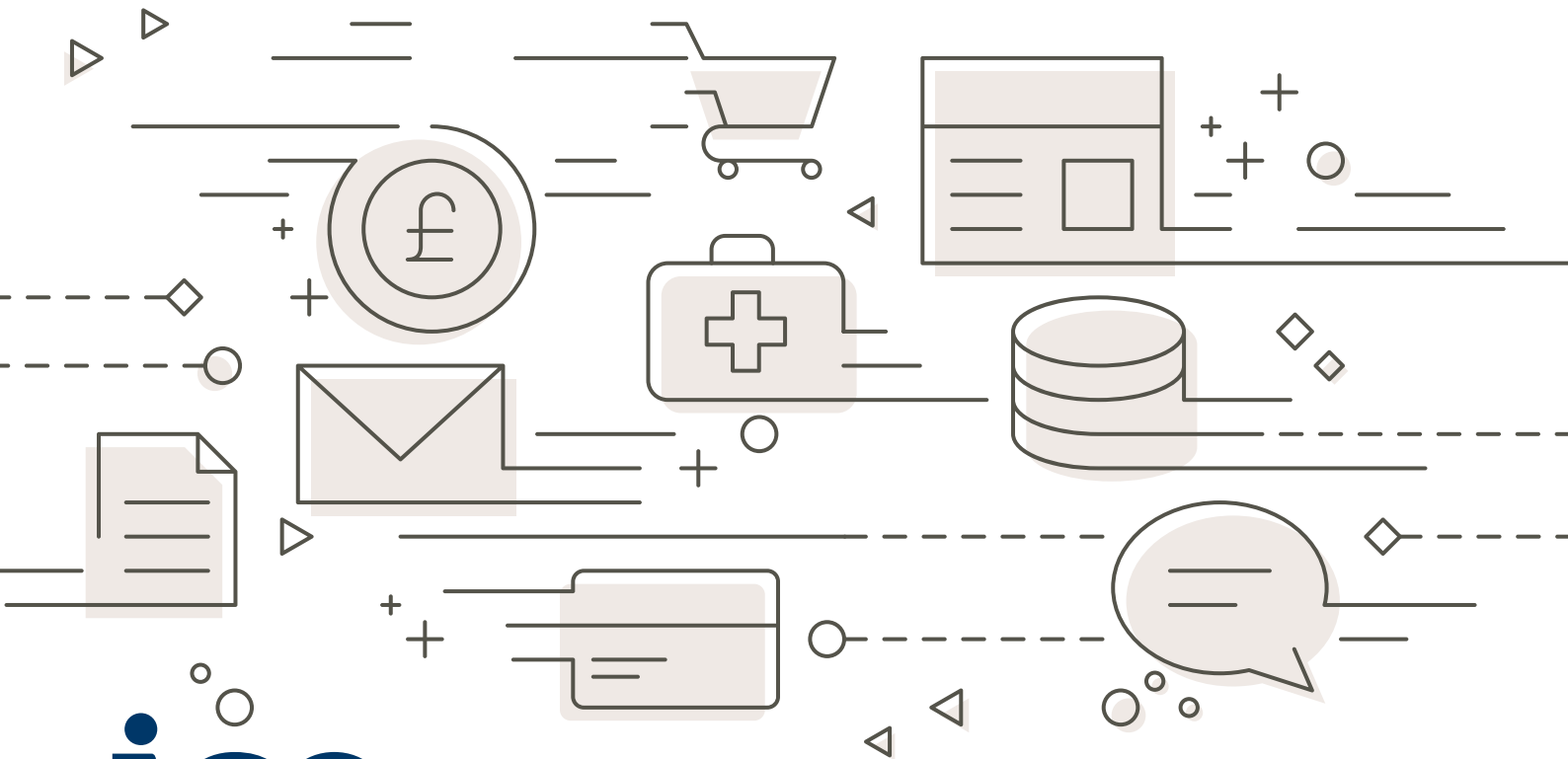


IDTA and TRA (IDTA Toolkit) impact assessment

Economic analysis – impact and evaluation

December 2022



Title: IDTA and TRA (IDTA Toolkit) impact assessment Lead department or agency: Information Commissioner's Office (ICO)	Impact Assessment (IA)
	Date: December 2022
	Stage: Final
	Source of intervention: Legislative

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

The ICO has developed and published the International Data Transfer Agreement (IDTA) following the UK's withdrawal from the European Union (EU). This was a necessary step because the old EU Standard Contractual Clauses (EU SCCs) were not aligned with UK General Data Protection Regulation (GDPR) and the new EU SCCs do not apply to the UK because they were implemented following the UK's withdrawal from the EU. The ICO has also published the UK Addendum to the EU SCCs that enables the new EU SCCs to be used in a UK context. Both the IDTA and the UK Addendum to the EU SCCs are designed to help streamline and secure safe and responsible restricted transfers. In addition, the ICO has published the Transfer Risk Assessment (TRA) tool to assist controllers in assessing the risks associated with restricted transfers. The requirement for a transfer risk assessment stems from the July 2020 Court of Justice of the European Union decision in Schrems II where data exporters are required to perform a transfer risk assessment when using Article 46 transfer.

What regulatory policy options have been considered, including any alternatives to regulation? Please justify preferred option.

The older EU SCCs were viewed as outdated in light of the UK GDPR and as such, there was a legal requirement to replace them. The development of a replacement is viewed as the only viable option as any alternative has the potential for substantial negative impacts on the economy and society. The transfer risk assessment tool and guidance is designed to assist organisations when undertaking the transfer risk assessment required by Schrems II. Alternatively, the ICO could have done nothing to assist organisations. However, this was not a viable option because the transfer risk assessment tool and guidance help to mitigate the impact of the legal requirement to perform a transfer risk assessment.

Will the intervention be reviewed?

The toolkit will be kept under review in line with good regulatory practice.

Contents

Executive summary.....	i
1. Introduction	1
1.1. Note on terminology	2
2. Our approach to the impact assessment.....	3
2.1. Theory of change	4
3. Context.....	9
3.1. Social and economic context.....	9
3.2. Policy context	20
4. International transfers guidance and tools.....	25
4.1. Approach to the toolkit	26
4.2. Scope of the guidance.....	27
4.3. Affected groups	28
5. Costs and benefits of the toolkit.....	32
5.1. Cost benefit analysis of the toolkit	33
5.2. Overall assessment of impacts	38
Annex A: Familiarisation costs.....	39
Organisations in scope	39
Familiarisation costs	45
Sensitivity analysis	48

Executive summary

This impact assessment sets out the benefits and costs associated with the International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses (the Addendum), the Transfer Risk Assessment (TRA) guidance and tool. For the purpose of this impact assessment, these are referred to as the IDTA toolkit. The Information Commissioner’s Office (ICO) aims to further develop associated tools and guidance beyond what is currently published. The impact assessment draws on evidence including desk-based research, stakeholder engagement, and previous ICO impact assessment analysis.

Overall assessment

Our overall assessment is summarised in Table 1.

- There are potentially significant familiarisation costs associated with the toolkit, however, there is a high degree of uncertainty around these figures. It is also not clear that these impacts can be fully attributed to the development of the toolkit, given the wider legislative context.¹
- There is potential for significant indirect benefits to the toolkit (eg increased organisational confidence to engage in international data transfers), given the importance of international data transfers to the UK economy and the associated risks to society.

Our assessment concludes that even a small reduction in the risks to businesses and organisations or improvement in their confidence would significantly outweigh the potential familiarisation costs associated with the toolkit.

Table 1: Summary of impacts

Impacts*	Positive, neutral or negative**	Attributable to the toolkit
Familiarisation costs	Negative	Attributable
Data protection harms	Positive	Partially attributable
Business and organisational confidence in doing transfers	Positive	Partially attributable

¹ Within the analysis we have assumed that these are attributable so as not to under scope any potential negative impacts.

*Descriptions of each of the impacts are provided in detail in Section 5.

**Positive (a net benefit); negative (a net cost); neutral (no impact)

Our approach to assessing impacts is set out in Section 2 and a theory of change is provided in Figure 1 which sets out, at a high level, how we expect the toolkit to generate impacts for different affected groups.

Context

Data is one of modern society's greatest assets, supporting economic growth, technological innovation and the delivery of more efficient and targeted services. Around 783,000 UK businesses and other organisations are estimated to transfer data to other entities outside of the UK. In 2020, the value of international data transfers to UK exports was £243 billion and to UK imports was £118 billion.

However, transfers of personal data are not without risk and transfer outside of the UK can elevate those risks. The potential harms associated with transferring personal data internationally are similar to those associated with transferring personal data within the UK. The key difference is that the UK government and the ICO have limited power over data controllers based outside of the UK.

With this toolkit, the ICO seeks to support UK businesses and organisations to realise the economic and social benefits from restricted transfers while ensuring an appropriate level of protection for UK citizens against potential harms.

The development of the IDTA was a necessary step because the old EU SCCs were not aligned with UK General Data Protection Regulation (GDPR) and the new EU SCCs do not apply to the UK because they were implemented following the UK's withdrawal from the European Union (EU). The UK Addendum to the EU SCCs enables the new EU SCCs to be used in a UK context. They are both designed to help streamline and secure safe and responsible restricted transfers. The requirement for a transfer risk assessment stems from the July 2020 Court of Justice of the European Union decision in *Schrems II*.

The toolkit aligns well with both published UK government policy and policy currently under development, including the National Data Strategy, the Digital Strategy and plans around data protection reform.

1. Introduction

This document sets out our findings relating to the International Data Transfer Agreement (IDTA) toolkit's impact assessment. The IDTA¹ and the UK Addendum to the EU Standard Contractual Clauses² (EU SCC) were issued under Section 119A(1) of Data Protection Act 2018³ (DPA 2018) and following parliamentary approval came into force on 21 March 2022. The Information Commissioner's Office (ICO) has also developed a suite of guidance and tools⁴ to support organisations in using the IDTA and Addendum. The suite of tools and guidance, alongside the IDTA and addendum, are what we refer to as the toolkit. The purpose of this impact assessment is to:

- provide an objective view of the costs and benefits of the toolkit;
- guide and inform the design of the toolkit and potential mitigation measures; and
- set a baseline for future review and evaluation activity.

The report is structured as follows:

- **Approach to the impact assessment:** setting out the approach taken to assessing the impacts of the toolkit and the limitations of the impact assessment.
- **Context:** setting out the economic, social and political context for the toolkit as well as the rationale for producing it.
- **The toolkit:** overview of the objectives of the toolkit, the approach to the toolkit and the affected groups.
- **Costs and benefits of the toolkit:** the costs benefit analysis covering both direct and indirect impacts of the toolkit.

¹ ICO (2022): <https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf>

² ICO (2022): <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>

³ Data Protection Act 2018, available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>, accessed 5th December 2022

⁴ ICO (2022): <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/>

1.1. Note on terminology

In this paper we use the following terms:

Table 2: Key terminology

Term	Definition
International data transfer	Sending or receiving data to or from a country outside of the UK. This includes but is not restricted to personal data.
Restricted transfer	A restricted transfer takes place when the UK General Data Protection Regulation (GDPR) applies to the processing of personal data which is then sent/made accessible to a separate receiver which is located in a country outside of the UK.

