conexus law

Transfer of data between the EU, the UK and the US

From 1 January 2021 the United Kingdom will lose its automatic status as a safe destination for EU data when it falls outside of the EU's legal jurisdiction. This means that for EU data to be transferred to the UK (or any 'third country' that is not an EEA member), then one of the following conditions must be met:

- The destination territory has been granted an adequacy decision by the EU;
- One or more of the appropriate safeguards is in place:
    - A legally binding and enforceable instrument between public authorities or bodies;
    - Binding corporate rules;
    - Standard Contractual Clauses adopted by the EU Commission;
    - Standard Contractual Clauses adopted by a supervisory authority and approved by the Commission;
    - An approved code of conduct together with binding and enforceable commitments of the receiver outside of the EEA;
    - Certification under an approved certification mechanism together with binding and enforceable commitments of the receiver outside the EEA;
    - Contractual clauses authorised by a supervisory authority;
    - Administrative arrangements between public authorities or bodies which include enforceable and effective rights for the individuals whose personal data is transferred, and which have been authorised by a supervisory authority; or
- It is covered by an exception under Article 49 of the GDPR.

Adequacy decision

Because the UK effectively adopted it's very own version of the GDPR under the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (amendments etc,) (EU Exit) Regulations 2019 it was widely expected that the EU Commission would give the UK an adequacy decision, thus enabling the ongoing flow of personal data to and from Europe. Indeed, the UK government even went as far as to say that it would be granting an equivalent Adequacy decision to the EEA member states.

Unfortunately this is not a certainty, and has been put in further doubt by a ruling of the European Court of Justice on 6 October in which they ruled that the collection of bulk communications data from telecoms and internet companies was a "particularly serious" interference of privacy rights under European law. The UK argued that such actions fell into the 'national security' exemptions, but the court found that this was not the case. The UK legislation fell foul because of the "general and indiscriminate transmission of traffic data and location data" was considered too wide to meet the exemption.

On this basis, it would seem unlikely that an adequacy decision could be granted to a country where government surveillance powers are in breach of EU law, although the court did suggest that such data retention could potentially be permissible if it was subject to review by a court or independent body and was only used where they face "a serious threat to national security that proves to be genuine and present or foreseeable". The court also suggested that targeted retention of data may be permissible under the national security exemption.

Time is running out for an adequacy decision to be made, and it is likely to involve changes to the UK's investigatory legislation to restrict such wide access to the data. Whilst the UK has shown it's hand by announcing that transfers to the EEA will be covered by an adequacy decision from the Home Secretary, the EU is remaining tight-lipped and this could become another political bargaining chip in the UK's withdrawal from the EU.

Binding Corporate Rules

Binding Corporate Rules are an internal code of conduct entered into by a multinational group (whether a corporate group or a group of undertakings engaged in a joint economic activity – such as franchises or joint ventures) which must be approved by a supervisory authority in an EEA country where one of the companies is based. These rules will need to be updated to cover the fact that the UK will become a 'third country' under the GDPR.

To use Binding Corporate Rules, you must also carry out (and document) your own assessment as to whether they ensure compliance with the level of protection essentially equivalent to that guaranteed within the EU by the GDPR, taking into account the circumstances of the transfers and any supplementary protective measures that you put in place. If it is impossible to ensure compliance, then such personal data transfers are prohibited.

We are still waiting on guidance from the European Data Protection Board on what sort of supplementary measures can be introduced in addition to the Binding Corporate Rules (and equally the Standard Contractual Clauses) and these are expected to be a mixture of legal, technical and operational measures.

Given the 6 October judgement, we can see that the UK's legislation around data retention and disclosure and national security agencies makes it very likely that such compliance is impossible if the data can be disclosed to law enforcement and security agencies in such a general and indiscriminate manner, and no supplementary measures would prevent the UK legislation from impinging on the data subjects' rights.

If you don't already have Binding Corporate Rules in place, then it is unlikely that you would be able to get a new set approved before the 31 December 2020 deadline.

Given the 6 October judgement, it appears that using Binding Corporate Rules is just as restricted as using an adequacy decision – and they will either both be resolved (in which case the adequacy decision will be of more use to most businesses as a lawful basis for transferring data) or neither will be effective.

conexus law

Standard Contractual Clauses

The EU Commission has adopted a set of Standard Contractual Clauses (often referred to as 'Model Clauses') which are entered into by a data exporter and the data importer and contain contractual obligations on the parties, and rights for data subjects which can be directly enforced.

