Title: Data Protection (Adequacy) (United States of America) Regulations 2023 - UK Extension to the EU-US Data Privacy Framework **IA No:** **RPC Reference No:** RPC-DSIT-5287(1) **Lead department or agency:** Department for Science, Innovation and Technology **Other departments or agencies:**	**Impact Assessment (IA)** **Date:** 20/09/2023 **Stage:** Final **Source of intervention:** Domestic **Type of measure:** Secondary **Enquiries:** data-adequacy-queries@dcms.gov.uk; vince.weaver@dsit.gov.uk

Summary: Intervention and Options

RPC Opinion: Fit for purpose

Cost of Preferred (or more likely) Option (in 2019 prices, 2020 present value)			
Total Net Present Social Value	**Business Net Present Value**	**Net Cost to Business per Year**	**Business Impact Target Status** Qualifying
£893.0m	£884.9m	-£78.4m	

What is the problem under consideration? Why is government action or intervention necessary?

1. The free flow of data underpins our everyday activities and experiences as well as our modern economies. As a world leader in digital, the UK champions free trade and a rules-based international system. Enabling international data transfers requires the free and secure exchange of data across borders.
2. The Data Protection Act 2018 includes provisions, which are set out in Sections 17A and 74A, that allow the UK to undertake assessments of countries' and jurisdictions' data protection legislation for the purpose of making data adequacy regulations for those countries.[1]
3. Adequacy regulations are made by the Secretary of State and specify individual countries, sectors or international organisations that the Secretary of State considers to ensure an adequate level of protection of personal data. It is the most straightforward mechanism for transferring personal data overseas and can also provide greater certainty and confidence in the regulatory landscape of another country. When a country is found 'adequate', UK-based organisations can transfer personal data to that country without restriction, subject to the terms of the adequacy regulations. In practice this means organisations (of any size) will not be required to put in place contractual safeguards, which come at a cost to organisations.
4. A decision by the Secretary of State to make adequacy regulations will also involve preserving trust and confidence that the level of protection of personal data, when transferring personal data to those countries, will not be undermined.
5. There is no way in which the market itself, or any stakeholder(s), would be able to introduce their own adequacy regulations. Whilst it is possible for businesses and organisations to put in place safeguards and contractual mechanisms to allow for the transfer of personal data, achieving the same intended outcome, adequacy regulations will relieve business and organisations of that burden. This will specifically benefit SMEs. The policy should reduce transaction costs due to the practical changes in compliance costs but also through the information signal that a country's data protection is adequate

[1] Replacing adequacy, 'data bridge' is the term now used by the UK government to describe the trusted flow of data from the UK to a third country without restrictions. However, for the purposes of this document, the legal term of adequacy is used throughout.

What are the policy objectives of the action or intervention and the intended effects?

- The primary policy objective is to reduce barriers and burdens (cost and resource) to organisations transferring personal data internationally.
- The Government is committed to providing trust and confidence that the level of protection of personal data is not undermined when personal data is transferred to other countries.
- To significantly increase the number of 'adequate' countries, to which organisations and Government can transfer personal data.
- Promote global interoperability of data protection frameworks to offset the risk of deeper global fragmentation on data issues.
- Proactively influence the global narrative on international data transfers.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details below)

- **Option 0 - Do nothing:** data transfers between the UK and third countries require 'alternative transfer mechanisms' (which are predominantly legal agreements between organisations). Some types of economic activity require data transfers. As such, there are necessary time, compliance and legal costs relating to the transfer of data to third countries before these economic activities can take place. Not to make adequacy regulations with the US would continue to expose businesses and organisations to the costs of alternative transfer mechanisms. This option would not address some of the key issues which previously invalidated the former US framework - Privacy Shield, since the UK will only be designated as a country that can access the new redress mechanism (created to address Privacy Shield criticisms) if it makes adequacy regulations for the Data Privacy Framework.

- **Option 1 - Grant adequacy status to the UK Extension to the Data Protection Framework:** adequacy regulations remove barriers for UK organisations to transfer personal data to US entities who have certified to the UK Extension to the Data Privacy Framework. The new Executive Order addresses concerns which previously invalidated the Privacy Shield, in order to ensure that the Data Privacy Framework meets the required data protection standards for UK adequacy. The UK will receive the benefits of the new redress mechanism now it is designated by the US: this will be on the basis that the UK permits data transfers to US organisations certified to the UK Extension to the Data Privacy Framework.

Is this measure likely to impact international trade and investment?		Yes		
Are any of these organisations in scope?	**Micro** Yes	**Small** Yes	**Medium** Yes	**Large** Yes
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)		**Traded: N/A**	**Non-traded: N/A**	

Will the policy be evaluated? It will. **If applicable, set review date:** Evaluation within 5 years.

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by senior analyst: Sarah Bingham Date: 20/09/2023

Signed by the responsible minister: Secretary of State Date: 20/09/2023

Summary: Analysis & Evidence

Policy Option 1

Description:

FULL ECONOMIC ASSESSMENT

Price Base Year 2019	PV Base Year 2020	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: 313.4	High: 1933.8	Best Estimate: 893.0

COSTS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	1.2	1	1.1	10.4
High	0.4		0.3	2.7
Best Estimate	0.8		0.4	8.4

Description and scale of key monetised costs by 'main affected groups'

The most substantial monetised costs are one-off familiarisation costs for private, government and non-profit organisations who:
a) currently transfer personal data to the US and
b) use standard data protection clauses.

These organisations will incur familiarisation costs in assessing what requirements the adequacy decision removes, through reading of ICO guidance as well as assessing whether recipients have signed up to the UK Extension to the Data Privacy Framework. These costs are estimated at £972,000 for the private sector, £6,100 for central and local government and £23,000 for non-profits.

There are also ongoing costs in re-verifying that recipients are signed up to the UK Extension to the Data Privacy Framework on an annual basis. We estimate these to be £200,000 for the private sector, £1,200 for central and local government and £4,800 for non-profits.

Lastly, there are also implementation costs for organisations who will have to update Data Privacy Notices. We estimate these costs to be around £428,500 for private sector organisations, £2,700 for central and local government and £6,800 for non-profits.

Other key non-monetised costs by 'main affected groups'

As it is likely that the regulations will lead to more data transfers, this could be perceived as creating more risks to privacy and security. However, the additional safeguards and new redress mechanisms implemented (under the US Executive Order 14086) for the Data Privacy Framework strengthen the protections available to UK data subjects whose data is transferred to the US.

BENEFITS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	0.0	N/A	37.0	316.1
High	0.0		227.7	1944.2
Best Estimate	0.0		105.6	901.4

Description and scale of key monetised benefits by 'main affected groups'
The main benefit is the removal of requirements to put standard data protection clauses in place to enable personal data transfers. In total we estimate a benefit of £84.1m a year to private sector businesses, £1.2m for government (central and local) and £2.7m for non-profit organisations. Increased exports, due to the reduced costs of putting standard data protection clauses in place, is estimated at £26.6m a year.
Other key non-monetised benefits by 'main affected groups'
There will be benefits to wider supply chains through businesses using services that benefit from US data transfers. There are likely additional benefits to both the private and public sectors such as an increased incentive to undertake research and development that are not captured in the removal of standard data protection clauses.
Key assumptions/sensitivities/risks **Discount rate (%) 3.5**
The underlying evidence base uses a range of surveys including the UK Business Data Survey. Where possible, parameters are split out by business size. Where assumptions have been used, we have undertaken sensitivity analysis in order to test these, taking these key assumptions in turn: ● The emerging evidence on continued sign-ups to the UK Extension to the Data Privacy Framework by US businesses suggests that assuming a 47.6% uptake of US organisations who receive UK personal data is justified. However, there is still uncertainty around this percentage which may have an impact on the realised Net Present Value. ● Another source of uncertainty is the assumed sectoral coverage of 80.4% of transfers and trade that go to US businesses based on the sectors of UK exporters as data on the sectors of US recipients is not available. ● The assumption that 23.4% of those organisations who currently send personal data to the US will be risk averse due to legal uncertainty and continue to use standard data protection clauses is based on evidence from EU transfers. However, the assumption may be too conservative as many businesses reverted to using standard data protection clauses for EU transfers due to the previous risk of no-deal Brexit. ● All three adjustments are conservative as they do not reflect that the value of trade disproportionately falls on the largest businesses so are more likely to utilise the Data Privacy Framework. ● The 95% confidence intervals for the UK Extension to the Data Privacy Framework take-up by US businesses and risk aversion are used in the low and high sensitivities. ● The government and non-profit benefits are derived by assuming the proportion of these organisations behave similarly to private sector organisations. Use of data transfers will vary by type of organisation but the underlying evidence base is focused on the private sector. ● A switching analysis is undertaken to indicate the scale at which the adjustments would have to be reduced for this assessment to not be positive in net-benefits, finding the total adjustment factor would have to fall from 29.4% to 0.6% in the central scenario.

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			**Score for Business Impact Target (qualifying provisions only) £m:**
Costs: 1.0	**Benefits:**79.3	**Net:** -78.4	-391.9

1.0 Policy Rationale

Introduction

6. It was agreed that following the submission and Regulatory Policy Committee (RPC) approval of the Rest of the World Adequacy Umbrella Impact Assessment,[2] individual country Impact

[2]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1118604/DCMS_RoW_Adequacy_Umbrella_Impact_Assessment.pdf

Assessments (IA) would be submitted as necessary. Not all individual country assessments will meet the threshold necessary for submission of an IA to the RPC as some will be below the de minimis threshold and will be subject to proportionate assessment within the department. A previous version of this Impact Assessment was green-rated by the RPC in September 2022. Following the conclusion of the technical assessment of the UK Extension to the EU-US Data Privacy Framework[3] (referred to henceforth as the "Data Privacy Framework"), the IA has been updated to reflect the policy detail of the finalised Data Privacy Framework. The analysis has also been refined to reflect the latest survey evidence, methodology and qualitative impacts.

7. An assessment of the Data Privacy Framework in light of changes made to US laws and practices surrounding government access to data has come to a conclusion, following which a recommendation was made to the Secretary of State to make adequacy regulations. Regulations have been made in accordance with Section 17A of the Data Protection Act 2018.

