



[Home](#) > [Business and industry](#) > [Trade and investment](#) > [Digital trade](#)
> [UK-US data bridge: supporting documents](#)

[Department for
Science, Innovation
& Technology](#)

Notice

UK-US data bridge: explainer

Published 21 September 2023

Contents

[Data bridges](#)

[Data Privacy Framework](#)

[Privacy](#)



© Crown copyright 2023

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at <https://www.gov.uk/government/publications/uk-us-data-bridge-supporting-documents/uk-us-data-bridge-explainer>

The UK Secretary of State for Science, Innovation, and Technology the Rt Hon Michelle Donelan MP took the decision to establish the UK-US data bridge and lay adequacy regulations in Parliament to this effect.

The Secretary of State took this decision, under Section 17A of the Data Protection Act 2018, to establish a data bridge with the United States of America through the UK Extension to the EU-US Data Privacy Framework. The Secretary of State has determined that the UK Extension to the EU-US Data Privacy Framework does not undermine the level of data protection for UK data subjects when their data is transferred to the US. This decision was based on their determination that the framework maintains high standards of privacy for UK personal data.

Adequacy regulations have been laid in Parliament today (21 September 2023) to give effect to this decision. UK businesses and organisations will be able to make use of this data bridge to safely and securely transfer personal data to certified organisations in the US, once the regulations come into force from the 12 October.

Supporting this decision, the US Attorney General, on the 18 September, designated the UK as a 'qualifying state' under Executive Order 14086. This will allow all UK individuals whose personal data has been transferred to the US under any transfer mechanisms (i.e. including those set out under UK GDPR Articles 46 and 49) access to the newly established redress mechanism in the event that they believe that their personal data has been accessed unlawfully by US authorities for national security purposes.

The laying of the SI today follows on from an announcement earlier in the year which highlighted the data bridge as a key deliverable for 2023 under the UK-US Comprehensive Dialogue on Technology and Data. A commitment in principle to establish the data bridge was also announced by the Prime Minister and President Biden in June this year as part of the Atlantic Declaration.

Data bridges

- The term ‘data bridge’ is our preferred public terminology for ‘adequacy’, and describes the decision to permit the flow of personal data from the UK to another country without the need for further safeguards. It symbolises the connection between destinations that is established by these decisions and encapsulates the UK’s collaborative approach with our international partners.
- Data bridges are not reciprocal, therefore they do not allow the free flow of data from other countries to the UK. Instead, a data bridge ensures that the level of protection for UK individuals’ personal data under UK GDPR is maintained.
- A data bridge assessment takes into account, amongst other things, the protection the country provides for personal data, the rule of law, respect for human rights and fundamental freedoms, and the existence and effective functioning of a regulator.
- Data bridges secure the free and safe exchange of personal data across borders, from the UK to another country. They unlock growth for businesses, allow us to share crucial information for life-saving research, and encourage science and innovation across borders. Reducing barriers to data sharing also makes things better for consumers, opening up opportunities for higher-quality services and lower prices on things they pay for.

Data Privacy Framework

- The EU-US Data Privacy Framework is a bespoke, opt-in certification scheme for US companies, enforced by the Federal Trade Commission (FTC) and Department of Transportation (DoT), and administered by the Department of Commerce (DoC).
- The Data Privacy Framework includes a set of enforceable principles and requirements that must be certified to, and complied with, in order for US

organisations to be able to join the Data Privacy Framework. These principles take the form of commitments to data protection and govern how an organisation uses, collects and discloses personal data.

- This replaces the previous Privacy Shield framework, established in 2016 to provide a legal basis for companies to comply with EU data protection requirements when transferring personal data to the US.
- The UK has established a data bridge for the “UK Extension to the Data Privacy Framework” that allows certified US companies to sign-up to be able to receive UK personal data through the framework.
- We will continue to monitor the Data Privacy Framework to ensure that it functions as intended, as part of the Department for Science, Innovation and Technology (DSIT’s) requirement to monitor data bridges.
- The US ‘designation’ of the UK relates to the US Executive Order 14086 (“Enhancing Safeguards for United States Signals Intelligence Activities”) which created an independent and binding redress mechanism which can be accessed by individuals whose personal data is transferred from qualifying states.
- The UK’s designation as a qualifying state therefore allows UK individuals to seek redress if they believe their personal data was collected or processed through US signals intelligence in a manner that violated applicable US law.
- This is a new and important safeguard that the US introduced to address the concerns raised in the 2020 Schrems II judgment, in preparation for the operationalisation of the new Data Privacy Framework.
- Designation by the US of the UK was an important factor that led to the data bridge assessment being successful, providing increased safeguards and redress mechanisms for UK individuals.

Privacy

- A data bridge ensures high protection for UK individuals when their data is transferred to another country. As discussed above, the US has introduced new rules and practices relating to government access to data which the UK has access to as a designated country.
- In establishing this data bridge, we have taken steps to ensure the level of protection people in the UK enjoy under the UK GDPR is not undermined. That includes closely assessing the level of protection of personal data under the Data Privacy Framework, as well as the wider legal and regulatory system. The US data bridge will ensure that high standards of protection for personal data are maintained when the data is sent to certified US organisations. Any US company that elects to receive UK data under the data bridge will be required to maintain those standards.
- Protecting individuals' privacy – particularly when it comes to their most sensitive information – is paramount. Under the data bridge, the level of protection your personal data has within UK GDPR will be maintained
- The data bridge will not remove the obligations of UK companies under UK data protection law to ensure that data, especially sensitive health data, is properly protected and the rights of data subjects upheld, including when they make decisions about transferring data to other organisations. The data bridge will ensure that these high standards of protection and privacy travel with the data when it leaves the UK to reach certified US organisations.

If you would like more information about UK GDPR, please visit the website of the [Information Commissioner's Office \(https://ico.org.uk/\)](https://ico.org.uk/) (ICO), the UK's independent data regulator.

[↑ Back to top](#)

OGL

All content is available under the Open Government Licence v3.0, except where otherwise stated

© Crown copyright