In this impact assessment, we classify organisations and businesses by number of employees in line with definition used by the Office of National Statistics.⁵

Table 3: Business classification

Business size	Number of employees
Sole trader	0
Micro	1 – 9
Small	10 – 49
Medium	50 – 249
Large	250+

⁵ Department for Business, Energy and Industrial Strategy (2022): <https://www.gov.uk/government/statistics/business-population-estimates-2022/business-population-estimates-for-the-uk-and-regions-2022-statistical-release-html>

2. Our approach to the impact assessment

We have assessed the impacts of the toolkit using cost-benefit analysis, which aims to identify the full range of impacts by assessing both the costs and benefits. However, it is not practical nor necessary to consider in detail all of the toolkit's implications.

Our approach follows HM Treasury's Green Book (The Green Book)⁶, Regulatory Policy Committee⁷, and Business Impact Target guidance⁸ on best practice for impact assessments.

In identifying the potential impacts of the toolkit it is important to distinguish between:

- Additional impacts that can be attributed to the toolkit – these impacts are affected by how the ICO chooses to develop the toolkit.
- Additional impacts that are not attributed to the toolkit – these impacts are not affected by how the ICO chooses to develop the toolkit. They simply arise from the legislative requirements such as those of the UK GDPR and the DPA 2018⁹. Controllers are already expected to comply with these requirements.

It is not always possible to categorise impacts distinctly, so our assessment identifies additional impacts and then focuses on those that can be attributed to the toolkit.¹⁰ Impacts that cannot be attributed to the toolkit, such as those associated with existing legislation, are excluded from the assessment.

Impacts may be direct or indirect:¹¹

- Direct impacts: these are 'first round' impacts that are generally immediate and unavoidable, with relatively few steps in the chain of logic between the introduction of the measure and the impact taking place. In our theory of change (see Figure 1 below) these relate to the immediate and intermediate outcomes.

⁶ HM Treasury (2022): <https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government>

⁷ Regulatory Policy Committee (2020): <https://www.gov.uk/government/collections/rpc-guidance-for-departments-and-regulators>

⁸ Department for Business, Energy and Industrial Strategy (2019): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776507/Business_Impact_Target_Statutory_Guidance_January_2019.pdf

⁹ Data Protection Act 2018, available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents>, accessed 5th December 2022

¹⁰ For more information on attribution see OECD (2014): <https://www.oecd.org/sti/inno/Causality-OECDImpact.pdf>

¹¹ Further discussion of direct and indirect impacts can be found in: Regulatory Policy Committee (2019): <https://www.gov.uk/government/publications/rpc-case-histories-direct-and-indirect-impacts-march-2019>

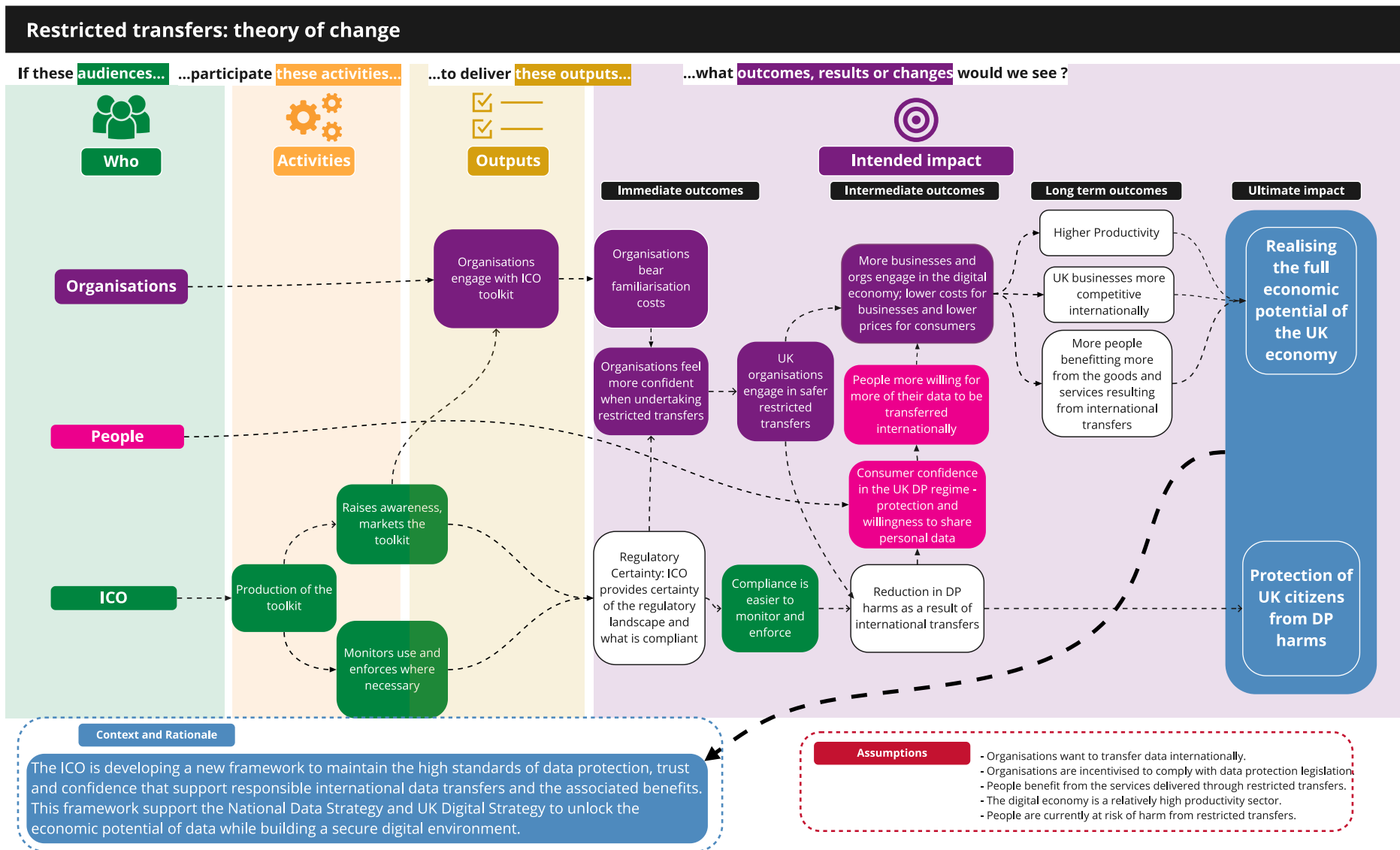
- Indirect impacts: these are 'second round' impacts that are often the result of changes in behaviour or reallocations of resources following the immediate impact of the introduction of the measure. Indirect impacts are linked to long term and ultimate impact in the theory of change.

Our assessment is split into two main parts considering the toolkit's costs and benefits.

2.1. Theory of change

Figure 1 plots our theory of change. We consider the activities carried out by the ICO, UK organisations and people in the UK and then consider how immediate, intermediate and long term outcomes contribute to impact. This framework also guides the structure of this report and the remaining chapters are colour coded according to the relevant section of the theory of change that they refer to. For example, our discussion of individuals and organisations affected by the tool kit is green reflecting the 'audiences' section of the theory of change.

Figure 1: Theory of change



We collected evidence for the impact assessment using the following methods and sources:

- desk-based research;
- responses to the public consultation;
- an ongoing evaluation of the implementation of IDTA by the Department for Digital Media, Culture and Sport (DCMS).

Consideration of options

The older EU SCCs were viewed as non-compliant in light of *Schrems II* and as such, there was a legal requirement to replace them.¹³ The development of a replacement is viewed as the only viable option as any alternative has the potential for substantial negative impacts on the economy and society.

The Commissioner did have discretion over:

- the length and makeup of the IDTA; and
- the supporting guidance and materials that make up the rest of the toolkit.

We do not consider it proportionate or appropriate to assess the impacts of alternative lengths and makeups of the toolkit. Where possible, we have provided ICO that could give insights into the relative impacts of each of the materials in the toolkit but have not gone further than this.

For these reasons, we have not considered the impact of alternative options in our assessment (aside from the counterfactual). We adopted a similarly proportionate approach to complete the impact assessments for the Draft Journalism Code¹⁴, Data sharing code of practice¹⁵ and the Age-appropriate design code of practice¹⁶.

Counterfactual

To help us to measure the impact of the toolkit, we need a counterfactual, which is the baseline against which we estimate the additional impacts of introducing the toolkit. In the absence of the introduction of the toolkit, then the underlying data protection legislation would continue to apply and form the counterfactual for the purposes of this assessment.

¹³ See Section 3. for more information

¹⁴ ICO (2021): <https://ico.org.uk/media/about-the-ico/documents/4018652/draft-economic-impact-assessment-202110.pdf>

¹⁵ ICO (2021): <https://ico.org.uk/media/2619796/ds-code-impact-assessment-202105.pdf>

¹⁶ ICO (2020): https://ico.org.uk/media/about-the-ico/documents/2617988/aadc-impact-assessment-v1_3.pdf

In line with impact assessment guidance¹⁷, and where appropriate, we assume compliance with legislation in the absence of specific evidence to suggest otherwise. This simplifies the assessment in some areas, but it is not intended to suggest that there is total compliance. If we did identify any specific lack of compliance, the toolkit would help controllers to improve.

It should be noted that the toolkit does not impose any additional legal obligations, which limits the toolkit's additional impacts over and above that of the counterfactual.

Monetising impacts

Quantified analysis of the impacts is particularly challenging for the toolkit because of its wide ranging scope and the difficulty in quantifying the affected groups.

Calculating the additional cost to controllers is also complex because the nature of these costs varies considerably depending on the different factors, for example:

- how sophisticated and mature the controller's existing data protection systems and processes are;
- the nature of the activities;
- the processing associated with those activities; and
- the level of risk to individuals.

It is similarly challenging to quantify many of the toolkit's benefits, such as:

- reductions in harm;
- increased regulatory certainty; or
- increased trust amongst the public because of their intangible nature.

Our analysis therefore focuses primarily on non-monetised impacts. However, where possible, we have provided high level quantitative analysis to indicate scale.

Uncertainty, risk and optimism bias

As set out in the Green Book¹⁸, it is necessary to consider the significant levels of uncertainty surrounding the impacts of the toolkit. Although optimism bias is typically only considered in capital projects¹⁹, we understand that there can be a

¹⁷ BEIS (2017):

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609201/business-impact-target-guidance-appraisal.pdf

¹⁸ HM Treasury (2022): <https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2020>

¹⁹ See section 2.6.27 of Department for Finance Northern Ireland's Risk and Optimism Bias Guidance: available at <https://www.finance-ni.gov.uk/articles/step-six-assess-risks-and-adjust-optimism-bias>, accessed 5th December 2022

tendency to overestimate engagement with guidance. To account for and demonstrate the implications of any potential bias, we have provided some sensitivity analysis for the impacts we have been able to quantify.²⁰ This tests the sensitivity of impact estimates to changes in assumptions and is provided in Annex A but is limited in accordance with the principle of proportionality in impact assessment.

²⁰ For more information on sensitivity analysis see paragraph 5.59 of HM Treasury (2022): <https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2020>

3. Context

The ICO has developed and published the IDTA following the UK's withdrawal from the EU. This was a necessary step because the old EU SCCs were not aligned with UK GDPR and the new EU SCCs do not apply to the UK because they were implemented following the UK's withdrawal from the EU. The ICO has also published the UK Addendum to the EU SCCs which enables the new EU SCCs to be used in a UK context.

Both the IDTA and the UK Addendum to the EU SCCs are designed to help streamline and secure safe and responsible restricted transfers.