8. This IA estimates the benefits for UK organisations following adequacy regulations being made in respect of the Data Privacy Framework. These benefits are the reduction in compliance costs from putting in place alternative transfer mechanisms and an estimate of the potential indirect increase in trade is made as a result. Currently, UK businesses mostly use standard data protection clauses, such as the International Data Transfer Agreement (IDTA) and EU Standard Contractual Clauses (SCCs),[4] and as a result this IA does not include other less common alternative transfer mechanisms, such as binding corporate rules and derogations in its assessment. Wider impacts and qualitative benefits are also explored. Familiarisation costs are estimated which represent the wage costs of reading any new guidance on what organisations no longer need to do as well as identifying whether US-based businesses have certified to the UK Extension to the Data Privacy Framework. An ongoing cost is estimated as UK organisations will be required to verify whether existing or new recipients of UK personal data are signed up to the Framework. Lastly, an ongoing implementation cost is estimated from changes to Data Privacy Notices, which require notifying the specific transfer mechanism being used to send data internationally.

Data Adequacy

9. Adequacy regulations are made by the Secretary of State and specify individual countries, sectors or international organisations that the Secretary of State considers to ensure an adequate level of protection of personal data. It is the most straightforward mechanism for transferring personal data and can also provide greater certainty and confidence in the regulatory landscape of another country. When a country is found 'adequate', UK-based organisations can transfer personal data to that country without additional safeguards.

10. UK organisations of all sizes and across all sectors rely on various services from overseas, such as email marketing, online retail, and communication platforms, and cloud storage in order to grow, collaborate, and innovate in a cost-effective manner. Under UK adequacy regulations for the US, a

[3] https://www.dataprivacyframework.gov/

[4] From 21 March 2022, the ICO's IDTA took effect as a replacement for the EU SCCs. Transitional Provisions also entered into force on 21 March 2022, disapplying Paragraph 7 of Part 3 in Schedule 21 of the Data Protection Act 2018, to the extent necessary to give effect to the following: Contracts concluded on or before 21 September 2022 on the basis of any Transitional Standard Clauses shall continue to provide appropriate safeguards for the purpose of Article 46(1) of the UK GDPR until 21 March 2024, provided that the processing operations that are the subject matter of the contract remain unchanged and reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards. For the purposes of this analysis, the old EU SCCs and the IDTAs are treated as equivalent in terms of how they function and how much they cost to implement. The evidence base underpinning the analysis is all based on evidence regarding the old EU SCCs. DSIT is currently undertaking an evaluation of the change to verify this assumption.

UK business in the tech sector (for example), who relies on a cloud service provider in the US to carry out large-scale analysis of data, would no longer have to resort to potentially costly and burdensome alternative transfer mechanisms to share UK personal data in a safe and secure manner.

11. The UK government has prioritised a number of countries for potential data partnerships; **Australia**, **Colombia**, **Dubai International Financial Centre**, **Singapore** and the **United States of America**. Longer term priority partners are: **Brazil**, **India**, **Indonesia**, and **Kenya**. Adequacy regulations for the **Republic of Korea** entered into force in December 2022.

Legislation

12. Following the end of the Transition Period of the UK Exit from the European Union on 31 December 2020, Sections 17A and 74A of the Data Protection Act 2018 conferred powers on the Secretary of State to make adequacy regulations, in relation to general and law enforcement processing respectively.

13. This legislation empowers the Secretary of State to assess countries (in part or in full), territories or sectors within a country, or international organisations for adequacy, and empowers SoS to permit all transfers to those countries, territories or sectors, or international organisations, or just certain transfers. Sectoral adequacy decisions may be important if country-wide adequacy is not appropriate (e.g. finance or health).

14. To give legal effect to a decision to specify a country as ‘adequate’, the Secretary of State must make regulations and lay these in Parliament. Once laid in Parliament, the adequacy regulations will be subject to the ‘negative resolution’ procedure.

2.0 Assessment

15. The UK’s test for adequacy as set out under Article 45 of the UK GDPR ensures the level of protection under the UK GDPR is not undermined. To determine this, the overall effect of a third country’s data protection laws is considered, including implementation, enforcement, and supervision. This involves systematically looking at the third country’s data protection laws and practices, making use of external expertise and insights from country partners

16. When understanding how a third country protects personal data the following factors - amongst other things - are taken into account:

    a. The rule of law, respect for human rights and fundamental freedoms, and the access of public authorities to personal data.

    b. The existence and effective functioning of an independent regulator.

    c. Relevant international commitments.

17. A respectful and considerate approach is taken, noting that necessary and proportionate interference with the right to privacy can be justified in order to protect the public and is compatible with high standards on privacy.

Assessment of the Data Privacy Framework

Context on the US' data protection framework and transatlantic data transfers

18. The US does not have federal all-sector privacy legislation. Instead, the US has multiple sectoral laws which apply on a federal level. In order to permit the transfer of personal data, the EU-US Privacy Shield Framework (the "Privacy Shield") was set up by the European Commission and the US Department of Commerce ("DoC") in 2016 to provide a legal basis for companies to comply with EU data protection requirements when transferring personal data to the US. The Privacy Shield worked as a bespoke, opt-in certification scheme for US companies, enforced by the Federal Trade Commission ("FTC") and Department of Transport ("DoT"), and administered by the DoC. As an EU Member State at the time, thousands of British businesses relied on the Privacy Shield to transfer data to the US as it provided them with a simple and transparent means of legally transferring data to the US without additional, expensive administrative and legal burdens.

19. The Privacy Shield included a set of principles and requirements that had to be certified to, and complied with, in order for organisations to be able to opt in. These principles took the form of commitments to data protection and governed how an organisation used, collected and disclosed personal data. Though self-certification to the Privacy Shield was voluntary, once an organisation had made a public commitment to comply with the Privacy Shield requirements, those commitments became enforceable. The Privacy Shield provided thousands of British businesses with a simple and transparent means of legally transferring data to the US without additional, expensive administrative and legal burdens.

20. In July 2020, the Court of Justice of the European Union (CJEU) invalidated the EU's adequacy decision for the Privacy Shield, impacting data flows to the US, in what is most commonly known as the *Schrems II* judgment (after Max Schrems, an Austrian privacy activist who brought the case). This was on the basis of US National Security laws and practices. The UK government responded to the CJEU's decision in the *Schrems II* case in July 2020 and set out its commitment to support UK organisations on international data transfers.[5] Due to the Transition Period after EU Exit, this decision applied in the UK. This resulted in the UK having no adequacy decision in place for the US, requiring businesses to put in place costly alternative transfer mechanisms.

21. The *Schrems II* judgment had a significant impact on UK businesses transferring data to the US. The invalidation of the Privacy Shield, which certified over 5,000 organisations in the US (mostly SMEs), particularly impacted digitally-intensive industries that rely upon the sharing of personal data between the UK and US. It increased the burden on businesses and increased barriers to the transatlantic free flow of personal data. Without the Privacy Shield, the onus is now on individual companies to evaluate the risk and legality of any data transfers made between the UK and the US. In practical terms, this has meant reverting back to more costly transfer mechanisms such as standard data protection clauses as outlined by survey evidence below. The legal and financial burden on companies has meant that organisations will have been forced to pay additional compliance costs or, if unattainable as is likely the case for many SMEs, may have meant they are now unable to make data transfers to the US. Most companies lack the means to go through the complex and expensive procedures at an individual company level to ensure their transfer of data to the US meets the standards required.

[5] https://www.gov.uk/government/news/uk-government-response-to-the-european-court-of-justice-decision-in-the-schrems-ii-case

22. As a result of the *Schrems II* judgment there is increased uncertainty over the stability of transatlantic data transfers and the enforcement approach of data protection regulators, increasing the burdens and risks placed upon businesses. European regulators are still grappling with the implications of the judgment. As recently as May 2023, the Irish Data Protection Commission (DPC) issued a decision that Meta violated the EU GDPR through its use of Standard Contractual Clauses (SCCs) to transfer personal information from the EU to the US following the *Schrems II* decision. Although the decision does not apply in the UK, it demonstrates that the wider impact of *Schrems II* continues to be felt and has far-reaching impacts on businesses, including individuals and SMEs.

The new UK Extension to the EU-US Data Privacy Framework

23. To address the barriers to transatlantic data flows, the European Commission and US Department of Commerce announced in March 2022 that they had agreed in principle to the establishment of the EU-US Data Privacy Framework, a new self-certification mechanism to permit the transfer of personal data to the US. The European Commission formally adopted an adequacy decision for the EU-US Data Privacy Framework in July 2023.

24. The EU-US Data Privacy Framework replaces the Privacy Shield framework. The concerns raised in the *Schrems II* judgment which invalidated the Privacy Shield are now addressed by the US Executive Order ("EO") 14086 "Enhancing Safeguards for United States Signals Intelligence Activities."[6] This introduced and further strengthened privacy and civil liberties safeguards for US signals intelligence activities and created a new method of redress for persons whose personal data is transferred from countries that have been designated by the US, on the basis that those countries will permit data flow to the US - ie: that they have declared the US adequate. In particular, EO 14086:

    a. Introduces further safeguards in relation to when signals intelligence can be carried out, including requirements that US signals intelligence activities shall be "necessary" and "proportionate" to a "validated intelligence priority."

    b. Sets forth requirements for the handling of personal information collected through signals intelligence.

    c. Introduces a new two-tier redress mechanism for non-US persons to seek review of the US Intelligence Community's signals intelligence activities. As of 18th September 2023, the UK has been designated by the US as being able to access this mechanism. This mechanism will be accessible by all individuals whose personal data has been transferred from the UK to the US (including via other non-adequacy-based international transfer mechanisms under the UK's data protection regime).

25. Following detailed technical discussions with US counterparts, the US and UK have worked together to extend the protections of the EU-US Data Privacy Framework to the UK, and make it available to organisations in the UK to use as a legal basis for transfers to participating US entities by agreeing the UK Extension to the EU-US Data Privacy Framework. US entities certifying to the Data Privacy Framework will be able to opt in to the UK Extension and will be listed on the Data Privacy Framework List as participating in the UK Extension to the EU-US Data Privacy Framework.

[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

26. There is a clear rationale for creating a UK extension to the EU-US Data Privacy Framework instead of negotiating a separate framework for UK-US transfers:

    a. The UK government has heard from stakeholders about how important it is that there is a solid and seamless mechanism for data transfers to the US. Adequacy regulations for the new Data Privacy Framework are vitally important to: reduce the burdens for businesses; provide a simple and robust mechanism for transatlantic data transfers; safeguard the rights of UK data subjects; and support UK objectives on trade and security.

    b. The UK Extension to the Data Privacy Framework provides a simple means for US businesses who were previously certified to the Privacy Shield to sign up, reducing the administrative burden (and therefore uncertainty) around US businesses signing up to the framework. Many US businesses have been transferred across from the Privacy Shield to the new Data Privacy Framework. Currently,[7] 2,514 businesses have signed up to the EU-US Data Privacy Framework, with 802 signed up to the UK Extension ahead of the adequacy regulations coming into force. Given the minor changes required by businesses to opt-into the UK Extension, nearly 2,000 US organisations are well placed to sign-up to the UK Extension once regulations come into force.

    c. The new safeguards provided by EO 14086 will provide important protections to UK data subjects and address concerns raised by the *Schrems II* judgment, which is considered retained EU case law in the UK.

