PAUL | TICHER

Data Protection after Brexit
November 2020

Although the UK has formally left the European Union, it has been in a transitional period during which much of the previous arrangements continued to apply. This comes to an end at 11.00pm on 31st December 2020. Among the things that will change are some aspects of data protection. This paper sets out what will (and what won't) change.

Legal framework

The UK has had the General Data Protection Regulation (GDPR) since May 2018 because it is an EU regulation, which came into force while the UK was a member of the EU. We are now becoming quite familiar with GDPR, and it appears to be working well.

From 1st January 2021 GDPR will no longer apply in the UK but, in preparation for leaving the EU, the UK passed the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. The main effect of this is to replace GDPR with a 'UK GDPR'. This essentially keeps GDPR as it is, but removes references to EU institutions and EU legislation.

For many organisations, therefore, there will be little or no practical difference – at least initially.

Changes could, however, emerge at some point. For one thing, the UK will lose its influence with the EU, as the Information Commissioner will no longer have voting rights in the European Data Protection Board, and we will no longer have to follow their decisions (though we might choose to, of course).

The ICO will remain our Data Protection Authority, but will not participate in the EU's cooperation and consistency mechanism. Legal decisions about the interpretation of GDPR in the UK will rest entirely with the UK courts, not the European Court of Justice.

Over time, the UK could therefore drift away from the EU in how GDPR is applied in practice.

There are even suggestions that the UK government might deliberately water down our data protection regime in the process of negotiating trade deals – with the USA, for example.

Transferring personal data between the UK and other countries

The biggest impact of the UK breaking away from the EU will be on international transfers.

In many organisations the only significant international transfer (if any) takes place because personal data is stored outside the UK in connection with a cloud-based service or application.

In some organisations personal data may be transferred to and from the UK in the course of services that are provided from the UK to individuals outside the UK, or in the context of collaborative working between UK organisations and those abroad.

Adequacy

Under GDPR, transfers of personal data within the European Economic Area (the EU plus Norway, Iceland and Liechtenstein) are not restricted (as long as the processing meets all the rest of the GDPR requirements, of course).

Transfers are also unrestricted where an 'adequacy' decision has been made by the country from which the data is transferred.

An adequacy decision means that the recipient country has been judged to have a data protection regime that is sufficient to maintain the same level of protection to personal data as in the sending country.

The EU has made full adequacy decisions for Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

In addition, adequacy decisions have been made for Canada (in respect of transfers to commercial organisations only) and Japan (for transfers to non-governmental organisations only.)

The UK has adopted all the adequacy decisions made by the EU so far, with the addition of Gibraltar, and including all the EEA countries.

However, the EU has not made an adequacy decision in respect of the UK. Consideration of adequacy decisions normally takes a long time, so there is not necessarily anything sinister in this. Since the UK GDPR is so closely based on the EU GDPR there is no obvious reason why a favourable adequacy decision will not eventually be made. In the meantime, however, transfers *from* the UK *to* the EU are unrestricted, but transfers in the opposite direction are problematic.

The USA

Transfers of personal data to the USA are even more problematic, thanks to a decision by the European Union Court of Justice (ECJ) on 16th July 2020, where paragraph 201 says, in full: "In the light of all of the foregoing considerations, it is to be concluded that the Privacy Shield Decision is invalid."

Privacy Shield was the mechanism put in place to protect personal data transfers to the USA after the Safe Harbour scheme was ruled by the ECJ as insufficient, but this decision means that Privacy Shield does not give adequate protection to the transfer of personal data to the USA, contrary to a previous decision of the court.

In addition to ruling Privacy Shield invalid, the ECJ decided that the alternative, Standard Contractual Clauses – discussed in more detail below, are also unsuitable for transfers to the USA, because they cannot prevent unwarranted access to personal data by the US government.

Standard Contractual Clauses

Where no adequacy decision exists, GDPR envisages that the usual way of protecting personal data that is transferred abroad should be through Standard Contractual Clauses (SCC) as part of the agreement between the sender and recipient of the data. There is an equivalent – Binding Corporate Rules (BCR) – for use where the transfer is between two parts of the same organisation.

A template contract using SCC can be found here on the ICO website.

Note, however, that on 12th November the European Commission opened a four-week consultation on draft revised SCCs largely in response to the ECJ ruling on the USA.

Other options

In the absence of an adequacy decision and where SCC or BCR is not possible and/or appropriate, GDPR provides a range of alternative options for international transfers. These are, briefly:

- with the data subject's informed consent;
- where necessary for the performance of a contract between the data subject and the controller;
- where necessary for the conclusion or performance of a contract in the interest of the data subject;
- where necessary for important reasons of public interest;
- where necessary in connection with legal claims;
- where necessary to protect the vital interests of the data subject or others, where the subject is incapable of giving consent;
- for a transfer from a public register.