As part of the suite of tools supporting the IDTA, the ICO has developed a Transfer Risk Assessment (TRA) tool to assist controllers in assessing the risks associated with restricted transfers. The requirement for a transfer risk assessment stems from the July 2020 CJEU decision in Schrems II. In this impact assessment we will refer to the IDTA, the TRA tool and the suite of supporting guidance as the toolkit.

This section sets out the economic, social and political context for restricted transfers (the transfer of personal data to and from the UK), the potential harms that can arise, as well as the rationale for the toolkit.

3.1. Social and economic context

Data is one of modern society's greatest assets. Sharing personal data can lead to many economic and social benefits, including economic growth, technological innovation and the delivery of more efficient and targeted services. The ability to engage in the cross-border trade in data has the potential to enhance these benefits to the UK economy and society.

However, transfers of personal data are not without risk. Once personal data has left the UK it is not exclusively subject to UK data protection law and thus, in some circumstances, the risk of harm may be elevated.

The protection of personal data through maintaining privacy and ensuring secure processing remain a key regulatory concern.

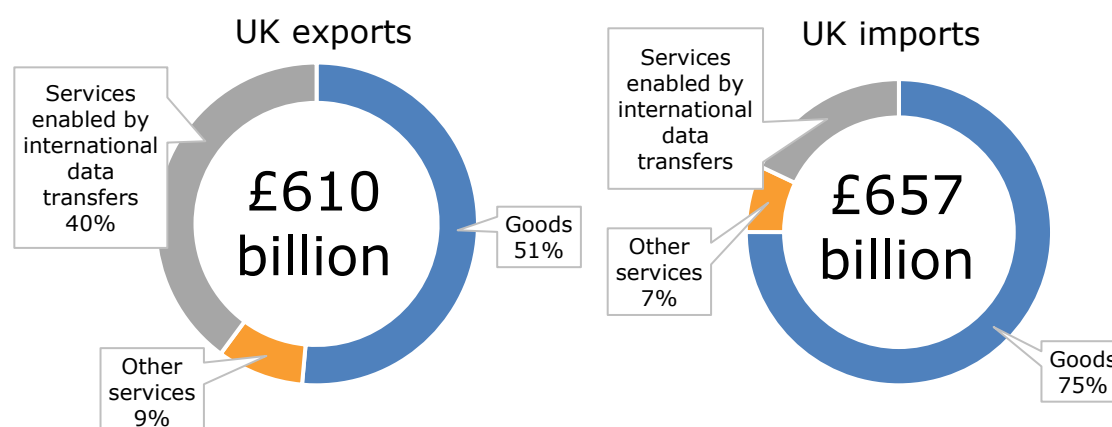
A degree of privacy and limits on the ability of organisations to share personal data is necessary for citizens' physical, mental and social well-being and development. The importance of privacy is recognised by both the UK courts and the European Court of Human Rights. The right to privacy is enshrined in the European Convention of Human Rights, which is reflected in the UK GDPR and the DPA 2018.

With this toolkit, the ICO seeks to support UK businesses and organisations to realise the economic and social benefits from restricted transfers while ensuring an appropriate level of protection for UK citizens against potential harms.

3.1.1. Significance to the UK economy of international data transfers

In 2020, the value of international data transfers to UK exports was £243 billion and to UK imports was £118 billion.²¹ This represented almost 40% of exports and just under a fifth of imports, as shown in Figure 2 below.

Figure 2: The value of services enabled by international data transfers to UK exports and imports in 2020



Source: DCMS (2021): [Data: a new direction, Analysis of Expected Impact, paragraph 61 2021](#); ONS, [UK Trade in services by modes of supply, 2020](#); ICO analysis.

The economic importance of international data transfers is further demonstrated by the level of business interaction. For example, it is likely that all cloud based systems will involve a data transfer²². Though data availability on this matter is limited to allow quantification. However, based on available data from the DCMS Business Data Survey 2022²³ and Department for Business, Energy and Industrial Policy's Business Population Estimates²⁴, we estimate that 783,000 UK businesses and organisations currently transfer data outside the UK, as shown in Table 4 below. The remainder of this section provides further detail on these numbers.

²¹ The value of data transfer to UK exports and imports is calculated using ONS Modes of Supply data (2022): <https://www.ons.gov.uk/businessindustryandtrade/internationaltrade/articles/modesofsupplyukexperimentalesimates/2020>. This follows the approach adopted by DCMS (2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016471/Data_Reform_Impact_Analysis_Paper.pdf paragraph 61, we assume 'Mode 1: Remote Trade' to be an estimate of digital or remotely delivered services.

²² The toolkit clarifies that only one entity is responsible for the transfer, i.e. the controller or the processor, and not both (different for joint controllers).

²³ DCMS (2022): <https://www.gov.uk/government/statistics/uk-business-data-survey-2022>

²⁴ BEIS (2021): <https://www.gov.uk/government/statistics/business-population-estimates-2021>

Table 4: Businesses or organisations that transfer (send or receive) data to or from other organisations, businesses or people based outside the UK

Sector	Estimated number
Private	756,000
Public	2,200
Charities	24,500
Whole economy	783,000

Source: [DCMS, UK Business Data Survey 2022](#); [BEIS, Business Population Estimates 2021](#); ICO analysis.

Analysis of the private sector

As illustrated in Table 5, the DCMS Business Data Survey²⁵ shows that around 756,000 companies transfer data internationally and large businesses are more likely to transfer than companies with fewer employees. While we are not able to estimate the number of jobs or the proportion of these jobs that are fully dependent on the international transfer of data, we expect this to be significant.

Table 5: Private sector organisations who transfer data outside UK by business size

Number of employees	Percentage that transfer (send or receive) data with other organisations or people based outside the UK	Estimated number of businesses
None	14%	566,000
1 to 49	13%	181,000
50 to 249	16%	5,770
250+	41%	3,010
Total	14%	756,000

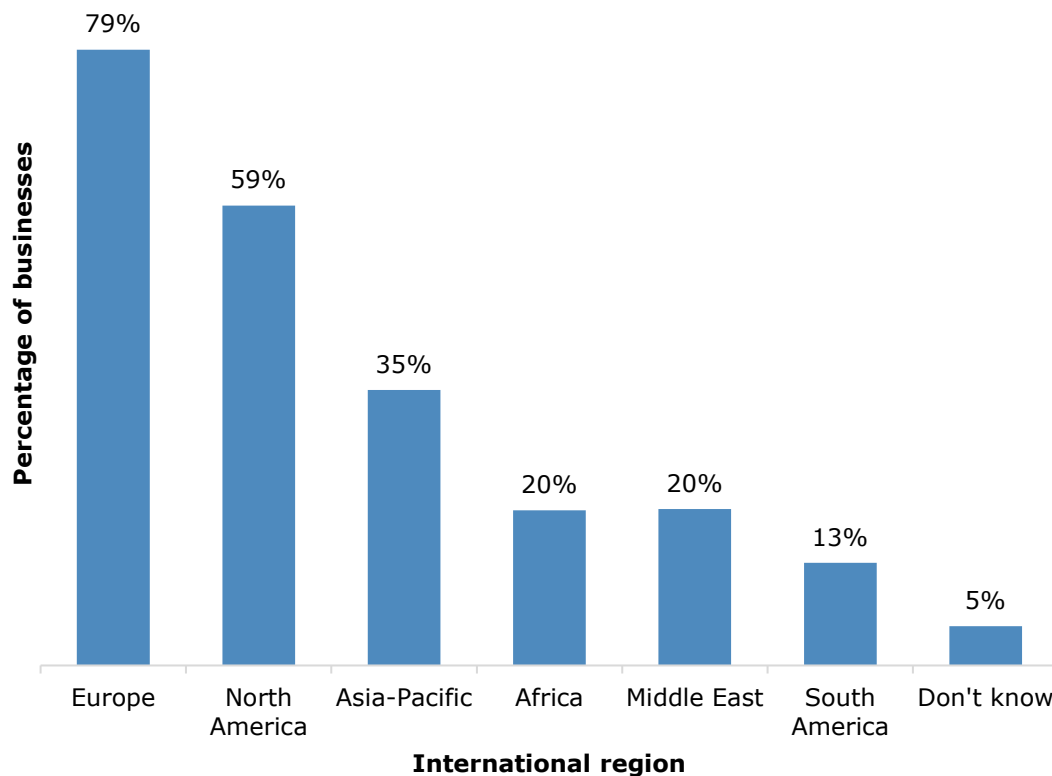
Source: [DCMS, UK Business Data Survey 2022](#).

Figure 3 shows, of businesses that transfer data internationally, 79% send or receive it to or from Europe, and 59% send or receive it to or from North

²⁵ DCMS (2022): <https://www.gov.uk/government/statistics/uk-business-data-survey-2022>

America. International data transfer to these regions is more significant making them more sensitive to the impact of regulatory activity.

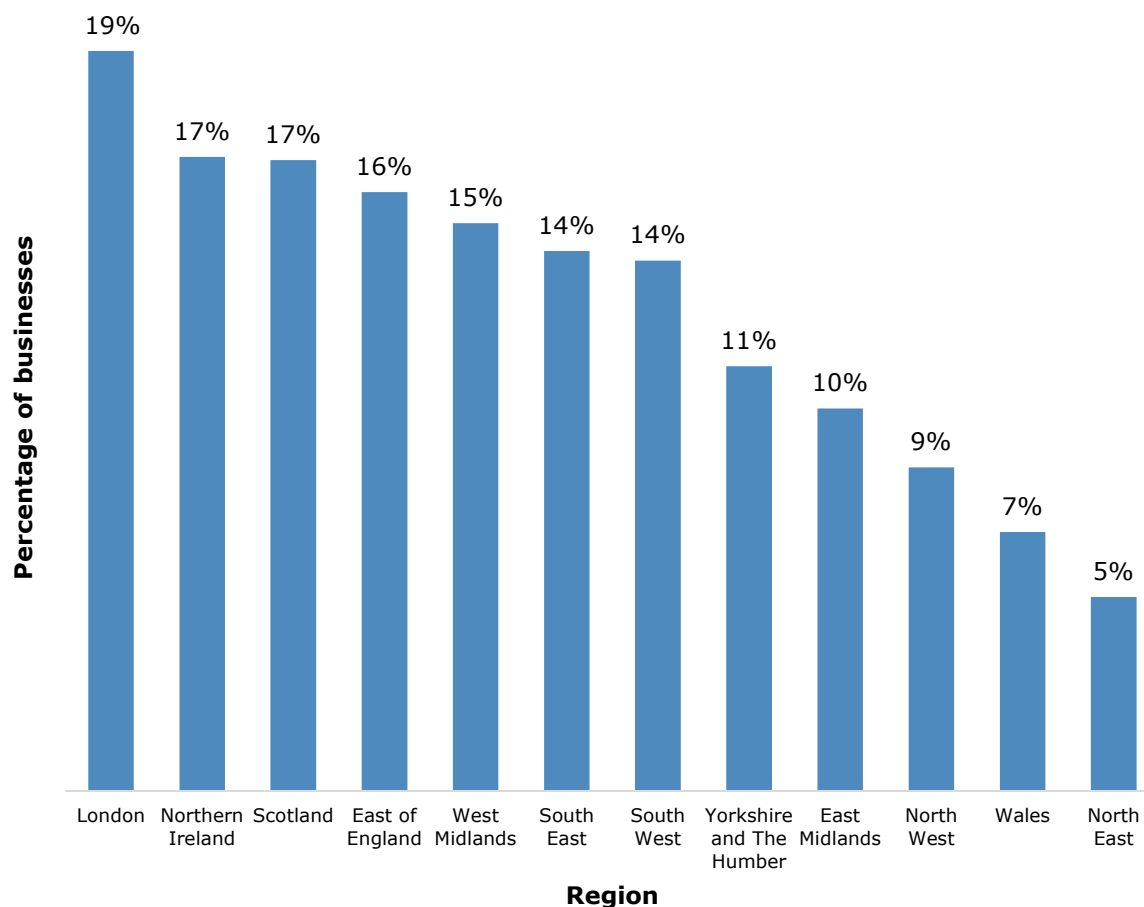
Figure 3: International regions businesses transfer (send or receive) data to or from as a percentage of businesses that transfer data outside of the UK



Source: [DCMS, UK Business Data Survey 2022](#)

As illustrated in Figure 4, UK businesses that transfer personal data internationally are based in all regions of the UK. There is a particular concentration in London, which may make it more sensitive to the impact of regulatory activity. The North East, North West and Wales are likely to be less sensitive to the impact of regulatory activity.