27. New businesses who wish to certify to the Data Privacy Framework have to self-certify to the DoC and pay a small certification fee to support the operation of the Data Privacy Framework program, which varies depending on an organisations annual revenue. This cost has remained constant since the Privacy Shield, and remains at most $3,250 per annum for the largest businesses (with an annual revenue over $5 billion) down to $250 per annum for the smallest ($0 to $5 million annual revenue).[8] As was the case under the Privacy Shield, their application must set out that they have internal procedures and policies in place to meet the Principles of the Data Privacy Framework, have put appropriate redress mechanisms in place to handle complaints, and confirm their regulatory jurisdiction under either the FTC or DoT. Organisations must publish a public privacy notice stating their adherence to the Data Privacy Framework at which point they are liable to enforcement action for violations. These self-certification requirements remain essentially the same as under the Privacy Shield and do not signal a change in the level of resource required by US businesses. It is therefore expected that the certification requirements will not impact uptake to the Data Privacy Framework.

28. Once the DoC have confirmed an organisation's self-certification is complete, it will place the organisation on the Data Privacy Framework List (DPF List), and if an organisation wishes to also opt-in to participate in the UK Extension this will be indicated on the DPF List. The UK's adequacy regulations specify that personal data will only be able to be transferred to US organisations which are indicated on the DPF List as participating in the UK Extension. An organisation must undergo an annual recertification to continue utilising the Data Privacy Framework.

29. The Data Privacy Framework can only be joined by organisations that are regulated by the FTC or the DoT. Similarly, US public sector bodies are not able to join the Data Privacy Framework as they sit outside of the regulatory jurisdiction of the FTC and DoT.

[7] As of 10 October 2023 (https://www.dataprivacyframework.gov/s/participant-search)
[8] https://www.dataprivacyframework.gov/s/article/FAQs-General-dpf

30. The Information Commissioner's Office (ICO) is the UK's independent data protection regulator and has specific roles under the Data Privacy Framework, including where necessary an advisory role as well. The ICO will act as the initial point of contact for individuals who wish to lodge a complaint with the DoC (who administer the Data Privacy Framework itself) and the FTC and DoT (who are the US regulatory authorities of the Data Privacy Framework). They also support the complaint process and continue to act as a liaison between UK data subjects and the new redress mechanism. Department for Science, Innovation and Technology ("DSIT") and the ICO have worked closely with relevant departments in the US government to establish contact points and routes of escalation to facilitate the smooth functioning of the new redress mechanism for UK data subjects. Under the previous adequacy decision for the Privacy Shield, the ICO performed a similar role to what will be required under the Data Privacy Framework. DSIT has worked closely with the ICO to ensure they are fully aware of their role once the adequacy regulations are in place and will continue to work closely with the ICO to ensure the adequacy regulations are functioning as expected. The ICO will liaise directly with the US Department of Justice, who have implemented the new redress mechanism, to facilitate the complaints process. This does not represent an increased burden on US or UK businesses.

The assessment process

31. A series of technical discussions with the US DoC were organised to understand the US' data protection laws and practices, as well as to line up the processes needed to "operationalise" the new Data Privacy Framework to encompass UK-US data transfers. This was complemented by further research and investigations into US laws and practices.

32. A further series of technical discussions were undertaken with the US to discuss changes that have been made to their national security laws and practices in order to raise and codify the standards of protection for personal data transferred from overseas and to formalise the US' designation of the UK as a qualifying state, which ensures UK data subjects may access the redress mechanism set out in EO 14086.

33. After collecting all the relevant information, DSIT assessors conducted an analysis of the data laws and practices that underpin the Data Privacy Framework, and have shared this analysis with the ICO.

Assessment findings

34. That the DSIT Secretary of State should make regulations under section 17A Data Protection Act 2018 specifying the UK Extension to the EU-US Data Privacy Framework as ensuring an adequate level of protection of personal data.

Interdependencies between the UK's data bridge and EU's adequacy decision

35. The decision taken by the UK to make adequacy regulations is independent and separate to the EU's already in force adequacy decision. The UK has conducted its own independent assessment and cannot rely on the EU's adequacy decision itself as a legal basis for UK-US transfers. If the European Commission decides for any reason in the future to amend, suspend or revoke its adequacy decision for the EU-US Data Privacy Framework, this will therefore not have an immediate effect on the UK's adequacy regulations for the UK Extension to the EU-US Data Privacy Framework. The UK has its own obligations as set out in the UK GDPR to review and monitor its adequacy regulations to ensure that the EU-US Data Privacy Framework continues to uphold high standards of data protection. The UK will monitor the Data Privacy Framework to

ensure that it continues to function as intended.[9]

36. Any future judgements by the CJEU regarding the EU's adequacy decision for the EU-US Data Privacy Framework will not directly affect the UK's adequacy regulations. If the CJEU invalidates the EU's adequacy decision for the EU-US Data Privacy Framework, UK organisations will continue to be able to rely on the UK extension to the EU-US Data Privacy Framework to transfer data to the US.

37. The UK's adequacy regulations can only be challenged in UK courts. The possibility that a legal challenge will be brought against the Secretary of State's decision to make adequacy regulations for the UK Extension to the EU-US Data Privacy Framework cannot be ruled out. Privacy concerns are an increasing focus for litigation, and there have already been two successful challenges in the EU courts (*Schrems I* and *Schrems II*) that were brought against the EU's previous adequacy decisions for data transfers to the US. In the event of a successful challenge in the UK courts quashing the adequacy regulations, organisations would be able to revert to using mechanisms such as standard data protection clauses to undertake transfers, facing the same costs as they currently do without the Data Privacy Framework (the counterfactual).

38. With regard to the EU's adequacy decisions for the UK, it is highly unlikely that UK adequacy regulations for the UK Extension to the EU-US Data Privacy Framework would pose risks to the maintenance of the EU's adequacy decisions for the UK as the EU has already found the same framework adequate. However, future risks may arise if the UK and EU approaches no longer align, for example in a scenario where the EU's adequacy decision for the EU-US Data Privacy Framework is invalidated by the CJEU or revoked by the European Commission. In this scenario, the UK government would engage closely with the EU to ensure that any potential risks are mitigated.

3.0 Problem under consideration

39. Currently, businesses are required to put in place alternative transfer mechanisms and undertake activities that add compliance and legal costs when transferring data to countries without adequacy regulations. For example, businesses may choose not to trade with the US if the regulatory costs associated with sending data to facilitate trade are greater than potential profits. Evidence from the UKBDS (see Table 1) shows the average total annual costs businesses who currently use standard data protection clauses face is £6798, which increases with business size, reflecting that more clauses are put in place by larger businesses. Therefore, there is a strong rationale for the UK to make adequacy regulations for the Data Privacy Framework as a mechanism for transatlantic personal data flows. As demonstrated through the UK's assessment of the Data Privacy Framework, the Data Privacy Framework provides an adequate level of protection to UK individuals, removing the need for individual organisations to make their own assessment.

Table 1: Total standard data protection clause cost per business by business size

	Sole Trader	Micro	Small	Medium	Large	Weighted Average
Total standard data	£6,029.8	£6,050.2	£11,815.0	£10,446.4	£23,283.1	£6,797.7

[9] If developments such as changes to legislation or specific practices negatively impact data protection standards, the government will engage with the relevant authorities in the country to better understand the developments and work with the authorities to address any issues of concern. If these cannot be resolved and the Secretary of State considers that the country no longer provides an adequate level of protection, the Secretary of State will be required to amend or revoke the regulations .

protection clause cost estimate per business						

40. Assessment of business-level productivity data in the UK shows that businesses trading internationally have higher productivity than those that do not. This may indicate that cost barriers to trade are restricting businesses, especially the smallest in productivity growth.[10] When costs are prohibitive, businesses may choose not to send data internationally. Similarly, the uncertainty and complexities of engaging with alternative transfer mechanisms could therefore be seen as a non-tariff barrier to trade, and detrimental to businesses' productivity, especially the smallest businesses who may be disproportionately affected by legal and compliance costs.

41. Currently, there is an imperfect information problem as businesses have to individually assess whether recipients of data maintain the high standards required under UK GDPR and put alternative transfer mechanisms, such as standard data protection clauses, in place to sufficiently protect data. Adequacy is the most efficient way to freely transfer personal data as it removes the need for UK organisations to use alternative transfer mechanisms, which can be costly and burdensome to implement. Adequacy can also provide consumers and organisations greater certainty and confidence in the regulatory landscape of another country.

4.0 Rationale for Intervention

42. There are strong trade and diplomatic considerations in favour of adequacy regulations for the Data Privacy Framework. Adequacy regulations for the Data Privacy Framework will support UK objectives on trade, opening up the US market to businesses of all sizes across the UK. Cross-border data flows are an important facilitator of digital trade in goods and services to and from the US. The US is the UK's largest trading partner country both overall and in data-enabled services exports. 89% of the UK's service exports to the US are data-enabled, amounting to £99bn or 32% of the UK's global data-enabled services exports. The government is working to remove barriers with the US to enable easier data-enabled flows and help support this already strong trading relationship.[11] As the largest economy in the world based on GDP, the benefits of a closer data partnership between the US and UK would be significant for British businesses.

43. The UK and US have over £700 billion invested in each other's economies, with over a million Britons and over a million Americans working for organisations from the other nation.[12] Adequacy regulations for the US would assist the UK in realising its public ambitions to be a more pragmatic and business-friendly data partner to key like-minded countries.

Policy objectives

44. The policy objectives of the action or intervention and the intended effects are:
    a. The primary policy objective is to reduce barriers and burdens (cost and resource) to organisations transferring personal data internationally.
    b. The government is committed to providing trust and confidence that the level of protection for personal data will not be undermined when it is transferred to other countries.

[10] Business-level labour productivity measures from the Annual Business Survey, UK: 1998 to 2019, ONS 2022

[11] https://www.gov.uk/government/news/uk-unveils-post-brexit-global-data-plans-to-boost-growth-increase-trade-and-improve-healthcare

[12] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/869592/UK_US_FTA_negotiations.pdf

c. To significantly increase the number of ‘adequate’ countries, to which organisations and government can transfer personal data.
d. Promote global interoperability of data protection frameworks to offset the risk of deeper global fragmentation on data issues.
e. Proactively influence the global narrative on international data transfers.

