MOORE ClearComm

ADVISORY NOTE 07/2022

Update to Advisory Note 02/2022 published in February 2022

International Data Transfers

26th September 2022

OVERVIEW

UK-based organisations sending personal data outside the UK or making it available to organisations in other countries need to comply with the rules on international transfers. In some cases, as this document will explain, it may be necessary to enter into a contract to provide safeguards for such transfers of personal data.

In March 2022, The Information Commissioner's Office (ICO), the UK's data protection regulator, issued standard clauses for this purpose, called the **International Data Transfer Agreement** (IDTA). They also issued a **UK Addendum** to the standard contractual clauses approved by the European Union in 2021 (2021 EU SCCs).

Prior to the UK's withdrawal from the European Union, some UK-based organisations may have signed previous versions of the EU SCCs. Any pre-2021 EU SCCs already signed will continue to be valid until **21st March 2024**.

Since March 2022, UK-based organisations have been able to use either the IDTA or the 2021 EU SCCs with the UK Addendum where such contracts are required. From **21st September 2022**, these are the only standard contractual clauses that may be used by organisations in the UK.

By **21st March 2024**, any pre-2021 EU SCCs will have to be updated to either the IDTA or the 2021 EU SCCs with the UK Addendum to comply with UK law.

WHAT IS A RESTRICTED TRANSFER?

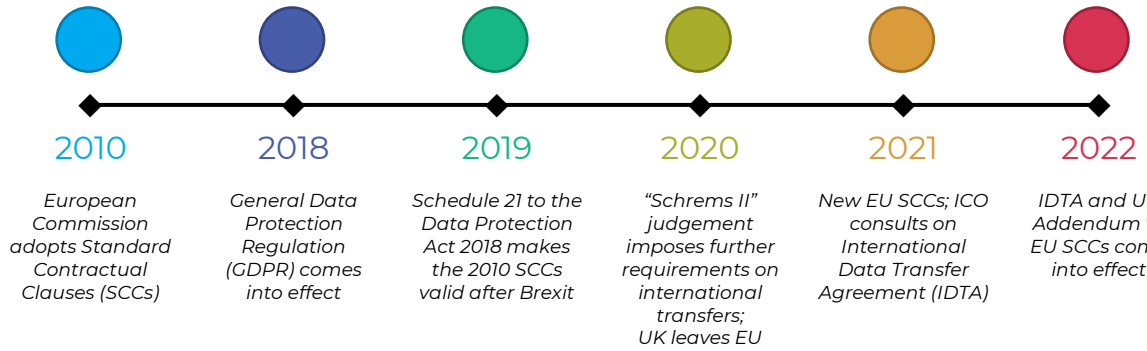
Transfers of personal data outside the UK are *restricted* by law if the organisation or its activities are subject to UK data protection law, for example if the controller is based in the UK, or they have a significant client base in the UK.

> ***Tip:*** A controller's employees, including agency workers, are not considered third parties, so if they are located outside the UK, accessing personal data would not be a 'restricted transfer'.
>
> Organisations should implement and maintain adequate technical and organisational measures to ensure the security of such data.

Similarly, if an organisation uses a third party provider located in another country to process personal data on their behalf, or shares personal data with another company outside the UK, they are making a restricted transfer.

If the UK has recognised a country, territory or international organisation as *adequate* in accordance with UK data protection law, then an organisation can transfer personal data to that country, territory or international organisation without the need to apply 'appropriate safeguards' (see Step 4 below). A list of countries specified as *adequate* by the UK is attached to this Advisory Note.

TIMELINE



CURRENT REQUIREMENTS

Step 1 – *Identify your international data transfers*

Are you transferring personal data outside the UK? Consider software-as-a-service (SaaS) providers, online/cloud storage, managed services where support staff have access to your systems.

Step 2 – Identify locations without adequacy

If you are sending or making personal data available to somewhere not subject to adequacy regulations, then you have additional requirements (see Step 3).

Step 3 – Conduct a transfer impact assessment

For each operation you have identified, you need to conduct a Transfer Impact Assessment (TIA), also known as a Transfer Risk Assessment (TRA) to consider the protections available to the personal data you are transferring and the people whose data it is.

Moore ClearComm can advise further on the format and detail required for a TIA/TRA.

Step 4 – Identify appropriate safeguards

The appropriate safeguards are:

1. A legally binding and enforceable instrument between public authorities or bodies *(e.g. an international treaty)*
2. Binding Corporate Rules *(usually between businesses in a global group).*
3. Standard contractual clauses as described in this document.
4. An approved code of conduct *(there are none currently approved)*
5. Certification under an approved scheme *(there are none currently approved)*
6. Custom contractual clauses authorised by the ICO.
7. Administrative agreements between public authorities or bodies *(such as a memorandum of understanding, when authorised by the ICO)*

Step 5 – Put it into action

Once you have documented what you have decided to do, you must ensure it is done and the measures maintained.

There are a limited number of exemptions to the requirements for appropriate safeguards, but these only apply to occasional or one-off data transfers. You can, for instance, request explicit consent from a person to transfer their personal data outside the UK, but you need to give them a lot of specific information so they can make an informed decision, and they must be able to withdraw that consent at any time, which is often impractical.

You cannot obtain valid consent for restricted transfers that will be routinely made to a country, territory or international organisation not subject to adequacy regulations. Such transfers must be conducted using the IDTA or 2021 EU SCCs with the UK Addendum to comply with UK law.

◆

CONTACT US

Call: **+44 (0) 20 7566 4000**
Email: **info@mooreclear.com**

Flag	Country	Type/Membership	Caveats	Legal Provision
	Andorra	Other	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e); Commission Decision 2010/625/EU of 19th October 2010
	Argentina	Other	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e); Commission Decision 2003/490/EC of 30th June 2003
	Austria	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Belgium	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Bulgaria	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Canada	Commonwealth	Commercial organisations only	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e); Commission Implementing Decision (EU) 2019/419 of 23rd January 2019
	Croatia	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Cyprus	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Czech Republic	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Denmark	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Estonia	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Faroe Islands	Other	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e); Commission Decision 2010/146/EU of 5th March 2010
	Finland	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	France	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Germany	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Gibraltar	British Overseas Territory	Not granted adequacy by the EC	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(b)
	Greece	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Guernsey	Crown Dependency	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e); Commission Decision 2003/821/EC of 21st November 2003
	Hungary	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Iceland	EEA (EFTA)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Ireland	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Isle of Man	Crown Dependency	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e); Commission Decision 2004/411/EC of 28th April 2004
	Israel	Other	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e);
	Italy	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Japan	Other	Commercial organisations only	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e); Commission Decision 2002/2/EC of 20th December 2000
	Jersey	Crown Dependency	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e); Commission Decision 2008/393/EC of 8th May 2008
	Latvia	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Liechtenstein	EEA (EFTA)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Lithuania	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Luxembourg	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Malta	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Netherlands	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)

Flag	Country	Type/Membership	Caveats	Legal Provision
	New Zealand	Commonwealth	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e);
	Norway	EEA (EFTA)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Poland	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Portugal	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Romania	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Slovakia	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Slovenia	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Spain	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Sweden	EEA (EU)	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(a)
	Switzerland	Other	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e); Commission Decision 2000/518/EC of 26th July 2000
	Uruguay	Other	-	Data Protection Act 2018, Schedule 21 Part 3 para. 5(1)(e); Commission Implementing Decision 2012/484/EU of 21st August 2012