And if none of those situations applies, you are able to make transfers which:

- are not repetitive;
- concern only a limited number of data subjects; [and]
- are necessary [in the controller's] compelling legitimate interests, which are not overridden by the interests, rights and freedoms of the data subject.

Scenario 1: Cloud provider

Your organisation is very likely to have some or all of its personal data hosted or backed up overseas; or perhaps you use online resources to collect and manage personal data or to process it in other ways (not forgetting that photographs can also be personal data) – and these services may be located wholly or partly abroad.

So what obstacles might you face, come January 2021?

If your supplier is based in the EU:

- data transfer from the UK should pose no problem.
- data transfer from the EU back to the UK, however, should be based on SCC unless and until the UK gets an adequacy decision from the EU.

If your supplier is based in an overseas location with an adequacy decision:

- data transfer from the UK should pose no problem.
- data transfer back to the UK would depend on their rules – SCC might be required.

If your supplier is based in an overseas location without an adequacy decision:

- data transfer from the UK must use SCC.
- data transfer back to the UK would depend on their rules – SCC might be required.

Obviously, there are very few cloud providers whose business model allows them to negotiate separate contracts with each user of their services.

If you need to consider SCC, therefore, your best option is where the provider has already responded to the situation and incorporated SCC into their standard terms and conditions.

Let's for the moment ignore the fact that the current SCC have been deemed ineffective regarding transfers to the USA. The consequences are still unclear.

Scenario 2: data subjects abroad

Where you are dealing with individuals abroad the key issue is not the nationality or location of the individuals but of their data.

In cases where the data has been sent to you by the individual themselves – for example if someone in Europe signs up to a newsletter – there are unlikely to be any significant implications.

If the data has been obtained by an organisation abroad, however – for example if you are working collaboratively – you might need to sign up to standard contractual clauses. For situations where that is not appropriate, you would need to think things through.

If the data originates in the EU:

- data transfer from the EU to the UK would need to fall under one of the 'other options' set out above
- data transfer from the UK back to the EU should pose no problem

If the data originates from a location abroad with an adequacy decision:

- data transfer to the UK might need to meet one of the 'other options' set out above, depending on the local rules
- data transfer back from the UK should pose no problem

If the data originates from a location abroad without an adequacy decision:

- data transfer to the UK depends on the local rules
- data transfer back from the UK would need to meet one of the 'other options' set out above

Working within the EU

If you have a branch or part of your organisation that is based within the EU they will have to comply with GDPR in the country where they are based, under that country's regulator.

If you have an operation that offers goods or services to people within the EU but no base of your own, you will need to have a 'representative' within one of the EU countries in which your data subjects are located.

For more detailed information on this, you may want to check out this guidance from the ICO.

What to do next

The most obvious first step for most voluntary organisations is to make sure you know where each of your cloud providers hold the personal data that they process on your behalf.

Many organisations have in the past aimed to avoid data protection complications by specifying that their data should be stored within the EU. You may now have the option of moving it to the UK, if you feel that is the best solution.

Alternatively, if you are happy for the data to remain in the EU, you would need to explore how far the provider has got in incorporating SCCs into their standard contract.

Data that is held in the USA, however, presents a much trickier problem. You would have to decide how seriously you are concerned about the decision that Privacy Shield is no good, and about the risk that even under SCCs the US government has potential access to the personal data you manage.

If your normal operations involve *regular* transfers between the UK and other countries you should review these to ensure that you are clear about the basis on which they take place.

You should probably also have a procedure for checking that that you have an acceptable basis for occasional transfers that you may want to make.

And finally, all organisations need to review their privacy notices. Remember that information about overseas transfers must be included as part of your obligation to be transparent. Previously you may have reassured people that you make no transfers outside the EU, for example, but now you would have to explain any transfers to other EU countries

And then what happens?

Chris Pounder, a well-known commentator on data protection of many years' experience, has written a rather depressing blog, setting out all the steps the UK government has taken to make it possible for our data protection provisions to be watered down, and the areas in which they might drift away from the EU approach (or even already have done).

I'm an independent specialist, with over 30 years' experience of Data Protection in the voluntary sector. However, I'm not a lawyer. This paper may not be a complete or accurate statement of the law, and it is not intended to be legal advice.

If you have any questions on this paper, please do contact me: on 0116 273 8191 or paul@paulticher.com