5.0 Description of options considered

45. The Secretary of State’s decision over whether to lay adequacy regulations for the Data Privacy Framework is a binary choice. The use of alternative transfer mechanisms by organisations is factored into the ‘do nothing’ option. The US is not currently a suitable candidate for a comprehensive adequacy assessment due to the lack of federal privacy legislation.

46. In this IA, two options are considered:

- **Option 0 - Do nothing:** data transfers between the UK and third countries require alternative transfer mechanisms, primarily standard data protection clauses such as IDTAs before restricted data transfers are permitted. To enable certain types of trade, data transfer is required which involves time and legal costs. Some businesses currently cannot trade as compliance costs are higher than the potential profits made from trade. Not to make adequacy regulations would continue to expose businesses and organisations to the costs of alternative transfer mechanisms and prohibit smaller businesses from exploring opportunities overseas. This option would not address some of the key issues raised in *Schrems II* concerning US national security laws and practices. The UK will only be designated as a country that can access the redress mechanism if it makes adequacy regulations for the Data Privacy Framework.

- **Option 1 - Grant adequacy status to the Data Protection Framework:** adequacy regulations remove the requirement for alternative transfer mechanisms such as IDTAs, thereby removing barriers to transfer personal data under the Data Privacy Framework to the United States. UK organisations will only be able to transfer to US entities who have certified to the Data Privacy Framework. The new Executive Order addresses concerns which previously invalidated the Privacy Shield, in order to ensure that the Data Privacy Framework meets the required data protection standards for UK adequacy. The UK will receive the benefits of the new redress mechanism now it has been designated by the US: this will be on the basis that the UK permits data transfers to US organisations designated under the Data Privacy Framework.

6.0 Cost & Benefits

Summary

47. The assessment follows Green Book principles. A net present value (NPV) for the case of the UK granting the US data adequacy has been calculated using 2022 prices and 2023 as its present value (when benefits/costs begin) with a 10-year appraisal period and 3.5% discount rate. The impact has been converted to 2019 prices and 2020 present value with a best estimate of having a total net present social value of £893.0m with a sensitivity range of between £313.4m and £1,933.8m.

48. It is estimated that around 54,300 businesses[13] will be impacted by the familiarisation costs in understanding the new framework. As outlined below, not all of those currently sending personal data to the US will benefit as some will remain risk-averse using standard data protection clauses as seen with EU transfers, US recipients are required to sign-up and not all sectors are covered. 96% of the costs accrue to small or micro businesses.

49. About 16,000 businesses will directly benefit from the reduction in standard data protection clause costs in moving to the Data Privacy Framework for future data transfers, 96% of them being small or micro organisations. A slightly smaller proportion of benefits, 92% accrue to small or micro reflecting that larger businesses currently spend more on standard data protection clauses. More businesses will also be impacted indirectly by the reduction of non-tariff trade barriers, disproportionately affecting smaller businesses. However, this has not been estimated as detailed data on the business size break-down of trade across all sectors was not available. The impacted businesses will be across a number of UK sectors, but more data intensive industries such as professional services and manufacturing will likely be disproportionately impacted.

50. The total benefits estimate comprises two elements:

    a. The removal of the cost of implementing new standard data protection clauses to businesses, the UK public sector and non-profit organisations .

    b. The realisation of additional revenue that is currently suppressed, due to this cost acting as a non-tariff barrier.

51. The estimate of the monetised cost consists of familiarisation costs to all organisations who currently use standard data protection clauses for transfer to the US in understanding what requirements adequacy removes and verifying that a recipient is certified. The requirement to verify recipients is an ongoing cost. Additionally organisations who choose to use the Data Privacy Framework face ongoing costs in updating Data Privacy Notices as it is required to ensure the mechanism used to transfer data internationally is outlined. There is short and clear guidance available on the ICO website for organisations to follow in order to comply with adequacy regulations.[14]

52. The focus of the analysis is UK organisations that send data to US businesses as well as those UK businesses who are currently dissuaded from trading with the US due to the compliance barriers. The impacts are under the assumption that businesses do not retrospectively move from standard data protection clauses already in place to the Data Privacy Framework. Instead, as new organisational relationships emerge and create new recipients of personal data or old contracts become outdated, these are replaced by use of the Data Privacy Framework. Trade benefits estimate the amount of trade that is currently suppressed due to compliance and legal costs (from the requirement of alternative transfer mechanisms). One aim of the policy is to increase the number of businesses that trade with the US with the lowering of trading costs.

53. The total annual costs of standard data protection clauses implemented by UK organisations for the specific purpose of sending data to the US has been estimated. The removal of standard data protection clauses in the case of US adequacy will free up this cost for UK traders transferring to US businesses certified to the Data Privacy Framework, allowing firms to allocate their financial

[13] This is the estimated total number of businesses that send personal data, use standard data protection clauses and state the US is an important country to transfer data to, equivalent to 0.9% of all businesses. UKBDS 2022 and ONS Business Population Estimates, 2023.

[14] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/

resources elsewhere, such as expansion or research and development. Whilst the regulations will also remove the need for other less common alternative transfer mechanisms, leading to additional benefits, the underlying evidence base does not exist to reliably estimate the costs averted. As a result, the quantified benefits are likely underestimated however it is likely these are marginal.

54. The UK Business Data Survey (UKBDS) is used to estimate the proportion of those who send personal data and use standard data protection clauses to update the top-down estimate calculated in the Rest of World (RoW) Umbrella Impact Assessment. 1.5% **of all UK businesses** (about 80,800) send personal data to the rest of the world and use SCCs with a range of 1.0% and 2.0% as the 95% confidence intervals. The use of these estimates drive the main differences in the sensitivity analysis of the IDTA benefits.

55. Bespoke YouGov surveys are used to estimate a proportion of UK exporters currently reliant on sending data to the US.[15] These allow an estimate of the number of businesses currently having to use standard data protection clauses to conduct trade with the US. An estimate of data-dependent trade is used to estimate the amount of trade that is currently suppressed due to non-tariff barriers. Latest trade data is used to reflect the changes in the UK's trading relationships. US-specific estimates of data-dependence are higher than the rest-of-the-world average.[16]

56. To measure the impact on central and local government and non-profit organisations, we extrapolate private sector benefits based on the profile of these organisations by employee size using ONS Business Population Estimates. The underlying evidence base is business-focused (such as the UKBDS) so the estimates make some key assumptions such as the use of standard data protection clauses and the cost of doing so (including the wage costs) being the same among all types of organisations. The reasons for transferring data are likely to differ by organisation type, for example private sector focused on enabling trade whilst public sector may be more focused on improving public services. The simple uplift approach therefore may under or overestimate the impacts for public sector organisations.

57. Given uncertainty in underlying parameters and survey evidence, sensitivity analysis is undertaken and ranges are presented below. We make three adjustments, which all reduce the net benefits: accounting for some sectors being out of scope; estimating scale of uptake of DPF; and estimating risk averse behaviour of businesses.[17]

    a. **Sectors in scope.** The Data Privacy Framework is only able to be joined by organisations within sectors regulated by the FTC and DoT - that is, banks, federal credit unions, and savings & loan institutions and 'common carriers.' These sectors make up to 19.6% of total UK-US exports: as a result, we reduce trade figures used to apportion IDTA benefits and suppressed trade by 80.4%.[18]

    b. **Scale of Data Privacy Framework uptake.** The estimated figures are adjusted for the amount of data-sharing that may still require alternative transfer mechanisms as the Data Privacy

[15] Outputs used from the survey are published: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1118371/DCMS_Data_Policy_YouGov_Surveys.ods

[16] Data dependency is defined as the percentage of businesses who transfer data with the named countries who stated 'Personal data transfers to/from this country are essential to core or important secondary functions of my business' model'

[17] These parameters are key to the calculation of the EANDCB. A full exploration of the impact of the assumptions on the NPV is explored in Table 5.

[18] Ideally, end-use trade figures, the proportion of UK exports going to US business in non-covered sectors would be used rather than the industry of UK exporters. However, this data does not exist. A simplifying assumption that the exporting industry is the same as the receiving industry in the US is used instead.

Framework requires US businesses to opt-in. When the Privacy Shield was fully operational before 2020, an estimated 47.6% of US traders who received UK personal data and imported UK goods or services were participants. As a result, up to 52.3% of UK data exporters could still require alternative transfer mechanisms and similarly reduce the increased export benefits. However, the parameter is likely conservative, as large firms account for proportionally more trade and so it is likely that the very largest importers will have an incentive to sign up to the DPF. Similarly, the NPV could be underestimated in future years as it is likely that more US businesses adopt the Data Privacy Framework over the full appraisal period of 10 years. In real terms, the costs of signing up to the Data Privacy Framework compared to the US Privacy Shield have fallen as there are no changes in the certification costs for US Businesses compared to the US Privacy Shield in 2019 when survey evidence was collected which may further increase take-up. The increased redress mechanisms compared to the US Privacy Shield add costs to US regulators with no extra compliance or monitoring costs accruing to US businesses. Currently, these additional regulator costs are not being recovered via higher certification costs. The parameter remains a good estimate of the expected proportion of affected US traders with the UK. Approximately 2,500 businesses remained signed up to the Privacy Shield (about half of those at time of it being invalidated) in anticipation of a new framework, despite an adequacy decision not being in place after the Privacy Shield was struck down. Additionally, the US government plans to publicise and undertake business engagements to increase uptake. A significant number of businesses have already signed up to the EU-US Data Privacy Framework, businesses will be easily able to make use of the UK Extension. It is likely this will continue to increase as UK regulations are put in place. Conversely, the take-up of the Data Privacy Framework is related to the EU-US Data Privacy Framework, in the event of legal challenge against it, US businesses may have less incentive to sign up to the UK extension as the fee is the same but with less options. We use the 95% confidence intervals from the survey evidence to adjust for parameter uncertainty in the low and high sensitivity scenarios.

c. **Risk aversion of businesses**. One potential risk is if a significant portion of businesses may be risk averse and maintain using standard data protection clauses even in the event of adequacy regulations being made. As stated in paragraph 37, there is a risk of legal challenge being brought to the adequacy regulations in the UK courts. Although the UK's decision is independent from the EU's, which means that any challenge brought against the EU-US Data Privacy Framework in the CJEU would not affect the adequacy regulations themselves, businesses may perceive legal risks and uncertainty in the event of such a challenge, resulting in less usage of the Data Privacy Framework. From the UKBDS, we estimate the proportion of businesses who send personal data to the EU and still use standard data protection clauses at 23.2%. As a result, we further adjust the impacts by an estimated 76.8% to reflect that despite adequacy regulations being in place, some businesses will continue using standard data protection clauses. However, the EU-focused evidence for this parameter is affected by no-deal EU exit planning as the UK Government communicated to businesses that they should put in place standard data protection clauses to maintain data transfers in the event of no deal.[19] As a result, this may mean the central parameter is an overestimate. Conversely, if legal challenges are made against the EU-US Data Privacy Framework, businesses in the UK may choose to become more risk-averse and maintain use of standard data protection clauses. We use the 95% confidence intervals to reflect the parameter uncertainty.

