Now that the Government has laid the regulations, we are publishing this Opinion to set out our views on the process and the Government's conclusion.

Key Finding

The Commissioner considers that, while it is reasonable for the Secretary of State to conclude that the UK Extension provides an adequate level of data protection and to lay regulations to that effect, there are four specific areas that could pose some risks to UK data subjects if the protections identified are not properly applied. These are detailed later in this Opinion.

The Secretary of State should monitor these areas closely to ensure UK data subjects are afforded equivalent protection in practice and their rights are not undermined. He also recommends monitoring the implementation of the UK Extension generally to ensure it operates as intended.

About this Opinion

Who is this Opinion for?

This Opinion is primarily for members of the UK Parliament to consider alongside the UK adequacy regulations laid by the Secretary of State.

It may also interest the wider public, data protection professionals and organisations that already transfer personal data to the United States of America (USA) or who are considering doing so.

What is an adequacy assessment?

The UK's data protection laws set out a framework for the responsible use of personal data by organisations. People may lose this protection when organisations transfer their personal data to organisations in other countries or to international organisations.[2] This is why the UK General Data Protection Regulation (UK GDPR) has specific rules on how to make international transfers of personal data. These rules mean that organisations must put in place continuing protections for people's personal data when transferring it to another jurisdiction, or one of a limited number of exemptions must apply.

One way that UK organisations can transfer personal data to another jurisdiction is by relying on UK adequacy regulations made by the Secretary of State. The Secretary of State can assess a country, territory or international organisation or a particular sector in a country or territory and decide if its legal framework offers a similar level of data protection to the UK.

Article 45 of the UK GDPR contains a list of criteria the Secretary of State must consider when carrying out an adequacy assessment.

> **Criteria to be considered in an adequacy assessment**[3]
>
> 2. When assessing the adequacy of the level of protection […], the Secretary of State shall, in particular, take account of the following elements:
>
> a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the Commissioner; and
>
> c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

If the Secretary of State decides the country, territory or international organisation, or a particular sector in a country or territory, provides an adequate level of data protection after considering all the above criteria, they can make regulations to give legal effect to their decision.

These adequacy regulations allow UK organisations to transfer personal data to a controller or processor located in a third country or to an international organisation. The transfer must adhere to the particular scope of those regulations.

What is the Commissioner's role in adequacy assessments?

Article 36(4) of the UK GDPR requires the Secretary of State to consult the Commissioner when preparing a proposal for a legislative measure which relates to processing. The Secretary of State must also consult the Commissioner before making regulations under the Data Protection Act 2018 (DPA 2018).[4]

The Secretary of State for Science, Innovation and Technology (previously the Secretary of State for Digital, Culture, Media and Sport) and the Information Commissioner entered into a Memorandum of Understanding (MoU) on the role and responsibilities of the ICO in relation to the Department for Science, Innovation and Technology's (DSIT's) work on UK adequacy assessments and regulations.[5]

As set out in the MoU, DSIT consults the Commissioner at various stages in their process. The Commissioner offers advice and comments on the information provided. However, the Commissioner does not make his own assessment of the adequacy of another country, territory or international organisation. He provides an independent assurance on the process followed and the factors that DSIT officials take into consideration. This allows the Secretary of State to make an informed and reasonable decision.

The MoU also says that the Commissioner may provide an Opinion to Parliament, including on the DSIT process and factors they take into account. These Opinions recognise that different countries have different ways of ensuring adequate levels of data protection.

Assessment of the UK Extension to the EU-US Data Privacy Framework

In 2021, the Secretary of State announced that the Government would assess the USA for adequacy under the UK GDPR.[6]

DSIT's assessment considered the level of data protection provided by UK Extension.

DSIT obtained information from:

- the EU-US Data Privacy Framework (DPF);
- the letters from the US Government to the UK Government;
- relevant US legislation;
- other desk-based research; and
- discussions and correspondence with the US Government.

DSIT officials provided their analysis of the UK Extension for review. DSIT officials responded positively to the ICO's suggestions of areas to clarify, and they explored these further. This ensures the final assessment is based on an appropriate range and depth of relevant factual information. The Commissioner gives this Opinion based on that information and has provided advice to the Secretary of State.

The assessment considered all the criteria for adequacy listed in article 45 of the UK GDPR to the appropriate extent.

The Commissioner considers, while it is reasonable for the Secretary of State to conclude that the UK Extension provides an adequate level of data protection and to lay regulations to that effect, there are four specific areas that could pose some risks to UK data subjects if the protections identified are not properly applied.

As well as monitoring the implementation of the UK Extension and relevant developments in the USA generally, the Secretary of State should monitor these areas closely to ensure UK data subjects are afforded substantially similar protection in practice and their rights are not undermined.