Figure 4: Percentage of UK businesses that transfer (send or receive) data with other organisations, businesses or people based outside the UK by region²⁶



Source: [DCMS, UK Business Data Survey 2022](#)

The public sector and charities

Our research was not able to source robust data on the number of public sector organisations or charities that engage in international personal data transfers.

For our modelling, we have estimated the number of public sector organisations and charities by number of employees and then assumed the same proportion transfer personal data internationally as in similar sized private sector businesses, as shown in Table 6 below. This is a simplifying assumption in the absence of additional evidence, see Annex A sections on **Public sector organisations** and **Charities** for further discussion on our assumptions.

²⁶ Data rounded to nearest whole number.

Table 6: Estimate of the number of organisations engaged in international transfers of data

Organisation size	Public sector (% by number of employees)	Charities (% by number of employees)
Micro	940 (13%)	22,000 (13%)
Small	200 (16%)	1,600 (16%)
Medium	370 (16%)	180 (16%)
Large	680 (41%)	560 (41%)
Total	2,200	24,500

Source: [DCMS, UK Business Data Survey 2022](#); [BEIS, Business Population Estimates 2021](#); ICO analysis.

3.1.2. Data protection harms related to the transfer of personal data to or from the UK

Given the wide and varied nature of international personal data transfers, the associated potential data protection harms vary significantly, in degree and type. In line with damages, as described in Article 82 of the UK GDPR²⁷, harms can include:

- **physical harm:** physical injury or other harms to physical health;
- **material harm:** harms that are more easily monetised such as financial harm; or
- **non-material harm:** less tangible harms such as distress.

This means that harm can arise from actual damage and more intangible harm, including any significant economic or social disadvantage. Of course, harms may also fall into more than one of these categories.²⁸

The potential harms associated with transferring personal data internationally are similar to those associated with transferring personal data within the UK. The key difference is that UK Government and the ICO have limited power over data controllers based outside of the UK.

The following cases are intended as indicative examples of the kind of harms that might occur when measures to keep personal data safe prove to be

²⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council, available at: <https://www.legislation.gov.uk/eur/2016/679/article/82>, accessed 5th December 2022

²⁸ For more information on data protection harms see ICO (2022): <https://ico.org.uk/about-the-ico/research-and-reports/data-protection-harms/>

insufficient to prevent harm. While all examples are theoretical, they are informed by ICO experience of where potential harms may occur. The examples are neither hierarchical nor exhaustive.

Financial harm

Financial harm occurs when personal data is negligently, knowingly or purposefully used in a way that causes financial loss to individuals.

Example: Cyber-attack on airline network

Airlines provide services to individuals across many countries. Many airlines group together to form networks which collectively offer perks to regular customers. This involves the transfer of sensitive personal data such as bank details and passport numbers. In the event of data being passed to a jurisdiction with lower levels of protection than the UK, the risk of a data breach is increased. Where the breach includes identity documents and credit card details there is a risk of financial loss to individuals.

Bodily and psychological harm

Bodily harm occurs when personal data is negligently, knowingly or purposefully used in a way that causes physical injury to individuals. Psychological harm occurs when personal data is negligently, knowingly or purposefully used in a way that causes emotional distress or disturbance to individuals.

Example: Personal data held by international organisation exposes vulnerable people

A database belonging to an international organisation is hacked and the personal data of political dissidents (including UK citizens) is stolen. The data includes information on individuals' locations. The awareness that data has been compromised could lead to emotional distress. The exposure of location could lead to vulnerable individuals being tracked down and subject to bodily harm.

Discriminatory harm

Discriminatory harms occurs when harm arises from bias, either consciously or unconsciously.

Example: Health data leaked online

The medical records of UK individuals are transferred to a jurisdiction with levels of data security below the standard of the UK. The database is hacked leading to an unauthorised disclosure of confidential data about individuals' health status. As a result, individuals affected could then be exposed to discrimination based

on their health status, such as being barred from travel to certain countries or denied employment opportunities.

Harm to national security

Societal harms can occur when national security is put at risk. When this occurs the harms or potential harms to society are usually greater than the harms to the individuals whose personal data is involved.

Example: Defence contractor hit by data breach

An overseas government contractor working on national defence is attacked by a hostile state actor which steals the personal data of UK military personnel. The highly sensitive nature of the personal data held by the contractor (location of critical military infrastructure) means there is the potential for further consequences for wider society.

3.1.3. Qualitative examples of benefits of International Data Transfers

The transfer of personal data internationally has resulted in many positive social and economic outcomes. Below we describe examples from different sectors of the economy.

Medical sciences

Transferring personal medical data internationally was crucial in the development of Covid-19 vaccines including that developed by AstraZeneca and Oxford University.²⁹ This vaccine was trialled in three countries, the UK, Brazil and South Africa, and the ability to share data internationally was crucial in securing enough data to assess efficacy and safety in a timely manner.

Medical research into drugs with small patient populations relies on international sharing of patient data in order to gather statistically significant populations to determine efficacy and safety.

Law enforcement

The International Criminal Police Organization (Interpol) shares and provides access to data on crimes and criminals across 195 member countries. This international collaboration allows police forces worldwide to tackle cybercrime, organised crime and terrorism.³⁰

²⁹ The Lancet (2020): [https://www.thelancet.com/journals/lancet/article/PIIS0140-6736\(20\)32661-1/fulltext](https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)32661-1/fulltext)

³⁰ Interpol, "What is INTERPOL?", available at: <https://www.interpol.int/Who-we-are/What-is-INTERPOL>, accessed 5th December 2022.

The United Nations shares data on identified instances of human trafficking, including individual and community data on prevalence and location, cause and effect, to develop knowledge and improve policies aimed at tackling it.³¹

Genealogy

Genealogy mapping is able to connect individuals with their geographical origins and with family members that they previously did not have contact with.³² This service would be significantly curtailed without the possibility of transferring genetic data across national borders.

Marketing

Transferring customer profile data allows companies to engage in targeted advertising, which reduces search costs for both business and consumers, leads to more trade and therefore greater social welfare. An international market for online marketing expands the pool of consumers, leading to greater competition, lower prices and greater social welfare than in a national market.

3.1.4. Barriers to international personal data transfers

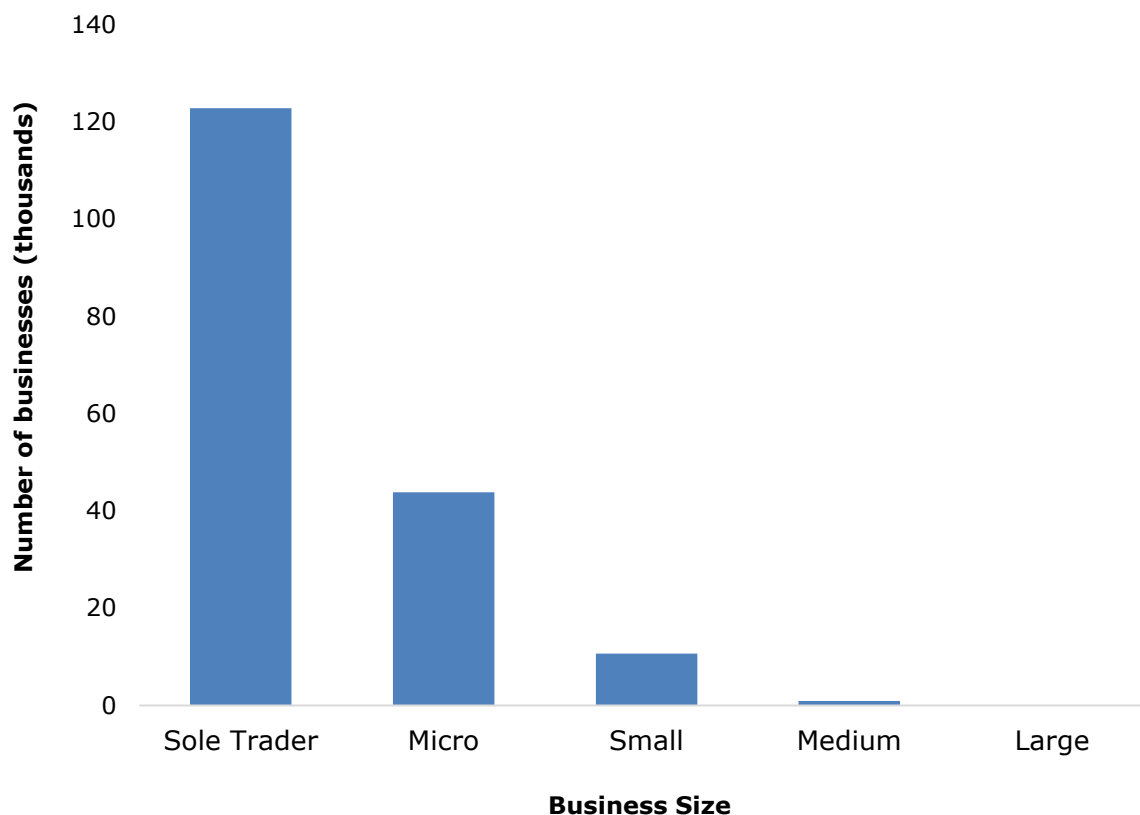
Around 3.9 million UK businesses that hold digitalised data do not transfer personal data outside of the UK.³³ Of these businesses, around 180,000 (3% of all UK businesses) do not transfer personal data outside of the UK because they are concerned about the legal risks or uncertainty relating to UK data protection laws. Most of these businesses are sole traders, micro or small businesses. Our guidance is designed to reduce uncertainty which will encourage the use of data transfer and result in positive economic impact. While we do not have comparable data for public sector organisations and charities, it seems likely that reducing uncertainty would also have a positive impact.

³¹ United Nations (2016), "*Combating transnational crime*", available at https://www.un.org/esa/ffd/wp-content/uploads/2016/01/Combating-transnational-crime_IOM_IATF-Issue-Brief.pdf, accessed 5th December 2022

³² Ancestry.com, available at: <https://www.ancestry.com/c/ancestry-family>, accessed 5th December 2022

³³ ICO analysis of BEIS (2021): <https://www.gov.uk/government/statistics/business-population-estimates-2021>, Table 1 and DCMS survey 2022, Table 1 and Table 29.