[19] https://ico.org.uk/media/for-organisations/data-protection-and-brexit/data-protection-if-theres-no-brexit-deal-1-0.pdf

58. These three combined adjustments (80.4% sectoral, 47.6% Data Privacy Framework usage in the US and 76.8% who choose to use the Data Privacy Framework as the mechanism in the UK) creates a factor of 29.4%. The sectoral adjustment is used across all sensitivities, the Data Privacy Framework sign-up by US businesses varies by 40.2% to 55.0% between the low and the high and the risk-aversion of UK organisations varies by 6% to 41.5% so creates a factor of 59.5% to 94.0% between the low and high scenarios. These create total adjustment factors in the low and high scenarios of 19.2% and 41.6% respectively.

59. The trade suppression ratio varies based on the underlying assumptions in the UK Business Impacts Model. The varying assumptions are used here to represent uncertainty in that underlying model. The average data-dependency for the rest of the world of 14% from the International Transfer Tools survey is used for the US in the low scenario (see table 1 below).

Table 2: Data adequacy model annual results summary (£m), 2022 prices

Impact	Best	Low	High
Costs			
Familiarisation Costs (Transition)			
Private Sector	£1.0m	£1.5m	£0.5m
Central and Local Government	£0.006m	£0.009m	£0.003m
Non-Profits	£0.023m	£0.035m	£0.012m
Data Privacy Notices Implementation Costs (Annual)			
Private Sector	£0.4m	£0.9m	£0.1m
Central and Local Government	£0.003m	£0.005m	£0.0009m
Non-Profits	£0.007m	£0.022m	£0.003m
Total Year 1 Costs	£1.4m	£2.4m	£0.6m
Data Privacy Framework Verification (Annual from Year 2)			
Private Sector	£0.2m	£0.2m	£0.2m
Central and Local Government	£0.001m	£0.002m	£0.001m
Non-Profits	£0.005m	£0.006m	£0.004m

Benefits			
Standard Data Protection Clauses (Annual)			
Private Sector	£84.1m	£26.9m	£173.5m
Central and Local Government	£1.2m	£0.4m	£2.4m
Non-Profits	£2.7m	£1.0m	£5.4m
Trade Suppression (Annual)			
Private Sector	£26.6m	£11.9m	£65.6m
Total Benefits	£114.5m	£40.2m	£247.0m

60. The combined annual benefits of reduction in annual standard data protection clauses costs for the private sector (£84.1m), central and local government (£1.2m) and non-profit sector (£2.7m) and annual increase in exports (£26.6m) gives an estimated total annual benefit to UK organisations of £114.5m.

61. The low estimates indicate £26.9m in private sector benefits, £0.4m in central and local government benefits, £1.0m in non-profit benefits and £11.9m in suppressed exports.The high estimates indicate £173.5m in private sector benefits, £2.4m in central and local government benefits, £5.4m in non-profit benefits and £65.6m in suppressed exports.

62. Organisations incur a cost as they familiarise themselves with the Data Privacy Framework and understand the particular requirements for US recipients before undertaking the data transfer. These costs have been estimated as a one-off cost of £1.0m of which £971,900 is associated with the private sector, £6,100 with central and local government and £23,200 is associated with the non-profit sector. An ongoing cost in future years to verify US recipients are certified is estimated at £206,000 of which £200,000 is associated with the private sector, £1,200 to government and £4,800 to non-profits. Qualitative costs and benefits are also assessed. A familiarisation cost will be needed to verify whether US businesses have signed up to the Data Privacy Framework.

63. Adequacy regulations will be beneficial to political, scientific and research relationships between the UK and the US potentially leading to onward innovation benefits. While the transfer of personal data by its nature includes a level of risk, the aim of an adequacy assessment is to ensure that the level of protection for data subjects is not undermined when their data is transferred to a country under an adequacy decision. As it is likely that the regulations will lead to more data transfers, this could be perceived as creating more risks to privacy and security. However, the additional safeguards and new redress mechanisms implemented by the US strengthens the protections available to UK data subjects and have been analysed in detail as part of the UK's adequacy assessment.

Monetised Costs

Familiarisation Costs (Direct Cost)

64. With the granting of adequacy to the US, a cost would be incurred by UK businesses establishing what they no longer need to do and understanding how the Data Privacy Framework functions. This is measured in time-cost. We assume that the guidance would be at a similar level of reading difficulty to the ICO's data sharing code, and therefore have used a similar Fleisch reading ease score of 40, which corresponds to a reading speed of 9 pages per hour. The wage assumptions vary by business size, reflecting that small and micro businesses, it is likely that managerial or director-level employees will do data protection activities rather than regulatory professionals. All wage estimates are uplifted by 22% for non-wage labour costs.[20] The hourly unit cost of this work was estimated to be £26.89 using median hourly managerial occupational earnings estimates from the Annual Survey of Hours and Earnings for sole, micro and small businesses.[21] For medium and large businesses with dedicated resources to undertake compliance activities we assume the median hourly wage for regulatory professionals at a unit cost of £25.74.

65. We have assumed a varying level of assumed new pages of guidance across the sensitivities. At a minimum, it is expected that businesses will read 2 pages of guidance on the ICO website confirming that the UK has made adequacy regulations in respect of the US. Given the particulars of the Data Privacy Framework, businesses will have to look up whether a potential recipient of data has signed up to the Data Privacy Framework which we have assumed is equivalent to 1 page of new guidance. 3 pages is used in our low costs (the high) scenario. However, it is expected that given additional guidance may be required to explain the Data Privacy Framework, in the central scenario we assume 3 additional pages of guidance (6 in total), following the published guidance for European businesses on the Data Privacy Framework website.[22] Lastly, we assume 3 additional pages of guidance in the high costs (the low) scenario (9 pages in total) to represent the length of the additional frequently asked question pages.[23] It is likely that UK-based guidance will follow a similar style and length to that published by the US. The government and non-profit uplifts using the ONS Business Population Estimates are also used for familiarisation costs. We assume all organisations who currently send personal data to the US and use standard data protection clauses face this familiarisation cost as it is prior to the decision to be risk-averse, before confirming what sectors are covered and whether recipients are signed up to the Data Privacy Framework.

66. Part of this cost will be ongoing. For the calculation of the NPV, we assume that businesses check on an annual basis whether current recipients have recertified or new recipients are signed up, equivalent to reading 1 page of guidance for all organisations.[24] Modelling as a single recurring annual cost may underestimate the cost if organisations have to verify recipients on a more regular basis. We assume this is not subject to the 47.6% adjustment as the organisation may find that the recipient is not signed up and not proceed with using the framework.

[20] RPC Short Guidance Note - Implementation Costs
[21] ONS Annual Survey of Hours and Earnings (2022)
[22] https://www.dataprivacyframework.gov/s/article/How-to-Verify-an-Organization-s-Data-Privacy-Framework-DPF-Commitments-dpf
[23] https://www.dataprivacyframework.gov/s/article/FAQs-UK-Extension-to-the-EU-U-S-Data-Privacy-Framework-UK-Extension-to-the-EU-U-S-DPF-dpf
[24] https://www.dataprivacyframework.gov/s/participant-search

67. The initial quantified familiarisation cost for the private sector has been estimated at £972,000, £6,100 for central and local government and £23,200 for the non-profits. These costs are faced by all organisations who currently send personal data to the US and use standard data protection clauses. The ongoing annual cost (from the second year) to verify that old recipients have recertified or new recipients are certified is estimated at £200,000 for private sector organisations, £1,200 for central and local government and £4,800 for non-profits.

Implementation Costs (Direct Cost)

68. We conservatively estimate costs in updating Data Privacy notices for those who use the Data Privacy Framework. Under UK GDPR Articles 13(1)(f) and 14(1)(f), organisations will need to provide information specifying that data is being transferred under US adequacy regulations to organisations certified to the UK Extension for the EU-US Data Privacy Framework. As a result, businesses will need to change references to standard data protection clauses to the Data Privacy Framework. We use a central estimate of 1 hour reflecting that as well as directly making the changes, they will need to publish them. We sensitivity test this assumption by varying between 0.5 and 1.5 hours in the high and low sensitivity respectively. We use the same wage unit costs with the non-wage uplift as the other familiarisation costs. The cost is subject to the three adjustments reflecting only those who make use of the Data Privacy Framework will face the cost. The ICO has guidance and a template for organisations to create and update Data Privacy Notices which should limit the time taken to make changes.[25] We conservatively estimate this as an ongoing cost throughout the appraisal period. This is despite this activity being required whenever organisations send personal data to a new recipient, so it is likely some of the changes will also be required in the counterfactual for new recipients. However, we know the number of new standard data protection clauses put in place on an annual basis rather than the extent to which those moving to the Data Privacy Framework will replace old contracts versus brand new recipients through new business relationships. We estimate these costs at £428,500 for private sector organisations, £2,700 for central and local government and £6,800 for non-profits.

Non-Monetised Costs

69. Most analysis available focuses on the issues around free trade and protectionism more broadly, rather than the tradeoff of “data openness” and security specifically. The gatekeeping and assessment process encompasses this in part through an assessment of data protection law and regulatory power. As part of the new Data Privacy Framework (option 1 - granting adequacy status), risks have been identified and mitigated through the new US Executive Order. Following data adequacy regulations being made, guidance and supporting material will be published by UK and US Governments on the safeguards and available routes for redress for UK data subjects.

70. Additional transfer of data may lead to increased risk of online harms and loss of privacy. However, the Data Privacy Framework puts in place additional safeguards and will provide UK data subjects with access to new routes of redress which were previously unavailable. These new routes of redress, which will only become available after adequacy regulations have been made, will be available for UK data subjects whether their personal data is transferred via adequacy regulations or via alternative transfer mechanisms, indicating that adequacy regulations could increase data protection standards for UK data subjects whose data is transferred to the US.

[25] https://ico.org.uk/for-organisations/advice-for-small-organisations/how-to-write-a-privacy-notice-and-what-goes-in-it/

71. There is also a perceived increased risk that, due to the lack of comprehensive federal data protection laws in the US, that personal data sent from the UK to the US may not be as secure. The protections afforded to UK personal data are reliant on the US organisation having certified to the Data Privacy Framework. However, the UK's assessment process accounts for both data protection laws in countries but also the effectiveness of enforcement such as the presence of an independent regulator. The purpose of undertaking a technical adequacy assessment is to ensure that the level of protection under the UK GDPR is not undermined when data is transferred to US organisations certified to the Data Privacy Framework. Therefore, risks are mitigated. The presence of the Data Privacy Framework ensures US-based companies meet a level of data protection which does not undermine UK data subjects' data and privacy rights.