The definition of 'sensitive information' under the UK Extension does not specify all the categories listed in Article 9 of the UK GDPR. Instead, the UK Extension includes a catch-all provision specifying, "...any other information received from a third party that is identified and treated by that party as sensitive." Accordingly, UK organisations will need to identify biometric, genetic, sexual orientation and criminal offence data as 'sensitive data' when sending it to a US certified organisation so it will be treated as sensitive information under the UK Extension. However, there is no current requirement for UK organisations to identify information as sensitive. This creates a risk that the protections may not be applied in practice. The Commissioner welcomes a proposal by DSIT to publish guidance for UK organisations to assist them in ensuring that special category data is identified as sensitive and treated accordingly. The Secretary of State should evaluate the effectiveness of this guidance in affecting practice.

The Secretary of State should monitor the following areas so that the differences in UK and US law do not result in a reduction in protections for data subjects.

- For criminal offence data, there may be some risks even where this is identified as sensitive because, as far as we are aware, there are no equivalent protections to those set out in the UK's Rehabilitation of Offenders Act 1974. This Act places limits on the use of data relating to criminal convictions when those convictions have become 'spent' following the relevant rehabilitation period, including the ability to request that this data is deleted. It is not clear how these protections would apply once the information has been transferred to the USA.
- The UK Extension does not contain a substantially similar right to the UK GDPR in protecting individuals from being subject to decisions based solely on automated processing which would produce legal effects or be similarly significant to an individual. In particular, the UK Extension does not provide for the right to obtain a review of an automated decision by a human.
- The UK Extension contains neither a substantially similar right to the UK GDPR's right to be forgotten nor an unconditional right to withdraw consent. While the UK Extension gives individuals some control over their personal data, this is not as extensive as the control they have in relation to their personal data when it is in the UK.

The Commissioner therefore gives a qualified assurance to Parliament as it considers the regulations.

Review and ongoing monitoring

The Secretary of State must undertake a review of the level of data protection provided by the UK Extension every four years from the date the regulations come into force.

The Secretary of State is also required to monitor, on an ongoing basis, developments in a country, territory or international organisation which is the subject of UK adequacy regulations.

If the Secretary of State becomes aware of a significant change in the level of data protection that applies to personal data transferred from the UK as a result of either the review or ongoing monitoring obligations, the Secretary of State must amend or revoke the regulations to the extent necessary.

As part of the Commissioner's role in the consultation process, he considered whether any of the information we reviewed highlighted particular aspects that the Secretary of State should monitor. In addition to the four areas mentioned above, he advised her to monitor:

- that the requirements under the DPF, including the Principles, rights and exemptions, work as intended;
- the implementation and compliance with the requirements of Executive Order 14086 by the US intelligence community;
- the effectiveness of US oversight and enforcement bodies in ensuring compliance with the DPF Principles, Executive Order 14086 and resolving complaints from individuals; and

- any significant changes in the US legal landscape.

In the course of his duties, the Commissioner, or his staff, may become aware of information that suggests the UK Extension no longer provides adequate data protection. Should that happen, he will inform the Secretary of State and may recommend they undertake a review of the regulations. Depending on the circumstances, he may revise this Opinion accordingly.

What is the status of this Opinion?

The Commissioner has several powers and functions around UK adequacy assessments. This includes section 115(3)(a) of the DPA 2018[7]. This gives the Commissioner a duty to advise the UK Parliament and Government, amongst others, on legislative and administrative measures. A key part of this links to the protection of people's rights and freedoms relating to the processing of personal data under the UK GDPR. UK adequacy regulations fall within this remit.

There is also section 115(3)(b) of the DPA 2018[8] which allows the Commissioner to issue Opinions to Parliament, the Government, other institutions and bodies and the public. They can cover any issue about the protection of personal data. The Commissioner can issue Opinions either on his own initiative or on request.

This Opinion sets out the Commissioner's view of the adequacy assessment process followed, and factors taken into consideration by the Secretary of State for DSIT for the UK Extension under section 17A of the DPA 2018 and article 45 of the UK GDPR.

---

[1] ICO25 strategic plan

[2] An international organisation is defined by the UK GDPR as "an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries".

[3] Article 45(2), UK GDPR

[4] Section 182(2), DPA 2018

[5] Memorandum of Understanding (MoU) on the role of the ICO in relation to new UK adequacy assessments

[6] DCMS, International data transfers: building trust, delivering growth and firing up innovation, 26 August 2021

[7] Another example is article 57(1)(c) of the UK GDPR.

[8] See also article 58(3)(b) of the UK GDPR.