Figure 5: Estimate of the number of UK businesses that do not share data with businesses, organisations or people outside the UK because they are concerned about the legal risks or uncertainty of transferring data internationally relating to the UK data protection

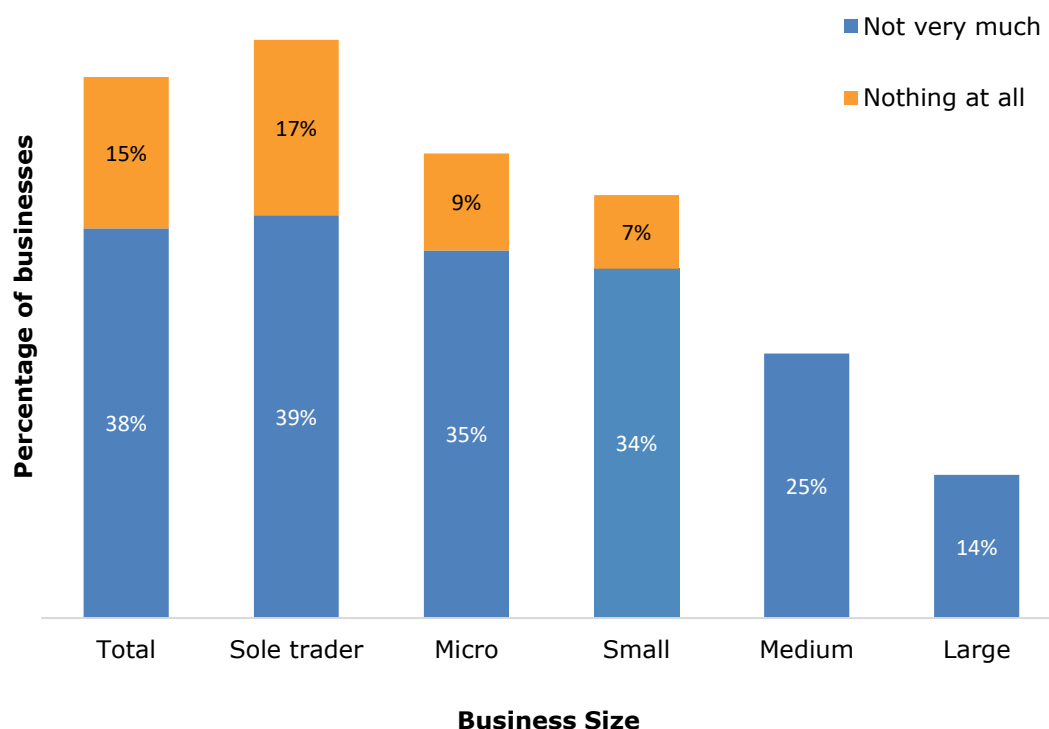


Source: [DCMS, UK Business Data Survey 2022](#); [BEIS, Business Population Estimates 2021](#); ICO analysis.

3.1.5. Business awareness of legal compliance

Amongst UK businesses that already transfer personal data outside of the UK, 53% state that they know 'nothing at all' or 'not very much' about the legal compliance necessary, as illustrated in Figure 6 below. This suggests an elevated risk of harm occurring to those whose personal data is transferred. The ICO's toolkit will increase awareness of legal compliance and is therefore likely to reduce the risk of harm to people in the UK.

Figure 6: Business awareness of legal compliance necessary to transfer personal data outside of the UK among businesses who already transfer data.



Source: [DCMS, UK Business Data Survey 2022](#); [BEIS, Business Population Estimates 2021](#); ICO analysis.

3.1.6. Market failure rationale

From an economic point of view, data and digital markets have the potential to raise a range of market failure issues.³⁴ Market failures are instances where the market alone is not resulting in an efficient outcome for the economy and society more widely, providing a rationale for intervention. This can lead to unrealised potential benefits (referred to as opportunity cost) or, in some cases, cause or exacerbate harms (covered in more detail in section 3.1.2).

Key market failures in relation to the international transfers of data can be summarised as follows:

- **Economies of scale and scope:** increased international trade in data and data products can lead to more data (including personal and non-personal data) being collected and/or different data sources being combined. While this can lead to innovation it can also incentivise the hoarding or restricting of data to gain a competitive advantage and distort

³⁴ HM Treasury (2018):

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf

markets. Where this behaviour is engaged in internationally, this may require an international response to ensure the benefits of economies of scale and scope whilst sustaining competition.

- **Information failure:** a lack of understanding about the legislative framework around international personal data transfers can lead to both the inappropriate transfer of personal data and an aversion to the transfer of personal data. A lack of understanding about how and why personal data is being transferred may lead data subjects withdrawing consent for future personal data transfers. Information failures that disincentivise personal data transfers through either means may require intervention.
- **Coordination failures:** to fully realise the benefits of international transfers, it is necessary to ensure that personal data protection measures align in sending and receiving economies to ensure data subjects, data controllers and other entities in the supply chain remain compliant with national law. Intervention may be necessary to ensure this is the case.
- **Externalities:** personal data sharing, including internationally, can lead to significant positive and negative externalities to individuals and organisations who are not directly involved in the transaction (third parties). This could include some of the benefits listed in section 3.1.3 or harms in section 3.1.2. Intervention may be required to ensure that market mechanisms, most often prices, take account of both positive and negative externalities.
- **Data as a public good:** data that is shared is non-rivalrous (multiple parties can use it simultaneously without diminishing its usefulness) and in some instances non-excludable (not possible to exclude individuals from using it) meaning that individuals and organisations may not be adequately incentivised to invest in and embark on data exchange as they are not able to reap the full rewards of doing so. This means intervention may be required to improve these incentives.

3.2. Policy context

An important part of the context for the toolkit and its objectives is its alignment with specific areas of policy that the UK government is pursuing and the wider policy landscape for international data transfers.

Schrems II

In light of the *Schrems II*³⁵ decision of July 2020, in order to comply with UK GDPR, a transfer risk assessment is required when transferring personal data internationally via an Article 46³⁶ transfer mechanism such as the IDTA or the Addendum. This is to ensure that the protections for rights and freedoms of data subjects remain sufficiently similar to the UK protections at any time.

Data protection reform

As of 1 January 2021, the UK officially left the EU. This means the UK has the powers to independently define and update the legislative framework applicable to international personal data transfers from the UK to third countries. The UK government considers international data flows (both personal and non-personal) key to enabling the development of the digital economy.

The ICO is developing the toolkit to maintain the high standards of data protection, trust and confidence that support responsible international data transfers and the associated benefits.

UK government strategy

The most relevant and recent policies are the government's National Data Strategy, published in December 2020, and the UK digital strategy, published in 2022.

National Data Strategy

The National Data Strategy³⁷ looks at how the UK's existing strengths can be used to boost the better use of data across businesses, government, civil society and individuals.

The strategy has five main missions which set out the priority areas for action for the strategy. Table 7 below shows the missions that the toolkit most closely aligns with.

³⁵ Short name given to the 2020 decision by Europe's top court (the Court of Justice of the European Union), that invalidated Privacy Shield, the adequacy decision that was relied on to legitimately transfer personal data from the European economic area (effectively including the UK at the time) to the United States of America. For more information see European Parliament (2020):

[https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATAG\(2020\)652073_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATAG(2020)652073_EN.pdf)

³⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council, available at:

<https://www.legislation.gov.uk/eur/2016/679/article/46>, accessed 5th December 2022

³⁷ DCMS (2020): <https://www.gov.uk/guidance/national-data-strategy>

Table 7: Alignment to National Data Strategy

National Data Strategy Missions	Toolkit alignment
Unlocking the value of data across the economy	By creating conditions for businesses and other organisations to engage in the global digital market with confidence that rights and intellectual property can be protected, this toolkit will support efforts to secure existing and unlock new economic opportunities for the UK, as discussed in section 3.1.3.
Securing a pro-growth and trusted data regime	This toolkit clarifies and simplifies the measures that businesses and organisations have to take to ensure restricted transfers are used responsibly and securely, without undue regulatory uncertainty or risk, to maintain and drive economic growth.
Transforming government's use of data to drive efficiency and improve public services	Provide public sector organisations with the confidence to engage with the global data market to support them in realising the untapped potential of government and public sector data to deliver better services.
Ensuring the security and resilience of the infrastructure on which data relies	Although the toolkit does not specifically cover infrastructure, many of the tools within it contribute to a secure and resilient architecture.
Championing the international flow of data	This toolkit helps businesses and organisations to engage in the exchange of information internationally, fuelling global business operations, supply chains and trade, and powering growth across the world

Source: ICO analysis and National Data Strategy.

UK Digital Strategy

The toolkit supports the UK government's delivery of the UK Digital Strategy,³⁸ as demonstrated in Table 8 below.

Table 8: Alignment to UK Digital Strategy

UK Digital Strategy	Toolkit alignment
Digital Foundations: Unlocking the power of data	<p>This toolkit aids the Government's stated aims of ensuring 'our reform of UK legislation of personal data is compatible with maintaining free flow of personal data from Europe'³⁹ and to 'reduce burdens of business and innovation, which impede the responsible use of personal data.'⁴⁰</p> <p>The toolkit further supports the Government's aim of 'seek[ing] international trade agreements to facilitate the free flow of data with trust.'⁴¹</p>
Digital Foundations: A secure digital environment	<p>The toolkit supports the goal of 'ensuring that the UK continues to be a leading responsible and democratic cyber power, able to protect and support our interests in and through cyberspace to achieve our national goals.'⁴²</p>
Enhancing the UK's place in the world	<p>The toolkit helps to ensure 'the international rules that govern digital, data and technology evolve in a way that enshrines openness at their core, preserves the existing multi-stakeholder governance models, and counters authoritarian states seeking to export their approaches.'⁴³</p> <p>Further the toolkit supports the goal of opposing 'unjustified data localisation, including by seeking to ensure that the free flow of data and anti-data localisation provisions are included in trade</p>

³⁸ DCMS (2022): <https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy>

³⁹ Ibid, p18.

⁴⁰ Ibid, p18.

⁴¹ Ibid, p19.

⁴² Ibid, p26.

⁴³ Ibid, p75.

agreements, such as free trade. agreements, that we reach with other countries.’⁴⁴

Source: ICO analysis and UK Digital Strategy.

As demonstrated above, the toolkit aligns well with recent relevant policy and has the potential to assist in progressing government objectives.

⁴⁴ Ibid, p77.



4. International transfers guidance and tools

The IDTA and Addendum were issued under Section 119A(1) of DPA 2018⁴⁵ and following parliamentary approval came into force on 21 March 2022. The ICO has also developed a suite of guidance and tools to support organisations in using the IDTA and Addendum. The suite of tools and guidance, alongside the IDTA and Addendum, are what we refer to as the toolkit.

When an organisation moves personal data outside countries deemed to have 'adequate' data protection legislation they must ensure that appropriate safeguards are in place to protect people's rights.

There are a number of appropriate safeguards listed in Article 46 UK GDPR⁴⁶. Before leaving the EU one type of appropriate safeguard often used was the EU SCCs. These clauses are a form of words that give appropriate legal protection, and minimise the need for every organisation to create the legal text from scratch.

With the UK leaving the EU, EU SCCs have now been replaced with:

- the IDTA which perform a similar function;
- the UK Addendum to the EU SCCs which allow EU SCCs to be adapted for compliance with UK regulations in certain circumstances; and
- guidance on how these should be applied, including a TRA.

