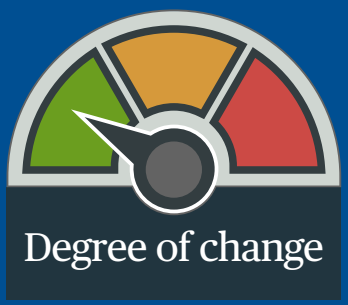
Transfers of personal data

At a glance

- Transfers of personal data to recipients in "third countries" (i.e. outside of the European Economic Area ("EEA")) continue to be regulated and restricted in certain circumstances.
- The GDPR's obligations are broadly similar to those imposed by the Data Protection Directive, with some compliance mechanism improvements available, notably the removal of the need to notify standard contract clauses to supervisory authorities, and encouragement for the development of transfer adequacy codes of practice and certification schemes.
- Data transfer compliance will remain a significant issue for multinational organisations and also for anyone using supply chains which process personal data outside the EEA.
- Breach of the GDPR's data transfer provisions is identified in the band of non-compliance issues for which the maximum level of fines can be imposed (up to 4% of worldwide annual turnover).
- Non-compliance proceedings can be brought against controllers and/or processors.



To do list

☐	Review and map key international data flows.
☐	Consider what data transfer mechanisms you have in place and whether these will continue to be appropriate.
☐	Review questions included in standard procurement templates and contract clauses to ensure that information about your supplier's proposed transfer of personal data for which you are responsible is understood and conducted in a compliant way.
☐	If you or your suppliers previously relied upon a Safe Harbor certification to ensure adequacy, this is no longer valid. This being said, you may consider seeking certification under its replacement, the Privacy Shield. In any event, you may want to re-evaluate your relationships with service providers and/or customers to establish a new legal basis that will justify on-going transatlantic data transfers.
☐	For intra group data transfers, consider whether BCRs would be a viable option.
☐	If you transfer personal data outside the EEA whilst supplying goods or services, expect to be questioned by customers about your (and your supplier's) approach to transfer compliance.
☐	Keep an eye on developments regarding approved codes of conduct and certification schemes carried out in the context of an organisation's activities.

Commentary

Transfers of personal data to "third countries" (i.e. outside of the EEA) continue to be restricted under the GDPR. This will remain a significant issue for any multinational organisation. However, the current requirements will broadly remain in place, with some improvements.

The main improvement is that the current process, whereby transfers based on standard contractual clauses have to be notified to or approved by data protection authorities, is abolished.

The Commission will have the power to determine that certain countries, territories, specified sectors or international organisations offer an adequate level of protection for data transfers. The existing list of countries which have previously been approved by the Commission will remain in force, namely: Andorra, Argentina, Canada (where PIPEDA applies), Switzerland, Faero Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand. Countries to be added to or taken off this list shall be published in the Official Journal.

The US safe harbor scheme which was previously approved by the Commission is no longer valid. However, on 12 July 2016, only 9 months after the invalidation of the Safe Harbor, the European Commission formally adopted a decision confirming the adequacy of its replacement - the EU-U.S. Privacy Shield. US organisations may self-certify to the standards set out in the Privacy Shield from 1 August 2016. The Privacy Shield provides for the European Commission to conduct periodic reviews in order to assess the level of protection provided by the Privacy Shield following the entry into force of the GDPR. The Privacy Shield is not referenced in the GDPR, although the GDPR does incorporate the key requirements assessing adequacy, as set out in the *Schrems* decision.

The GDPR provides more detail on the particular procedures and criteria that the Commission should consider when determining adequacy, stressing the need to ensure that the third country offers levels of protection that are *"essentially equivalent to that ensured within the Union"*, and providing data subjects with effective and enforceable rights and means of redress. The Commission shall consult with the EDPB when assessing levels of protection and ensure that there is on-going monitoring and review of any adequacy decisions made (at least every four years). The Commission also has the power to repeal, amend or suspend any adequacy decisions.

Other existing methods of transferring personal data continue to be recognised: Standard contractual clauses (either adopted by the Commission or adopted by a supervisory authority and approved by the Commission) will remain an option and the existing sets of approved clauses will remain in force.

The use of other appropriate safeguards, such as binding corporate rules (BCRs) and legally binding and enforceable instruments between public authorities, will also be accepted.

Significantly, transfers will be permitted where an approved code of conduct (based on the new scheme in Article 40) or an approved certification mechanism (based on the new scheme in Article 42) is used, provided that binding and enforceable commitments are made by the controller or processor in the third country to apply the appropriate safeguards, including as regards the data subjects' rights. There are also provisions for ad hoc safeguards to be agreed, subject to authorisation from the competent supervisory authority.

With respect to BCRs, the GDPR writes into law the current requirements for BCRs for controllers and processors. These will still require approval from the competent supervisory authority but this has to be determined in accordance with a consistency mechanism. This will be helpful in those few Member States which are still not able to accept BCRs.

There continue to be a number of derogations permitting transfers of personal data in limited circumstances, which are similar to existing derogations, and include: explicit consent, contractual necessity, important reasons of public interest, legal claims, vital interests, and public register data. There is also a new (limited) derogation for non-repetitive transfers involving a limited number of data subjects where the transfer is necessary for compelling legitimate interests of the controllers (which are not overridden by the interests or rights of the data subject) and where the controller has assessed (and documented) all the circumstances surrounding the data transfer and concluded there is adequacy. The controller must inform the supervisory authority and the data subjects when relying on this derogation.

Finally, as widely expected, the GDPR makes it clear that it is not lawful to transfer personal data outside the EEA in response to a legal requirement from a third country, unless the requirement is based on an international agreement or one of the other grounds for transfer applies. The UK has opted out of this provision.

Where can I find this?

Articles 40-45, Recitals 78-91