Monetised Benefits

Standard Data Protection Clause Benefits (Direct Benefit)

72. The UKBDS 2022 included a number of questions which have allowed us to update the estimate of the standard data protection clause cost per business replacing the previous estimates derived from the RoW Umbrella IA, which were derived from bespoke survey evidence and discussions with legal professionals ahead of EU Exit. The time taken to put in place a standard data protection clause both in internal staff and external legal hourly costs is used in conjunction with estimates of the number of clauses put in place on an annual basis by business size. Internal wage estimates are the same as used for the familiarisation costs. External legal advice costs are estimated as the hourly wage for legal professionals from ASHE data of £23.27.[26] We additionally applied the average service sector profitability of 15.4%, to represent the additional profit margin.[27] The non-wage labour uplift of 22% is applied to create the final hourly unit cost of £32.76.

73. The methodology is improved as the previous estimate using the RoW Umbrella IA made a number of assumptions. The new method directly estimates the number of clauses put in place from businesses trading with non-EU/EEA based businesses. This is instead of the previous estimate derived from asking businesses what the costs would be in the event of losing EU adequacy, in reference to data transfers to the EU/EEA. Previously we also assumed a five-year contract cycle to forecast future compliance costs, while the new approach directly estimates the number of clauses put in place in a single year using the UKBDS. The use of the UKBDS ensures we can monitor and evaluate the usage of standard data protection clauses in the future. DSIT will update the RoW Umbrella IA in due course.

74. As set out in table 1, the average standard data protection clause cost has been calculated for each business size. To establish the total amount being spent by each business size on standard data protection clauses per annum in the UK, the adjusted average standard data protection clauses cost for each business size is multiplied against the total number of businesses of that size sending data to an international partner in the rest of the world as a percentage of total UK businesses.

75. The analysis is forward-facing, in that there are no benefits assumed for those standard data protection clauses already in place. We assume that all those who currently have standard data protection clauses will familiarise themselves with the Data Privacy Framework but will not retrospectively remove their contracts in place, instead as new business relationships emerge and

[26] Annual Survey of Household Earnings, 2022.; Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14.6a, 2023

[27] Annual Survey of Household Earnings, 2022.; Profitability of UK companies time series, 2023.

contracts become outdated that businesses will use the Data Privacy Framework (minus those who are risk-averse).

76. As the number of data-dependent UK businesses is a small part of the business population, it is difficult to sample these businesses in more detail through the UKBDS. As the UKBDS only captures countries in which data transfers are made often, using this will overestimate the impacts estimated for the US. As a result, apportioning the total benefits using the proportion of data-dependent trade captures the relative importance of each country including smaller countries.

77. We apportion based on the amount of data-dependent trade attributed to the US as a proportion of all data-dependent trade with countries that do not already have adequacy regulations. A YouGov Survey, commissioned by DCMS, conducted in 2019, provided an estimate of the percentage of UK-US exporters who are data-dependent. The calculated data dependency rate was 18%.[28] The figures from this survey are marginally higher than the 14% found in the International Transfer Tools Survey used in the RoW Umbrella IA. The higher US data dependency is expected given that UK-US exports are more services-based (66%) compared to the rest-of-world average (54%). We apply the 14% data dependency figure used in the RoW Umbrella IA for all other countries to estimate their data-dependent trade. Trade data is updated to the latest ONS release.[29]

78. UK-US exports are worth £168.3bn of which 18% is data dependent or £30.3bn. US data-dependent trade makes up about 50% of the total data-dependent exports within the list of all rest-of-world exports. The US makes up about 35%, with the higher proportion of data-dependent trade being driven by the higher data dependency. This ratio is applied to the updated top-down figure calculated in the RoW Adequacy Umbrella IA of £549.4m.[30] As a result, the unadjusted alternative standard data protection clause cost estimate is calculated at £286.0m.

Data-Dependency %	x	US Exports	=	Data-Dependent US Exports
(18%)		(£168.3bn)		(£30.3bn)

Data-Dependency %	x	Trade for RoW Non-Adequate Countries	=	Total Data-Dependent Trade
(14% for all other countries 18% for the US)		(£325.9bn)		(£58.2bn)

79. Once adjusting for the sector coverage and Data Privacy Framework adjustment this gives an estimate of £81.9m. To estimate the number of businesses affected, we use the % of all UK businesses who send personal data and use SCCs and say that data transfer with the US is

28 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1118371/DCMS_Data_Policy_YouGov_Surveys.ods

29 UK total trade: all countries, non-seasonally adjusted

30 See RoW Adequacy Umbrella IA for full details of methodology. The estimate differs from the original £360m estimate in the RoW Adequacy Umbrella IA as Business Population Estimates, ONS trade data, UKBDS parameters on those who send personal data and use standard data protection clauses and country-specific data-dependencies (where available) have been updated to the latest available. 2021 Business Population Estimates show a decline in the smallest registered businesses. DSIT analysts will continue to update underlying data as individual country IAs are produced.

important to them. This estimate is 0.9% of all UK businesses or 54,318 businesses; with the adjustments this falls to 15,965.

80. Similarly, the ratio by business size of central and local government to private sector and non-profit to private sector organisations from the ONS Business Population Estimates is used to estimate benefits to these sectors (see Table 3 below). Central and Local Government and Non-profit organisations are disproportionately larger, compared to the wider business population, but are much smaller in number. The uplifts are applied to the private sector benefits to estimate a total rest-of-world adequacy estimate and apportioned the same way as the private sector benefits (US data-dependent exports as a proportion of all rest-of-world exports). We estimate a total central and local government benefit for the US adequacy regulations of £1.2m with a range of £0.4m to £2.4m. Similarly, we estimate a non-profit benefit of £2.7m with a range of £1.0m to £5.4m.

Table 3: Government and Non-Profit Benefit Uplift Factors

	Sole trader	Micro	Small	Medium	Large
Central and Local Government Benefits Factor	1.00	1.01	1.01	1.06	1.22
Non-Profit Benefits Factor	1.00	1.06	1.06	1.09	1.16

Export Revenue Gain (Suppressed Trade) (Indirect Benefit)

81. To estimate the export revenue gain, the *UK Business Impacts Model*[31] is used to estimate the value of EU Adequacy. The model considered using survey data on exporters, the value of exports and their data dependency, whether they would choose to incur compliance costs or choose not to export in the event of losing EU adequacy. This assessment does not consider this impact in its scope but uses assumptions, such as the standard data protection clause costs derived for estimating the potential costs of losing EU adequacy, and the outputs, such as the estimated trade suppression ratio, to support this analysis.

82. A ratio of 0.3% was estimated as the direct amount of suppressed trade within that model and is applied here. It should be noted that the underlying analysis in the UK Business Impacts Model does not cover the smallest businesses who may benefit most as standard data protection clause costs may proportionally be a more significant cost to these businesses. As a result, this ratio may be too low. Similarly, the model is solely in partial equilibrium so does not consider potential trade diversion with third parties. The wider impacts section below details a gravity modelling approach which estimates more medium-term trade impacts which explicitly capture trade diversion.

83. To estimate the second benefit, the inverse of this suppression factor is applied to the value of current data-dependent US exports, on the assumption that trade is already suppressed in the same manner. Therefore, the following formula is applied to the export value. This formula 'inflates' the current export value up to 100% from its presumably suppressed value, and takes the difference between that and the suppressed value.

[31]The UK Business Impacts Model has been independently quality assured three times: when it was first completed in early 2019, after being updated toward the end of 2019 and most recently following updates made for the final Data Protection and Digital Information Bill analysis. The final results have been used in numerous papers and submissions, including the published Data Protection and Digital Information Bill IA.

$$d\frac{1}{1-s}-d$$

where:

Data-dependent US exports[32], d = £168.3bn * 18% = £30.2bn

The data-dependency value of 18% is taken from the YouGov Data Dependency Survey.[33]
Suppression factor, s = 0.30% (high=0.50%; low=0.26%)[34]

84. As a result, we estimate an unadjusted trade suppression on exports to the US of £90.5m.

85. Similarly to standard data protection clause benefits, a portion of trade will still fall under the need to have standard data protection clauses in place and therefore remain suppressed. As a result, we adjust the export benefits by the same 29.4% adjustment to reflect the proportion of US businesses that have certified to the Data Privacy Framework, are in sectors covered by the regulations and the risk-aversion of UK businesses. This is likely to be a conservative adjustment as the largest businesses represent a significant proportion of all trade and are more likely to have certified to the Data Privacy Framework. Similarly, the sector adjustment is based on the industry of UK exports opposed to the destination industry of those services. An assumption is made that the industry of the exporter is the same as that of the recipient of the services. Our best estimate is an annual increase in export trade of £26.6m.

86. The number of businesses affected is not estimated as it is an indirect benefit as this will be a combination of both those that currently trade and expand the amount they trade as well as those currently dissuaded from exporting at all which are directly captured or estimated in the analysis.

87. The low scenario uses a lower assumed data-dependency of 14% from the Rest-of-World average from the International Transfer Tools Survey to account for parameter uncertainty. A range of ratios is estimated to account for uncertainty from the UK Business Impacts Model. These are used to produce a range of export revenue increase figures. Table 4 below presents the range of estimates from £11.9m to £65.6m.

Table 4: UK Export Revenue Increases

Scenario	Best	Low	High
Assumptions			
Trade Suppression Ratio	0.3%	0.26%	0.5%
Assumed Data-Dependency	18%	14%	18%
Data Privacy Framework Adjustment	47.6%	40.2%	55.0%

[32] UK total trade: all countries, non-seasonally adjusted
[33] The data-dependency percentages, i.e. the proportion of businesses, by sector and size category, that depend on transfers of personal data for their important primary or secondary business functions, are taken from analysis of survey data and are considered to be statistically robust.
[34] Ratios calculated from the UK Business Impacts Model.

Risk Aversion Adjustment	76.8%	59.5%	94.0%
Sectoral Adjustment	80.4%		
Export Benefits			
Benefit	£90.5m	£61.9m	£157.7m
Adjusted Benefit	£26.6m	£11.9m	£65.6m

Total Benefits

88. Combining the suppressed trade with the upper and lower bound standard data protection clause costs estimates, UK businesses could see an annual impact of £114.5m in the best scenario. The sensitivity testing indicates a range of £40.2m and £247.0m.