ITDA Toolkit

Suite of guidance and tools to enable exporters to comply with Article 46 of the UK GDPR when making restricted transfers

Clauses

IDTA

International Data Transfer Agreement replacing standard contractual clauses for international transfers

Clauses

Addendum

European Commission's standard contractual clauses for international data transfers

Guidance

IDTA guidance

Guidance on how to use and understand the IDTA and addendum

Tool

TRA tool

Tool providing step by step process for carrying out a transfer risk assessment

Guidance

TRA guidance

Guidance on how to use and understand the TRA Tool and Record

Example

TRA examples

Worked examples of transfer risk assessments

⁴⁵ Data Protection Act (2018), available at:

<https://www.legislation.gov.uk/ukpga/2018/12/section/119/enacted>, accessed 5th December 2022

⁴⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council, available at:

<https://www.legislation.gov.uk/eur/2016/679/article/46>, accessed 5th December 2022

The IDTA came into force on 21 March 2022 and the ICO transfer risk assessment tool was published in November 2022. The IDTA guidance is still under development but is expected to be published by early 2023 followed by additional TRA examples.⁴⁷

Organisations were still able to rely on transitional provisions for contracts signed on or before 21 September 2022 allowing them to use EU SCCs. From then on any new contracts are required to use the IDTA or the EU SCC Addendum. Contracts using EU SCCs, relying on transitional provisions, will need to be amended or replaced on or before 21 March 2024.⁴⁸

The aims of the toolkit are:

- to provide greater regulatory certainty and assist organisations to comply with the law;
- for the UK to develop its own tools and resources in recognition of the importance of international data flows to the UK's digital economy and maintaining high standards of data protection;
- to enable compliance with the *Schrems II* judgement where the Court held that risk assessments must be undertaken before tools such as the IDTA can be relied on; and
- to form part of a wider UK package to assist international transfers, including independently supporting the UK government's approach to adequacy assessments of third countries.⁴⁹

The toolkit does not impose any legal requirements beyond those already in the legislation. It is assumed controllers understand their legal obligations under the UK GDPR and the DPA 2018 and comply effectively.

4.1. Approach to the toolkit

The toolkit was developed in consultation with industry and other relevant bodies. A number of workshops have also been carried out to assist in the development of the toolkit. Specific dissemination activities include:

- A draft consultation between August 2021 and October 2021;⁵⁰
- Six workshops with stakeholders held in September 2021; and
- Communications and marketing activity.

⁴⁷ In 'Annex A: Familiarisation costs' we have included a working draft of the IDTA guidance in our analysis.

⁴⁸ ICO (2022): [scc-transitional-provisions.pdf \(ico.org.uk\)](https://ico.org.uk/for-organisations/our-work/transfer-risk-assessment-toolkit/scc-transitional-provisions.pdf)

⁴⁹ DCMS / ICO (2021): <https://ico.org.uk/media/about-the-ico/mou/2619468/uk-adequacy-assessments-ico-dcms-memorandum-of-understanding.pdf>

⁵⁰ The consultation received 97 responses.

In response to the feedback received during the consultation, the ICO:

- Revised the processes set out in the TRA tool to streamline the approach;
- Shortened the documents that make up the toolkit;
- Made the TRA tool more interactive, allowing information to be documented in the tool; and
- Used simple language and examples to make it easier for business to comply with legislation.

4.2. Scope of the guidance

The toolkit contains guidance for organisations transferring data to and from the UK who must comply with the UK GDPR and DPA 2018. Although the toolkit is potentially useful to all organisations considering an international data transfer, it is most useful for those making a restricted transfer. Those considering transfers to countries where an adequacy agreement is in place, will not necessarily need to engage with the toolkit.



4.3. Affected groups

Although the scope of international personal data transfers is far reaching, in the interests of a proportionate assessment, we have sought to identify those with the highest potential to be affected by the toolkit.

The groups and individuals that will be affected by the toolkit are:

- UK businesses, organisations and charities;
- Individuals whose data is transferred;
- The Information Commissioner's Office;
- Justice system; and
- Wider society.

We now examine each of these groups in detail.

4.3.1. UK businesses, organisations and charities

The way that businesses and other organisations will be affected will differ due to a number of factors such size, employee numbers, sector, etc. These factors are explored in more detail in Annex A.

- We estimate that around 783,000 businesses and organisations that currently engage in international personal data transfers will be directly affected by the toolkit.
- There are an additional 4 million business or organisations who already hold digitalised data but do not necessarily engage in international transfers. There is some potential for the toolkit to provide some additional confidence for them to engage in international transfers.

We have set out the broad groups of affected businesses and other organisations in more detail below.

Businesses or organisations that currently transfer data internationally

As explored in Section 3.1.1 and summarised in Table 9, we estimate that around 783,000 UK businesses or organisations currently transfer personal data outside the UK.⁵¹ This group could benefit from the increased regulatory certainty and a reduced administrative burden through the use of the toolkit.

⁵¹ DCMS (2022): <https://www.gov.uk/government/statistics/uk-business-data-survey-2022>; ICO Analysis – Note: we were not able to source estimates for the proportion of non-business organisations that transfer data outside the UK. As such the proportions for businesses by size band we're applied to public sector organisations and charities by size band.

Table 9: Businesses or organisations that transfer (send or receive) data with other organisations, businesses or people based outside the UK

Sector	Estimated number	Percentage of sector
Private	756,000	13.5%
Public	2,200	18%
Charities	24,500	13%
Whole economy	783,000	13.5%

Source: [DCMS, UK Business Data Survey 2022](#); [BEIS, Business Population Estimates 2021](#); ICO analysis.

Considering the private sector alone, using the assumption set out in Section 3.1.5, around 395,000 (53%) businesses that currently transfer personal data outside of the UK are not aware of necessary legal compliance, as shown in Table 10 below. This is more common amongst smaller businesses. This lack of awareness is a risk to individuals whose personal data is transferred and also a legal risk to the businesses engaging in the transfers. The toolkit has the potential to mitigate some of this risk.

Table 10: Businesses that are not aware of necessary legal compliance for transfer outside of the UK

Business size	Estimated number	Percentage of businesses of this size that transfer data
Sole traders	315,000	56%
Micro	65,000	45%
Small	13,000	41%
Medium	1,500	25%
Large	500	14%
Total	395,000	

Source: [DCMS, UK Business Data Survey 2022](#); [BEIS, Business Population Estimates 2021](#); ICO analysis.

Businesses or organisations that do not transfer data internationally because of concerns around legal risk

Using the assumptions set out in Section 3.1.4, up to 181,000 UK businesses could benefit from increased legal certainty provided by the toolkit and stand to achieve gains from international personal data transfers, as shown in Table 11.

Table 11: Business that currently do not transfer personal data due to concerns about legal risks

Business size	Estimated number	Percentage of UK businesses of this size
Sole traders	125,000	3%
Micro	45,000	4%
Small	10,000	5%
Medium	1,000	3%
Large	0	0%
Total	181,000	

Source: [DCMS, UK Business Data Survey 2022](#); [BEIS, Business Population Estimates 2021](#); ICO analysis.

Other businesses or organisations that do not currently transfer personal data internationally

Around 3.9 million (84%) of UK businesses that hold digitalised data do not currently transfer personal data outside the UK. This group may be experiencing some of the market failures outlined in Section 3.1.6. This toolkit could help to alleviate these market failures and facilitate an indirect positive economic impact on these businesses.

Summary

We estimate that this toolkit will directly impact 783,000 organisations (13.5% of whole economy) who currently engage in international transfers of personal data. We further find that for up to 3.9 million organisations (67% of whole economy), the toolkit could have a positive economic benefit.

4.3.2. Individuals whose data is transferred

Although we cannot be certain, given the widespread use of tools and services in other countries, we believe it is reasonable to assume that all individuals in the UK are indirectly subject to an international data transfer at some stage. We therefore assume that the number of people directly affected to be the whole UK

population. The latest Office for National Statistics (ONS) data puts this at 67.1 million in 2020.⁵²

4.3.3. The Information Commissioner's Office

The ICO will be affected, as the regulator of data protection legislation and as the producer of the toolkit.

4.3.4. Justice system

As the IDTA is a legislative instrument, the justice system will be affected and use of the toolkit is likely to be a factor in some judicial proceedings.

4.3.5. Wider society

As set out in the theory of change, the toolkit is intended to contribute to the realisation of the full economic potential of the UK economy through facilitation of safe and compliant international data transfers and to the protection of UK citizens from data protection harms.

A stronger economy would benefit all UK citizens: UK workers, UK consumers and recipients of UK government services, around 67.1 million individuals.⁵³

Better protection could directly benefit all UK data subjects. Reduction in data protection harms will indirectly impact other UK citizens through a reduction in societal harms and harms to family, friends or associates.

⁵² ONS (2021):

<https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/timeseries/ukpop/pop>

⁵³ ONS (2021):

<https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/timeseries/ukpop/pop>



5. Costs and benefits of the toolkit

In this section, we consider the toolkit's potential costs and benefits. Our aim is to understand whether there are likely to be significant impacts on affected groups (both positive and negative) and to judge the toolkit's overall impact on society.

We draw on a mixture of quantitative and qualitative evidence, as detailed in Annex A. However, as noted previously, our analysis is limited by the evidence available.

The analysis of impacts is split into three parts:

- Familiarisation costs
- Reduction in data protection harms
- Impact of greater organisational confidence to carry out international data transfers

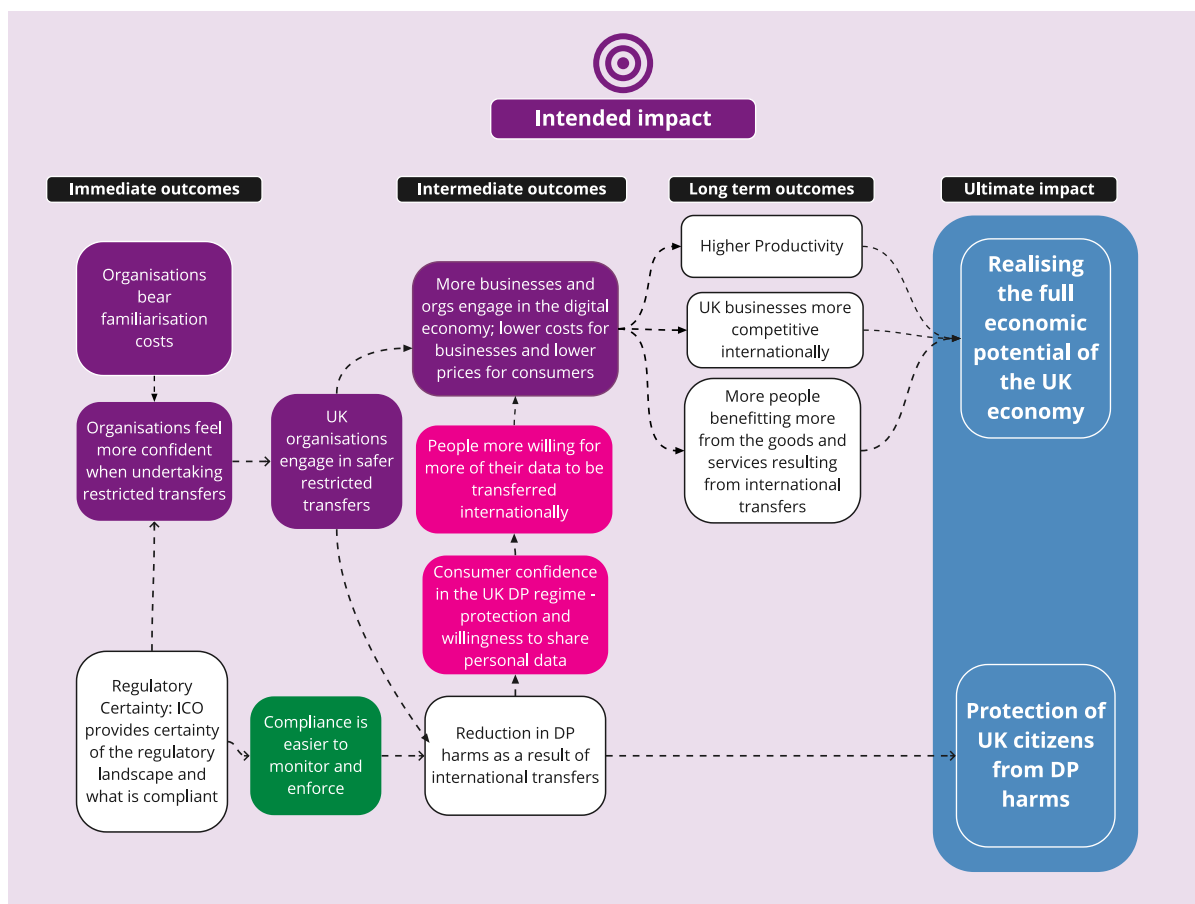
Our analysis excludes impacts that result from existing legislation. For example, the requirement to produce a transfer risk assessment does not stem from the toolkit, this is an existing requirement of DPA 2018 and UK GDPR.