There are four sets of standard clauses that have been adopted (two sets for controller to controller transfers, and two sets for controller to processor) and they must be entered into in their entirety and without amendment. Additional clauses can be added on business related issues provided they do not contradict the standard clauses.

Unfortunately the Standard Contractual Clauses are in need of an update, as they all pre-date the adoption of the GDPR by some time, and they also do not contain any provision for the transfer of data by a data processor to a sub-processor. Needless to say, these updates and guidance have been sought (and promised) since the GDPR was enacted, but we are still waiting.

A supervisory authority is able to adopt their own set of standard clauses (which must then be approved by the EU Commission) but as yet, no supervisory authority has done so.

Similar to using the Binding Corporate Rules, it is not enough to simply adopt the Standard Contractual Clauses though. You must also carry out an assessment taking into account the circumstances of the transfers and any supplementary measures that you put in place to ensure that UK law does not impinge on the adequate level of protection provided by the Standard Contractual Clauses. These supplementary measures would include encryption and other pseudonymisation, but care must be taken to ensure that the keys to such other pseudonymisation are not available to the relevant authorities by virtue of their being held on the same systems.

The Standard Contractual Clauses are the most common method of transferring personal data from the EU to third countries where no adequacy decision has been made, despite the fact that they are far from perfect. It is hoped that the proposed revised clauses and guidance (including processor to sub-processor versions) will rectify this, but we have been waiting on these since the GDPR was first enacted in 2016 and so it seems unlikely that they will be provided prior to 31 December.

As with the other exemptions, the 6 October ruling appears to rule out the efficacy of the Standard Contractual Clauses, as any assessment of data subject rights will fail due to the illegality of the UK surveillance legislation under EU law unless sufficient supplementary measures are put in place to protect the personal data. This will mean that care must be taken to ensure that the personal data is not in itself accessible by way of secure encryption, or by pseudonymising the data at source, with no ability for that to be undone within the UK – which is highly unlikely if the data is to be actively processed (rather than just held) within the UK.

Approved Code of Conduct

As yet, there are no approved codes of conduct for data transfers.

Approved Certification Mechanism

As yet, there are no approved certification mechanisms.

Section 49 Exceptions

- **Explicit consent**

  In theory, valid consent could be given for a restricted transfer, but for the consent to be specific and informed, the data subject would need quite a lot of detail about the transfer, including the potential risks, and a general consent would not be enough.

  Given the level of detail required to grant specific and informed consent, allied to the fact that consent can be withdrawn at any time, it is hard to see that consent is a practical basis for such transfers where they occur on a wholesale basis. There may be scope for using consent where the transfer and processing is limited but this should be used as an exception of last resort.

- **Transfers necessary for the performance of a contract between the data subject and the controller**

  This exception is explicitly only for occasional restricted transfers which are objectively necessary for the purpose of the contract or to enter into the contract. It will not cover regular transfers such as the use of a cloud-based IT system.

  This exception is aimed to help businesses remain compliant where such transfers are the exception. The ICO gives the example of a bespoke travel agent sending names of guests, room requirements and length of stay to a hotel in Peru, but states that the exception would fail if the agent regularly sends its guests to that hotel in which case alternative safeguards should be used.

- **Transfers necessary for the performance of a contract benefitting the individual whose data is being transferred**

  Whilst similar to the above exception, this exception does not cover the pre-contract steps.

  To use the ICO's example above, this would cover the transfer of the customer's family members' details to the hotel.

- **Necessary transfers for important reasons of public interest**

  There must be an EU law which states or implies that this type of transfer is allowed for important reasons of public interest (for example an international agreement or convention). It only applies to specific, and not systematic, transfers.

  The EPB has stated that the essential requirement for the applicability of this exception is the finding of an important public interest and not the nature of the organisation, and therefore the use of this exception should be restricted to specific situations and meet the necessity test.

- **Legal claims**

  This exception applies to occasional transfers where there is a close connection between the need for the transfer and the relevant legal claim (whether establishing if you have a legal claim or making or defending a legal claim).