Non-Monetised Benefits

Other Alternative Transfer Mechanisms

89. As above, this analysis has focused on standard data protection clauses as these are the most commonly used alternative transfer mechanism. However, the analysis does not quantify the additional benefits from all other mechanisms as the underlying evidence base does not capture as robustly the usage and costs associated with putting these in place. For example, the use of derogations, which provides exceptions that allow transfers, are associated with familiarisation costs as businesses understand whether they are allowed to utilise certain exceptions. As a result, the costs associated with these are likely to be much smaller than estimated for standard data protection clauses. Similarly, the reporting of usage of binding corporate rules in the UKBDS is overrepresented compared to the 40 or so multinational groups, which could include a number of separate UK entities, published by the ICO online.[35] There are high costs associated with putting in place binding corporate rules but these cover transfers within corporate groups so adequacy regulations with the US may not necessarily reduce the usage of these if a multinational group is beyond just the UK and US. As a result, there will be additional benefits that are unquantified, however given the lower cost of derogations and the much lower usage of binding corporate rules, are likely to be marginal to the impacts already quantified.

Indirect Supplier Benefits

90. Other, strictly domestic businesses utilise services crucial to their business from businesses that rely on cross-border transfers. There may be additional indirect benefits for businesses who do not

[35] A full list of those multinational groups currently approved to use binding corporate rules under UK GDPR and the DPA 2018 can be found: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/guide-to-binding-corporate-rules/bcr-approvals/bcrs-approved-under-uk-gdpr/ and https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/guide-to-binding-corporate-rules/bcr-approvals/list-of-bcr-holders-approved-pursuant-to-paragraph-9-part-3-schedule-21-to-the-dpa-2018/

undertake cross-border transfers in terms of productivity as services improve due to easier cross-border transfers of data. One example may be research and development benefits from sharing data internationally that lead to the development of a service. The strictly domestic business then uses the improved service that leads to an improvement in productivity.

Additional Public Sector Benefits

91. The suppressed export benefit which is calculated above captures the reduced business activity undertaken due to current restrictions in data transfer. The adequacy regulations may 'release' economic activity that previously was not undertaken due to costs and legal uncertainties. Similarly, the UK public sector may not currently undertake data transfers due to the cost (time and resource) in putting in place alternative transfer mechanisms. This may result in lost opportunities such as greater knowledge sharing and innovation. Whilst these benefits do not materialise in terms of direct trade benefits, they may result in impacts such as increased public sector efficiency. For example, greater data-sharing may lead to greater competition in public procurement leading to efficiencies.

Import Benefits

92. The *UK Business Impacts Model* uses detailed survey data on business size and sectors which was only available for exporters. As a result, the trade suppression ratios used were only estimated for impacts on exports. However, we would also expect an increase in imports as UK importers would similarly benefit from the free flow of data to the US. With greater cooperation with trading partners in the US, UK importers may have easier access to data potentially allowing firms to cut costs and expand trade with the US. The gravity modelling explored in the trade section estimates the medium-term impact on imports indicating an increase larger than the export benefits.

Consumer Benefits

93. The focus of this analysis has been primarily business or public sector organisation benefits. As data sharing increases and businesses face lower costs, consumers are likely to directly benefit from better services and potentially lower prices. We have not estimated whether these impacts are additional to the reduction in costs and increased exports.

Adequacy Reciprocation

94. Currently in the US, there are no overarching federal data protection laws, with only certain US states enforcing their own. As a result, a significant amount of US businesses can already send personal data to the UK. However, adequacy granted by the UK may serve to strengthen commercial relationships between UK and US organisations, indirectly benefiting UK businesses by encouraging reciprocal data-sharing, increasing the positive impact on trade between UK and US businesses.

Diplomatic Benefits

95. Adequacy may have further indirect benefits to the US-UK relationship. Establishing adequacy with a large economy such as the US could result in benefits to establishing further adequacy agreements with other countries. Granting adequacy to the US is a chance for the UK to build on the pre-existing diplomatic relationship between the UK and US, such as through the

Comprehensive Dialogue on Technology and Data[36] and the Atlantic Declaration.[37] The UK has also become the first country in the world to be granted Associate status in the Global Cross Border Privacy Rules (CBPR) Forum, of which the US is a member and current chair.[38] Adequacy regulations would also set an example to other similar nations in promoting the indirect benefits to business of a secure, international exchange of data, including finding solutions to address the barriers to cross-border data transfers. The closer diplomatic status with the US could help the UK be a more attractive partner for any further data agreements, trade partnerships or foreign investment, providing a solid platform for economic growth and investment in the UK economy.

Net Present Value

96. When estimating the NPV we have assumed a static Data Privacy Framework adjustment with no increased take-up over the appraisal period. Table 5 below details how changes in assumptions over time may affect the NPV.

97. The NPV for the UK granting the US data adequacy has been calculated using 2022 prices and 2023 as its present value (when benefits/costs begin) with a 10-year appraisal period and 3.5% discount rate with an assumed background 3% of private sector growth.[39] The NPV calculator has been set to estimate the value of this policy over the next 10 years. The impact has been converted to 2019 prices and 2020 present value with a best estimate of having a total net present social value of £893.0m with a low estimate of £313.4m and a high estimate of £1933.8m.

98. Standard data protection clause benefits and familiarisation costs are a direct business impact for private and non-profit organisations. Trade suppression benefits are an indirect business cost.

99. The net direct cost to business per year has been estimated at -£78.4m with a business impact target (BIT) score of -£-391.9m.

Table 5: Assumed Parameters NPV Impact

Parameter	Assumed	Direction of NPV
Data Privacy Framework Take-up	47.6% and stays constant. The 95% confidence intervals are used in low and high sensitivities to reflect parameter uncertainty.	As outlined above, there are a number of reasons for expecting the level to return to the take-up seen with the US Privacy Shield. If it increases beyond the take-up previously, given the longer time horizon than the time the Privacy Shield had been active from the survey evidence, the NPV would increase. As outlined, there remains the risk of legal challenge and although the UK's decision is independent, any uncertainties may reduce US take-up of the framework, lowering the NPV.

[36] https://www.gov.uk/government/publications/uk-and-us-progress-tech-and-data-partnership/uk-us-joint-statement-new-comprehensive-dialogue-on-technology-and-data-and-progress-on-data-adequacy
[37] https://www.gov.uk/government/publications/the-atlantic-declaration
[38] https://www.gov.uk/government/news/uk-gets-new-status-in-global-data-privacy-certification-programme
[39] Business Population Estimates ONS 2000-20 show an average annual business population growth of 3% per annum. Government and non-profit organisations are assumed to have no background growth in number.

Background business growth	Number of businesses in the economy has grown by 3% historically.	If the growth in businesses doing business with the US increases beyond background business growth seen economy-wide, the NPV will increase. Given the focus of the analysis is data-intensive businesses that are growing faster than agree this may be likely.
Data Dependency	18% for the US, 14% for other countries. Stays constant throughout the appraisal period.	If data dependency was to rise over time, due to wider digitisation, more businesses in the counterfactual would have put in place standard data protection clauses, resulting in an increase in the NPV.
Take-up	Assume that a proportion of businesses 23.2% will choose to use standard data protection clauses due to risk-aversion.	Some businesses may still use standard data protection clauses despite not having to. This would reduce the NPV. If perceived risks or uncertainties increase, this proportion could increase. Similarly, if over time, the Data Privacy Framework becomes a trusted mechanism for data transfers, risk-aversion could fall, increasing the NPV.
Background non-profit and government growth	Assume that no growth in these types of businesses over the appraisal period.	If the number were to grow, the NPV would be larger.
Appraisal Period	Assumed 10 years	As discussed above, in the event of a successful legal challenge, organisations would revert to using the transfer mechanisms that they currently use such as standard data protection clauses. Businesses would still have benefited from the time in which they did not need to put in place costly standard data protection clauses. Although, for any ongoing data-sharing, organisations would be required to use standard data protection clauses. This would truncate the benefits and any ongoing costs. As a result, the NPV would be lower but still net-positive.

7.0 Wider Impacts:

Small and Micro Business Assessment

100. There are no exceptions based on business size of needing to use standard data protection clauses when sending personal data to the US. The government does not consider an exemption for this legislation as it is significantly beneficial for all firms to use these clauses.

101. The sample sizes from underlying surveys do not allow disaggregated results. However, the standard data protection clause benefits and costs can be disaggregated by business size. Trade data and suppression ratios are not disaggregated enough to robustly break down the trade impacts.

102. The proportion of UK businesses that are traders and send or receive data from the US by business size is calculated from the UKBDS. We apply these percentages to the total standard data protection clause benefits calculated above.

103. Due to small sample sizes, we cannot disaggregate the Data Privacy Framework and risk-aversion adjustment to provide estimates by business size. The 47.6% adjustment is used uniformly across all business sizes as a result. This is likely conservative, as Data Privacy Framework use likely increases with business size. The risk-aversion factor at 76.8% is applied across business sizes, on one hand smaller businesses may be more likely to perceive legal risks however given that costs are likely a bigger share of business turnover, they may be more incentivised to begin using the Data Privacy Framework. Conversely, large firms will likely have data policy expertise internal to their organisations however perceived risks may be higher due to the likely larger amounts of data held by large firms. The UKBDS could not produce disaggregate results of the usage of standard data protection clauses for EU transfers by business size so this is assumed constant. The sectoral adjustment of 80.4% is applied across business sizes.

Table 6: Small and Micro Business Assessment Results[40]

	Sole Trader	Micro	Small	Medium	Large	Total
Affected Private Sector Businesses	10,128	4,046	1,195	390	205	15,965
Standard Data Protection Clause Benefits						
Private Sector	£47.3m	£19.0m	£10.9m	£3.2m	£3.7m	£84.1m
Government	£0.7m	£0.3m	£0.2m	£0.0m	£0.1m	£1.2m
Non-Profit Orgs	£1.5m	£0.6m	£0.3m	£0.1m	£0.1m	£2.7m
Familiarisation Costs						
Private Sector	£616,531	£246,326	£72,776	£23,736	£12,482	£971,852
Government	£0	£1,501	£429	£1,403	£2,732	£6,066
Non-Profit Orgs	£0	£14,417	£4,618	£2,236	£1,943	£23,214
Data Privacy Notice Costs						
Private Sector	£271,800	£108,600	£32,100	£10,500	£5,500	£428,500
Government	£0	£700	£200	£600	£1,200	£2,700
Non-Profit Orgs	£0	£6,400	£2,000	£1000	£900	£10,000
Percentage of Benefits	56.3%	22.6%	13.0%	3.8%	4.4%	100.0%

[40] Business sizes are as follows: sole trader is a business with zero employees, micro 1-9 employees, small 10-49 employees, medium 50-249 employees and large 250+ employees.