The impacts are assessed under the following headings which then feed into our conclusion on the toolkit's overall impact on society.

- **Cost:** a discussion of the related costs that could bring about significant impacts to affected groups.
- **Benefits:** as with costs.
- **Categorisation of impact:** our assessment of whether there is likely to be a significant net cost or benefit as well as the categorisation of the impact (ie level of attribution of the toolkit).

Figure 7 below sets out the intended impacts of the toolkit from our theory of change.

Figure 7: Intended impacts



Source: ICO analysis.

5.1. Cost benefit analysis of the toolkit

We summarise our assessment of impacts in the table below and then discuss each impact in turn.

Table 12: Impacts of the toolkit

Impacts	Positive, neutral or negative	Attributable to the toolkit
Familiarisation costs	Negative	Attributable
Data protection harms	Positive	Partially attributable
Business and organisational confidence in doing transfers	Positive	Partially attributable

5.1.1. Costs

Potential costs of the toolkit are set out below.

Familiarisation costs

Organisations will incur a cost to familiarise themselves with the toolkit because of the time taken to read and become familiar with it. These are referred to as familiarisation costs.⁵⁴

Organisations are not required by law to familiarise themselves with the toolkit. However, as the toolkit is designed to make international data transfers simpler, our expectation is that some organisations will familiarise themselves with it. That said, the extent to which this is required, and for which elements of the toolkit, will vary significantly between organisations. We have made assumptions about the mix of materials that will be read according to likelihood of engagement with the toolkit.

Combining this analysis with evidence from the Department for Business, Energy and Industrial Strategy (BEIS) Business Population Estimates and DCMS survey data, we estimate 783,000 organisations will engage with the toolkit at an indicative familiarisation cost to the UK economy of around £45 million.⁵⁵ It should be noted that this is likely an upper end estimate of the total costs as it is not clear to what extent particular organisations will engage with the toolkit, if at all.⁵⁶

Table 13: Familiarisation cost to UK economy

Likelihood to engage with the toolkit based on sector/size	Organisations (millions)	Estimated cost £ per organisation	Total cost (£ millions)
Low	0.57	£27	£15.4
Medium	0.15	£116	£17.4
High	0.06	£214	£12.6
Total	0.78	£58	£45.4

Source: ICO analysis.

⁵⁴ For guidance on familiarisation costs, see: BEIS (2017): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776507/Business_Impact_Target_Statutory_Guidance_January_2019.pdf

⁵⁵ For a description of how these estimates were reached see [Annex A: Familiarisation costs](#).

⁵⁶ Anecdotal evidence from as yet published research undertaken for DCMS indicates that smaller organisations in particular are not engaging with the existing materials.

This estimate is only intended to indicate the scale of the impact and is based on a number of assumptions. Details on how these figures were calculated and the assumptions that informed them, as well as sensitivity analysis, are included in Annex A.

Categorisation of impact

Engaging with the toolkit is optional however it is designed to make the process of engaging in international personal data transfers simpler, so we would expect organisations to choose to familiarise themselves with it. Also, the limited alternative options are likely to be disproportionately burdensome and run a higher risk of non-compliance.

There is no specific legal obligation within DPA 2018 placed on the ICO to develop the toolkit and therefore, the costs of familiarisation should be viewed as an additional burden on controllers. However, there was a legal requirement for something to replace the older SCCs as they were non-compliant and as such the question of additionality is complicated. We have assessed this as attributable to avoid underestimating any negative impacts.

Organisations who choose to engage will incur familiarisation costs. It is not possible to accurately estimate the impacts of familiarisation, as set out above. However, based on the available evidence, this impact is assessed as negative and attributable to the toolkit.

5.1.2. Benefits

The potential benefits of the toolkit are set out below.

Reduction of data protection harms

Engagement with the toolkit leads organisations to carry out safer international personal data transfers. This in turn will lead to a reduction of the data protection harms experienced by people in the UK. Examples of the types of harms are provided in section 3.1.2. and the benefits are summarised in Table 14.

Table 14: Benefits that accrue as a result of reduction in data protection harms

Beneficiary	Benefit
Data controllers	<p>Reduced risk of prosecution for violation of the law. Our analysis suggests around 400,000 UK businesses currently are not fully aware of the necessary legal compliance to engage in international data transfers.⁵⁷</p> <p>Greater consumer confidence in controllers leading to a better reputation and more customers.</p>
Individuals	Reduction in data protection harms, including those referred to in section 3.1.2.
Society	<p>Easier enforcement of individual's data rights.</p> <p>Growth of the digital economy.</p> <p>Reduction in the costs of supporting victims of data protection harms.</p>

Categorisation of impact

It is not possible to accurately estimate impacts, however, any reduction in data protection harms will result in a net benefit to the UK economy and society. The toolkit will help controllers to reduce the risk of these harms and therefore we determine the impact to be attributable.

Business and organisational confidence in dealing with international data transfers

By producing this toolkit, the ICO is providing regulatory certainty to businesses and organisations that are engaging or could benefit from engaging in international data transfers. As a result, we expect to see greater confidence to engage in international trade and a reduction in market failures outline in section 3.1.6. Table 15 provides an overview of the benefits. For example, if the number of compliant international data transfers were to increase, this has the potential to raise the positive externalities associated with it.

⁵⁷ See section 3.1.5.

The benefits of organisations becoming familiar with the toolkit are:

- Reduced legal and advisory costs of understanding the legislation and their legal obligations;
- Increased regulatory certainty, making it easier for organisations to comply with existing legislation and streamlining decision making.

Table 15: Benefits that accrue as a result of business and organisational confidence in dealing with international data transfers

Beneficiary	Benefit
Data controllers	Increased organisational confidence to engage in international data transfers and the benefits associated with them.
	Reduction in advisory or legal costs of gaining regulatory certainty. Our analysis suggests up to 180,000 businesses do not engage in international data transfers because they are concerned with the legal risks. In enabling these business to engage with confidence, the toolkit increases the total number of business by 24%. We are unable to estimate this in monetary terms.
Individuals	Potential reduction in market prices.
	Greater numbers of individuals benefitting from goods and services delivered by the digital economy.
Society	Higher productivity due to more organisations engaging in the digital economy.
	Positive externalities associated with greater levels of competition and innovation.

Categorisation of impact

Business and organisational confidence in dealing with international data transfers will result in a net benefit to UK economy and society. It is not possible

to accurately estimate the impacts of increased confidence, however, given the scale of benefits associated with international data transfers, if the toolkit were to provide even a marginal uplift in these benefits, the impacts on the economy and society would be significant. The toolkit contributes directly to this greater confidence and therefore the impact is attributable.

5.2. Overall assessment of impacts

Table 12 above outlines the overall impacts of the toolkit. The toolkit is likely to incur significant familiarisation costs and it is not possible to even indicatively monetise any of the benefits. However, even a small improvement in organisational confidence to transfer or a small reduction in potential data protection harms is likely to significantly outweigh the estimated familiarisation costs. As such, we would expect there to be a significant benefit associated with the toolkit.

Annex A: Familiarisation costs

This annex sets out the approach taken to estimating familiarisation costs for:

- The International Data Transfer Agreement guidance⁵⁸;
- The International Data Transfer Agreement issued by the Information Commissioner for Parties making Restricted Transfers;
- The International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Information Commissioner for Parties making Restricted Transfers;
- The Transfer Risk Assessment Guidance;
- The Transfer Risk Assessment Tool; and
- The Transfer Risk Assessment worked examples⁵⁹.

A similar approach was taken for the impacts of familiarisation of the ICO's Age-Appropriate Design Code, Data Sharing Code And Draft Journalism Code.⁶⁰

In high level terms, we take all organisations in the UK, estimate what proportion transfer data internationally and then provide an indicative estimate of how likely they are to engage with the toolkit. We then estimate the cost of familiarisation with the toolkit and apply this to the organisations to arrive at a total estimate of familiarisation costs.

Organisations in scope

The organisations covered in the analysis of familiarisation costs are businesses, public sector organisations, and charities as described in Section 4.3.

The number of private and public sector organisations is estimated using BEIS Business Population Estimates.⁶¹ For charities we use data from the Charity Commission⁶², the Scottish Charity Regulator⁶³ and The Charity Commission for Northern Ireland⁶⁴. These bodies report a higher number of charities than are

⁵⁸ Our analysis is based on a working draft of the IDTA guidance, which is due for finalisation in early 2023.

⁵⁹ Similarly our inclusion of the TRA examples in our costing analysis is based on working drafts.

⁶⁰ ICO (2021): <https://ico.org.uk/media/about-the-ico/documents/4018652/draft-economic-impact-assessment-202110.pdf>; ICO (2021): <https://ico.org.uk/media/2619796/ds-code-impact-assessment-202105.pdf>; ICO (2020): https://ico.org.uk/media/about-the-ico/documents/2617988/aadc-impact-assessment-v1_3.pdf

⁶¹ BEIS (2021): <https://www.gov.uk/government/statistics/business-population-estimates-2021>

⁶² Charity Commission for England and Wales, available at: <https://register-of-charities.charitycommission.gov.uk/sector-data/sector-overview>, accessed 18th August 2022

⁶³ Scottish Charity Register, available at: <https://www.oscr.org.uk/>, accessed 18th August 2022

⁶⁴ The Charity Commission for Northern Ireland, available at: <https://www.charitycommissionni.org.uk/>, accessed 18th August 2022

reflected by the BEIS Business Population Estimates. This may mean that our analysis double counts charities that are also registered as private businesses. We therefore present our estimate for charities as an upper end estimate. In the context of the UK economy, charities account for 3% of all organisations likely to be impacted by the toolkit and as such, this simplifying assumption has a relatively small impact on the overall figures.

Private sector organisations

We estimate the number of affected private sector organisations by first considering business size and then by considering the likely extent of engagement with the toolkit.