  The claim must have a basis in law but is not just judicial or administrative procedures and so can be interpreted widely to cover regulatory investigations or approval processes. It cannot be used if there is only the possibility of a claim.

- **Protection of vital interests of an individual**

  In a medical emergency the imminent risk of serious harm to an individual outweighs any data protection concerns. This exception cannot be relied on where the individual is physically and legally capable of giving consent.

- **Transfers from a public register**

  This covers transfers from registers created under EU law which are open to the public in general, or to any person who can demonstrate a legitimate interest in access. It does not cover registers run by private companies such as credit reference databases. The whole of the register cannot be transferred, nor whole categories of data.

- **Compelling legitimate interests**

  The final exception is aimed at cases where no other safeguards or exceptions apply and there are compelling legitimate interests which outweigh the rights and freedoms of the individuals.

  Needless to say, to use this exception you need to appropriately assess and document the circumstances surrounding the transfer and put in place appropriate safeguards where possible. The individuals should be notified of the transfer and the compelling legitimate interests explained. It is also recommended that the relevant supervisory authority is informed of the transfer.

As you can see, it is doubtful at the moment that any transfer from the EU to the UK will be compliant with the GDPR – and similarly no transfers to the US would be compliant following the Max Schrems II case in July 2020 which rendered Privacy Shield invalid. This clearly poses a huge threat to international business and it is hard to see that it will be allowed to continue, although equally the contrasting views of Europe and the US as to data protection mean it is a difficult one to see resolved without wholesale legislative changes to either the European or US regimes. The UK is clearly more aligned with the rest of Europe, and so one would hope that the differences can be resolved swiftly and effectively but given the political implications of Brexit across Europe there remains a distinct lack of clarity.

On the other hand, whilst the UK has adopted its own version of the GDPR it will be able to depart from the EU Commission in aspects such as adequacy decisions and so we may find that it becomes easier to transfer UK data than it is to transfer EU data under the GDPR. The dual-system will mean that it is more important than ever to ensure that you understand which rules apply to the data sets that you hold, and for effective management of any international transfers of data.

conexus law

What should we be doing now?

Map international transfers

- Both intra-group and external international transfers should be mapped out so that we can understand:
- Where and how was the personal data collected?
- Where is personal data being transferred?
- What mechanisms are currently being relied on for those transfers?
- Are the transfers strictly necessary? (can the data be stored elsewhere?)

Implement alternative transfer mechanisms

- As both UK and US adequacy findings seem unlikely, consider the alternative safeguarding mechanisms. Whilst the two EUCJ decisions mean that technically any data transfer assessment may fail, the options are limited if transfers are to continue.

Carry out data transfer assessments

- Carry out assessments as to whether the protections are safeguarded and record them in appropriate registers.
- These assessments need to be kept under continuous review, especially once more guidance becomes available.

Consider Article 49 derogations

- These are unlikely to be a viable long-term solution but may apply in exceptional cases.

Supplementary measures

- Whilst we are waiting for guidance from regulators as to what these could entail, enhanced encryption and pseudonymisation etc. is unlikely to be detrimental.

Contractual protection

- Look to augment the SCCs with additional protection. Whilst we are waiting for updated SCCs, we've been waiting for 4 years and so this should not delay their adoption.

Whilst a lot is up in the air, given the lack of guidance it seems unlikely that any regulator (whether in the EU or the UK) will look to penalise organisations who have undertaken appropriate reviews and adopted the SCCs, supplemented where possible with additional safeguards such as encryption. Of course, this doesn't help in itself if the data is to be actively processed (rather than just stored) in a third country as the encryption will not be permanent. Clearly this may be subject to change as additional guidance or legislation is produced, but for now this appears to be the best that any organisation can do to continue to transfer personal data between the UK, the EU and the US.

conexus law

HOW CAN CONEXUS LAW HELP?

Businesses and individuals will need legal advice to help them understand the risks they may face and the options that may be open to them.

We are available to assist in reviewing the laws in many jurisdictions across the world, and to review specific contracts. We are also available to provide practical, business-orientated advice on how to best protect yourself from the ongoing commercial effects of Covid-19.

Contact

For further advice on GDPR or pursing your contractual rights, please contact Philip Brown.

T: +44 (0)20 7390 0289

M: +44 (0)7887 538308

E: philip@conexuslaw.com