Percentage of Costs	61.6%	26.2%	7.8%	2.7%	1.7%	100.0%

104. The number of affected businesses by the removal of needing to place standard data protection clauses for US data transfers is 15,965 in total. 96% of the businesses that benefit are small or micro businesses. Table 6 above indicates the majority of the standard data protection clause benefits fall on the smallest businesses with the vast majority (91.8%) falling on small and micro businesses. The smaller familiarisation costs fall even more so on small and micro businesses (95.5%) representing that costs more equally fall on businesses as the amount of guidance required for familiarisation is the same across business sizes whilst the number of standard data protection clauses increases by business size.

105. The UK government is engaging with the ICO and the DoC to ensure there is sufficient guidance provided to businesses to aid them in appropriately utilising the adequacy decision for the Data Privacy Framework. Guidance will be published online and made easily accessible for all businesses, including SMEs. The UK government plans to publicise the benefits and opportunities of the adequacy regulations in order to make businesses aware of the change.

Competition

106. Securing and enhancing outbound flows of data between the UK and the US, through seeking reciprocal arrangements for the transfer of data will bring new opportunities for innovation, collaboration and trade, especially in data-intensive sectors like scientific research and artificial intelligence. The greatest benefits of international data flows will be realised when personal data can flow freely and securely in both directions.

107. The policy should increase the number of UK-based exporters to the US as well as increase overall trade with the US increasing competition in both UK and US markets.

108. Currently an imperfect information problem exists in which businesses have to undertake compliance activities to ensure data protection of recipients of UK data is of sufficient quality on a case by case basis. Businesses might lack the required information needed about their business partners and are unable, or unequipped, to observe and understand their data practices in detail. This problem compounds when data might not be the primary focus of one of the businesses in any transaction but merely its enabler, creating large additional costs to build expertise and do these evaluations. This is a particular problem for smaller firms that might lack the resources and the data processing frameworks that larger firms often have in place, raising further barriers to trade. By granting adequacy to the US, the government and regulators are reducing this asymmetry by assessing the Data Privacy Framework (and therefore certified organisations in the US) more generally, reducing the burden on businesses.

Equalities and Distributional Impacts

109. As part of the gatekeeping and assessment process, adequacy assessments take into account, amongst other things, the rule of law, respect for human rights and fundamental freedoms, and the existence and effective functioning of a regulator in the third country. The Secretary of State is required to have due regard to the public sector equality duty (‘PSED’) under s149(1) Equality Act 2010. Based on DSIT’s analysis, it is not expected that the policy will result in negative or disproportionate impacts on UK data subjects’ equality.

110. As part of the PSED analysis, regard was given to specific protected characteristics and the likely risk of data pertaining to these being treated differently once within the US federal jurisdiction. Characteristics of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion, sex and sexual orientation were all scrutinised. Consideration has been given to the impacts of the proposed regulations and whether they will or will not be likely to lead to direct or indirect discrimination or disadvantage. DSIT has concluded that the policy will not result in negative or disproportionate impacts on UK data subjects' equality. In the scenario that definitions exist in one jurisdiction but not the other (e.g. 'sexual orientation' is not referenced as such in the US), the team is content that data marked as 'sensitive' by UK controllers will be treated as such under the requirements of the US Data Privacy Framework. All aspects of the US framework under the data bridge will continue to be monitored once the policy has been implemented.

111. Considering the distributional impacts of the legislation, the UKBDS finds some evidence that businesses in London are more likely to transfer data internationally than those in some other regions. However, there are no statistically significant regional disparities in international personal data sharing. Similarly, other survey evidence underpinning this analysis was not disaggregated enough to estimate region-specific impacts. As a result no assessment of the regional impacts has been completed.

Trade

112. As described above, the measure will increase exports, as currently a proportion of trade is suppressed due to the barrier that using alternative transfer mechanisms creates. The impact is likely to impact the smallest businesses the most. As a result, we would expect a more competitive market as businesses enter the market. Due to the methodology of the trade suppression benefits, only impacts on exports have been estimated. There would also be an impact on imports.

113. To capture the more macro-level impacts of adequacy regulations, DSIT has used a complementary gravity modelling approach to estimate the medium-term impact on trade.[41] The analysis should be seen alongside the business-level approach identified above but ultimately have different methodological foundations. The analysis was originally produced for the Data Protection and Digital Information IA and full details of the modelling can be found in the Gravity Modelling Annex published alongside.[42] Full methodological detail of the underlying model can be found in DIT's published Services Trade Modelling Working Paper.[43] The modelling has been rerun testing the impact of US adequacy regulations in isolation finding an impact of £299.9m. Similarly, imports could increase by even more at £331.2m. The UK sectors covered in the analysis were limited to reflect the sectoral coverage of the Data Privacy Framework, making the same conservative assumption that the destination industry (the US importer) is the same industry as the UK exporter. The sectors assessed were transport, other business services and distribution. Impacts are concentrated on Other Business Services. Manufacturing or other goods sectors are not covered. As a result, these impacts are likely underestimated. Table 6 below outlines the impacts by sectors split by imports and exports.

[41] The gravity model of international trade states that the volume of trade between two countries is proportional to their economic mass and a measure of their relative trade frictions. The gravity model has been commonly used in international trade analysis for several decades due to its intuitive appeal. Medium-term here reflects

[42] Data Protection and Digital Information Bill Impact Assessment, Gravity trade modelling annex

[43] Services trade modelling Working Paper and for further detail on the methodology underpinning the model please see An Advanced Guide to Trade Policy Analysis: The Structural Gravity Model. WTO iLibrary.

Table 6: Gravity modelling sectoral results

Sector	Change in Exports	Change in Imports
Transport	£50.1m	£21.9m
Other Business Services	£238.0m	£284.4m
Distribution	£11.6m	£24.9m
Total	£299.7m	£331.2m

114. These results are not presented in the main benefits or the NPV as the impact is uncertain in regards to timings. These trade impacts are larger than the impacts found above as the macro approach captures indirect, general equilibrium effects from liberalising trade policy, as opposed to the more direct business-level approach calculated above.

7.0 Switching Analysis

115. Given the criticality of the impact of the assumed adjustments on the results, we assess through switching analysis what the total adjustment would have to be to switch the impacts from a net-positive position to net-neutral (i.e. net-benefits of zero). The final combined factors applied to the benefits and the data privacy notice costs are between 19.2% and 41.6% with a central estimate of 29.4%. The required combined factor would instead have to be 0.6% in the central scenario for the net-benefits to be equal to zero. Illustratively, holding the sectoral coverage and risk-aversion constant, the take-up by US businesses would have to be 1% not 47.6% for the benefits not to outweigh the costs. Similarly, each adjustment would have to be uniformly 2.2% of its current size for the costs to equal the benefits. Considering the wider low and high sensitivities, the required factor would have to be 1.8% in the low scenario and 0.2% in the high scenario. This is conservative as costs are highest in the first year, reducing to smaller ongoing verification that recipients are certified and data privacy notices costs in future years. Benefits, on the other hand, are maintained throughout the appraisal period and as a result, the required factors for the NPV to be net-neutral will be even smaller. It is therefore extremely likely that the net positive results from this analysis are robust, regardless of how much the individual adjustments of the risk aversion, sectoral coverage and Data Privacy Framework sign-up rates by US businesses are varied.

116. As above, as the benefits accrue in each year, the net-benefits increase in each year as costs are smaller in future years. As a result, if we assume costs are borne on the first day of the legislation being in place whilst benefits accrue uniformly across the year as organisations switch from using standard data protection clauses to the Data Privacy Framework, assuming the central adjustments used, the benefits outweigh the costs after 8 days of being in place.

8.0 Monitoring and Evaluation Plan:

117. We will carry out proportionate monitoring and evaluation activities throughout the next 3-5 years to determine whether the impacts identified in the IA have materialised and what drivers have contributed or limited these. An evaluation report will be produced with the findings of this analysis within 3-5 years of implementation.

118. We assume it will cost businesses less to implement the Data Privacy Framework compared to currently available data transfer mechanisms. As such, success will be the adoption of the Framework over other mechanisms.

119. To measure this,

    a. DSIT will run a survey on the UK business population, identifying those that currently use digitised data, and trade with the US. UK businesses will likely answer questions on:

        i. Whether they are aware of the changes in requirements.

        ii. Whether familiarisation or other costs have been incurred as a result of the changes.

        iii. What benefits they see resulting from the changes.

        iv. Whether they think the adequacy regulations contribute to their trade in that country.

        v. What steps UK businesses have to take to verify recipients have the Data Privacy Framework in place.

    b. We will commission a repeat survey in a few years, likely in 2025 and published in 2026, to track changes. In this way, we will establish the size of any change towards uptake of the Data Privacy Framework. Our interpretation of any quantitative change will be complemented by detailed interviews to a selection of respondents at both time points.

120. DSIT aims to continue conducting the UKBDS. This provides nationally representative figures for many key assumptions in this IA, including:

    a. The proportion of businesses sharing data internationally.

    b. Which countries that data is being shared with.

    c. The size of these businesses.

    d. The legal mechanisms these organisations use to share the data.

121. Evidence based on surveying businesses will be conducted by an experienced research organisation. The department and the contractor act as joint data controllers and a privacy notice details how respondents can expect the data to be handled appropriately, following data protection regulations and requirements for Official Statistics. Respondents are pointed towards the privacy notice before they agree to participate in the survey work.

122. We will also carry out research to help verify assumptions made in this IA. This will be done through use of the interviews to businesses mentioned above. It will also be achieved using research instruments designed and commissioned for this purpose, and survey evidence from existing sources to track metrics which indicate relevant factors.

123. Similarly, qualitative interviews will be used to assess whether there are any unintended consequences as a result of the legislation through more open-ended interviews. As the regulations are part of a programme, findings from the initial set can be reflected in future policy design. For example, if awareness of adequacy regulations is found to be low, more communication with businesses could be planned.

124. It is unlikely that causal impacts of the policy change will be directly estimated given other underlying drivers of trade with the US such as EU Exit and continued underlying growth in data-enabled and data-dependent trade.

125. The monitoring and evaluation should make it possible to further refine this analysis including underlying parameters. For example, the number of organisations signed up to the UK Extension to the Data Privacy Framework will be published on the website. This will allow a measure of the take-up of the Framework which could be assessed against the 47.6% of US businesses who import UK goods or services factor used in this IA.

126. The relief of suppressed trade to the US will be evaluated by monitoring the UK's annual exports figures to the US following the implementation of US adequacy. Indicators used to evaluate the relevant changes will be:

    a. Total increase in value of exports to the US.
    b. Changes in the proportion of data enabled and data dependent goods and services being traded.
    c. The change in value of data enabled and data dependent exports.