Business Size

There are 5.6 million private sector organisations in the UK, which are broken down by size in Table 16.⁶⁵

Table 16: Businesses in UK economy according to business size⁶⁶

Number of employees	Percentage of businesses by size	Estimated number of businesses by size
None	74.7%	4,180,000
1 to 49	24.6%	1,380,000
50 to 249	0.6%	33,500
250+	0.1%	5,590
Total	100%	5,590,000

Source: [BEIS, Business Population Estimate 2021](#).

DCMS research shows the percentage of private sector organisations that transfer personal data abroad. This analysis can be used to estimate the number of businesses that are exposed to international data transfers, as per our application in Table 17.

⁶⁵ BEIS (2021): <https://www.gov.uk/government/statistics/business-population-estimates-2021>

⁶⁶ Note the ONS reports business size by number of employees and specifies four categories rather than the five specified by DCMS. Under the ONS categorisation, businesses with between 1 and 49 employees are designated as a single category.

Table 17: Private sector organisations exposed to international data transfers

Number of employees	Percentage of businesses that transfer (send or receive) data with other organisations or people based outside of the UK	Estimated number of businesses
None	14%	566,000
1 to 49	13%	181,000
50 to 249	16%	5,770
250+	41%	3,010
Total	14%	756,000

Source: [DCMS, UK Business Data Survey 2022](#); [BEIS, Business Population Estimates 2021](#); ICO analysis.

We note that this cohort of businesses may include some that transfer data only with the EU, which would be covered by adequacy. However given the data available it is not possible to identify this cohort. We therefore consider our estimates to be an upper limit.

Likely engagement with the toolkit

Our central estimate of familiarisation costs assumes that organisations with no employees are on average far less likely to need to engage with the full toolkit. We assume these businesses are more likely to transfer data internationally for business administration purposes, for example book-keeping services.⁶⁷

We make the simplifying assumption therefore that businesses without employees have a low level of engagement with the toolkit. This assumption is tested as part of sensitivity analysis.

For businesses with employees, we assume that the likelihood of making restricted transfers and the volume of personal data held is linked to sector characteristics and will determine engagement with the guidance and tools, as per Table 18.

⁶⁷ We have considered factors such as cloud-based computing systems and responsibility for transfers (controllers and processors). Given the data available, we believe these assumptions to be reasonable.

Table 18: Likelihood of engagement with the toolkit by business sector

Sector	Likelihood of engagement with the toolkit	Justification
Agriculture, Forestry and Fishing	Low	International transfers of data possible. Very unlikely to hold much personal data.
Mining and Quarrying; Utilities	Medium	International transfers of data likely. Mixed data types with utility providers expected to have lots of customer data but mining and quarrying businesses will not.
Manufacturing	Medium	International transfers of data likely. Low potential for large amounts of customer data but larger sized businesses may hold personal data in the form of employee and contractor data.
Construction	Medium	International transfers of data likely. Low potential for large amounts of customer data but larger sized businesses may hold personal data in the form of employee and contractor data.
Wholesale and Retail Trade including auto-repair	Medium	International transfers of data likely. Mixed in terms of potential for personal data. Retail organisations likely to hold customer data, wholesale organisations less likely to hold large amounts of personal data.
Transportation and Storage	Medium	International transfers of data likely. Mostly business to business so unlikely to involve much personal data.
Accommodation and Food Service Activities	Medium	International transfers of data likely. Likely to hold some personal data.

Information and Communication	High	International transfers of data highly likely. Likely to hold large amounts of personal data.
Financial and Insurance Activities	High	International transfers of data highly likely. Likely to hold large amounts of sensitive personal data.
Real Estate Activities	High	International transfers of data likely. Likely to hold large amounts of sensitive personal data.
Professional, Scientific and Technical Activities	High	Sector includes lawyers, researchers and others with high-risk data and potential for sharing internationally.
Administrative and Support Service Activities	Medium	International transfers of data likely. Mostly business to business services but potential to handle some personal data, for example on workers.
Education	High	International transfer of data likely. Likely to hold large amounts of personal data.
Human Health and Social Work Activities	High	International transfer of data likely. Potential for high levels of high-risk data including medical and children's data
Arts, Entertainment and Recreation	Medium	International transfers of data possible. Likely to hold and use large amounts of personal data.
Other Service Activities	Medium	Unknown, mid-point assumed

Source: ICO analysis. The likelihood of engagement categorisation is based on professional judgement.

Public sector organisations

BEIS estimates that there are 12,400 public sector organisations in the UK. We have assumed that, in general, public sector organisations hold and process

large amounts of personal data, including high-risk personal data and that they are likely to need to carry out restricted transfers. We have assumed that larger organisations are more likely to do so, for example a local authority outsourcing its payroll function or using software or platforms that involve making restricted transfers. This approach is broadly aligned with the approach taken in the ICO's impact assessment for the data sharing toolkit of practice.⁶⁸

We were unable to find evidence to robustly estimate the number of public sector organisations that transfer data internationally. As a suitable proxy, we have applied the same proportions by size of organisation as in the private sector from Table 17.

Table 19: Likelihood of engagement with the toolkit by public sector organisation size

Number of employees	Number of organisations	Likelihood of engagement with the toolkit
0 to 49	1,150	Medium
50 and over	1,050	High

Source: [DCMS, UK Business Data Survey 2022](#); [BEIS, Business Population Estimates 2021](#); ICO analysis.

Charities

There are 169,100 charities registered in the UK. Charities are likely to hold large amounts of personal data, most commonly for fundraising activities. We believe that charities with larger annual income are more likely to transfer personal data internationally and therefore more likely to need to engage with our guidance.

We were unable to find evidence to robustly estimate the number of charities that transfer data internationally. As a suitable proxy, we have applied the same proportions by size of organisation as in the private sector from Table 17, with the results shown in Table 20 below.

Table 20: Likelihood of engagement with the toolkit by charity size

Annual income band	Number of organisations	Likelihood of engagement with the toolkit
£0 to £5 million	23,700	Medium
£5 million +	740	High

⁶⁸ ICO (2021): [ds-toolkit-impact-assessment-202105.pdf \(ico.org.uk\)](#)

Source: [Charity Commission](#), the [Scottish Charity Regulator](#) and [The Charity Commission for Northern Ireland](#); ICO analysis.

Summary of organisations in scope

This table summarises our estimate for organisations in scope.

Table 21: Summary of organisations in scope⁶⁹

Sector	Likelihood of engagement with the toolkit		
	Low	Medium	High
Private	573,000	126,000	57,000
Public	0	1,150	1,050
Charities	0	23,700	740
Total	573,000	151,000	59,000

Source: ICO analysis.

Familiarisation costs

Drawing on the assessment of likelihood of engagement with the toolkit above, we make indicative assumptions about which documents a typical organisation would be expected to read in each of the categories. This is informed by the initial results of ongoing evaluation activity being carried out on behalf of DCMS. As such, the results should be treated with caution.

Organisations with higher likelihood of engagement are assumed to be likely to engage with the whole toolkit, whereas organisations with lower likelihood are likely to only engage with the TRA materials.

Table 22: Analysis of documents to be read by likelihood of engagement with the toolkit

Element of the Guidance	Likely engagement with the toolkit and proportion of documents to be read			Description
	Low	Medium	High	
IDTA guidance		50%	100%	Guidance on when and how to carry out an IDTA

⁶⁹ Figures do not sum as data is rounded to prevent disclosure of respondent information.

IDTA		25%	100%	Model IDTA contract
IDTA Addendum		25%	100%	Model contract clauses for an IDTA
TRA guidance	100%	100%	100%	Guidance on when and how to carry out TRAs
TRA tool	100%	100%	100%	Assessment Tool for an IDTA – explanatory notes
TRA worked example*		100%	100%	Worked example of implementation of the TRA tool

Source: ICO analysis. * For the worked examples, there are likely to be around 5 of these, however, we have made the simplifying assumption that most organisations will only engage with the one most similar to their situation.

These assumptions provide us with an indicative average of familiarisation costs. While we recognise that within these broad groups, organisations will have specific needs and therefore read more or less of this guidance, on average we believe this assumption to be reasonable. It should also be noted that this should not be taken as an instruction to organisations on what to familiarise themselves with. Organisations should make this decision based on their specific circumstances.

Table 23: Estimate of the average time taken to read toolkit documents

Element of Guidance	Word count	Fleisch reading ease score	Assumed words per minute	Estimated reading time (hr:min)
IDTA Guidance*	15,864	49.2	75	3:31
IDTA	9,338	40.5	75	2:05
IDTA Addendum	2,072	37.6	75	0:28
TRA guidance	1,631	47.1	75	0:22
TRA tool	7,635	54.3	100	1:16
TRA worked example*	1,275	31.1	75	0:17

Source: ICO analysis, [Business Impact Target guidance](#). *Our analysis is based on draft documents and is thus subject to change.

The impact of familiarisation on organisations can be monetised using data on wages from the ONS Annual Survey of Hours and Earnings.⁷⁰ Assuming that the relevant 'occupational group' is 'Managers, Directors and Senior Officials', the 2021 median hourly earnings (excluding overtime) for this group is £22.01.⁷¹

This hourly cost is uprated for non-wage costs using the latest figures from Eurostat and in line with Regulatory Policy Committee guidance,⁷² resulting in an uplift of 22% and an hourly cost of £26.84. We use the hourly cost and the simplifying assumption of one individual handling familiarisation for each organisation to establish a cost per organisation.

Summary of familiarisation costs

In summary, we believe the familiarisation cost to the economy as a whole to be around £45.4 million.

⁷⁰ See Eurostat (2022): https://ec.europa.eu/eurostat/statistics-explained/index.php/Hourly_labour_costs; and ONS (2022): <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/bulletins/annualsurveyofhoursandearnings/2022>

⁷¹ ONS (2021): [Annual Survey of Hours and Earnings time series of selected estimates - Office for National Statistics \(ons.gov.uk\)](#)

⁷² See guidance in Regulatory Policy Committee (2019): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827926/RPC_short_guidance_note_-_Implementation_costs_August_2019.pdf

Table 24: Central estimate of familiarisation costs

Likelihood of engagement with toolkit based on size/sector	Organisations (millions)	Estimated cost per organisation	Total cost (millions)
Low	0.57	£27	£15.4
Medium	0.15	£116	£17.4
High	0.06	£214	£12.6
Total	0.78	£57	£45.4

Source: ICO analysis.

Sensitivity analysis

There are uncertainties associated with the estimates used in the analysis and the figures are sensitive to the assumptions made. We therefore provide some alternative scenarios below to demonstrate this uncertainty.

Our analysis assumes that not all affected businesses and organisations would engage with all the materials in the toolkit. If we relax this assumption and rather assume that all businesses and organisations that transfer data internationally familiarise themselves with the whole toolkit then the cost to the UK economy would be around £167.5 million.

As yet unpublished research by DCMS suggests that business awareness of the requirements around international transfers is currently low among businesses that do transfer. For example, anecdotal evidence from the research suggests that smaller organisations rely on larger organisations to put in place an IDTA and carry out the appropriate checks to support a transfer. Consequently, our central estimate that assumes all relevant organisations will engage with the toolkit may be too high. To provide an indicative estimate of the implications of this, if we assumed only those that are assumed highly likely to engage with the toolkit, engaged at all, this would put the total costs at around £12.6 million.

Using the two scenarios as the upper and lower end of the range of likely costs suggest a range of £12.6 million to £167.5 million. This demonstrates the high degree of uncertainty around the central estimate used in the assessment.