GDPR Blog Chapter 9: International Transfers of Data – *updated for the Data Protection Act 2018*

Welcome to Chapter 9. Time is getting short. May – the month, not the politician - is almost upon us. As every diligent reader of Bar Talk will now know, May is the month in which the new European-authored General Data Protection Regulation (GDPR) comes into force. It will be accompanied by a new Data Protection Act in the UK. The latter is still under Parliamentary scrutiny, and as we have previously explained, we have concentrated on briefing you on the "knowns" in GDPR rather than the "unknowns" in the new Data Protection Act. A summary of the latter will follow when it emerges from the Parliamentary process and becomes Law ***which of course, it now has, as the DPA 2018 and we have inserted into the text of the blogs, references to the updated DPA 2018.***

We have broken down the new Regulation into a number of theatrical scenes, dubbed Chapters. This seemed to us to be an appropriate metaphor for the Bar. So far, the scenes are as follows: an Introduction (the Programme) *[here]*,Chapter 1, (the Players) *[here]*, Chapter 2 (Roles of Principal Members of the Cast – the Data Controller) *[here]*; Chapter 3 (A Continuation of the Data Controller's role) *[here]*; Chapter 4 (Further data protection principles with which the Data Controller has to comply) *[here]*, and Chapter 5 (Roles of Principal Members of the Cast – the Data Subject) *[here]*; Chapter 6 (Roles of the principal members of the Cast – the Data Processor *[here]*, and Chapter 7 (The Melodrama Part 1 -What happens when it all goes wrong) [here]; Chapter 8 (the Melodrama Part 2 – How much could it cost you to get it wrong) *[here]*.

Please do read these. They are a relatively light-hearted look at the world of Data Protection. They are very important given the tighter emphasis on this area in the GDPR.

In this Chapter, we concentrate on transferring "**personal data**" to recipients abroad – Under the Data Protection Act 1998 this is where the 8th data protection Principle, which we have previously mentioned is relevant, with which you (currently) have to comply – ***up to 25 May 2018***.

You might think this is easy; press of a button on the computer to a number of recipients including those in countries outside the EU. However, this may not be such a great idea. Many countries do not operate to the standards of the European Union when it comes to safeguarding their citizens' privacy.

But, remember, it is "personal data" i.e. information about a living individual, about which there is a concern. Anything else is outside the scope of GDPR.

That said, don't forget that all your clients' information must be protected from disclosure and that just because your client is a company, that doesn't mean that you are not dealing with personal data, e.g. information about staff and/or witnesses.

Transfers of "personal data" to "third countries" or "international organisations" is governed by GDPR Chapter V, starting at Art. 44. Incidentally, if you were wondering what an "international organisation" is, Article 4(26) defines this as *"an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between one or more countries"*. We will use "third country" to cover both expressions.

We will now talk you through the GDPR provisions.

What is the remit of this Chapter of the Regulation?

It applies to:

- Personal data which undergoing processing (and remember, "processing" has a very wide ambit and includes storage)
- Personal data intended to be processed after transfer to a third country
- Personal data which is likely to be further transferred from one third country to another third country
- Both Data Processors and Data Controllers (N.B. this is different to the current Act).

A third country can mean a territory (or one or more specified sectors) within that third country.

It does NOT apply to data in transit (as opposed to "transfer") via non-EU countries. This example demonstrates the difference:

> an email is sent from country A to country B routed via country C. There is no access to or manipulation of the information while it is in country C. Any storage of the message in country C is transitory. This is a transfer to country B from country A but only a transit through country C.

Essentially, you have to comply with Chapter V in its entirety before you can transfer personal data to third countries. One immediate practical consequence is that you cannot just have anyone, anywhere, acting as your "cloud" for data storage, unless you are satisfied with the risk posed to the data.

Who decides whether a third country has adequate levels of protection for the receipt and processing of data?

The European Commission decides this on the basis of a number of criteria. These criteria are in Article 45.2. They include:

- The rule of law (respect for human rights and freedoms, appropriate data protection regimes, security and defence and criminal law, rules for onward transmission of data etc – there is a list of criteria in Art.45(2)(a) but it is still the EU Commission that makes the decision, taking into account all the relevant criteria in this sub-article)
- The existence of an effective equivalent of the ICO, with adequate enforcement powers
- Each third country's international commitments that it has previously undertaken with respect to data protection.

If the European Commission is happy after assessing the adequacy of data protection measures in any specific country (or territory within that country, or specified sectors within that third country), it will issue an "implementing act" to give effect to this under Art.45.3.

The Commission is required to monitor and review data protection in third countries and may withdraw approval if the data protection conditions are no longer adequate. It is also mandated to consult with that third country with a view to remedying the position. **So, watch out for changes to a third country's existing approved status, particularly in view of the tighter regime to be implemented by GDPR.**

So, how do I know if the EU Commission believe a country has adequate data protection measures?

A number of countries have been assessed under the existing provisions and found to have adequate protections. These are called adequacy decisions. You may have heard of this term, as it is being discussed as what the UK will require after Brexit is implemented.

For those who study the *Official Journal of the European Union* with their morning cornflakes, approved countries are listed in this, as are changes to a previous status, and those who are seeking adequacy decisions. If you don't eat breakfast and/or read the *Journal*, the information is on this page of the EU Commission website;

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

What happens if the Commission has <u>not</u> made a decision that a particular third country has adequate data protection provisions?

You CAN transfer personal data to a third country if no such decision has been made AND without the specific approval of the ICO, **BUT**

- You have to provide appropriate safeguards for the Data Subject, ***of the kind set out in Art.46.2 and 46.3***
- There have to be enforceable Data Subject rights and legal remedies for Data Subjects.

How do I recognise the above?

We will not mention those aspects that might be said to be irrelevant for the Bar and chambers. However, if you are advising a client, or you have a chambers annex in a non-EU country, you will need to look at Art. 46. So, relevant appropriate safeguards might be:

- A legally binding and enforceable instrument between public authorities or bodies

- Standard data protection clauses issued by the ICO and approved by the Commission – available under the Act but not yet drafted for the GDPR

- Standard data protection clauses issued by the EU Commission itself (also not yet drafted for the GDPR)

- Approved codes of conduct together with binding and enforceable commitments of the Data Controller or Data Processor in the third country to apply the appropriate safeguards (none are as yet planned for the legal sector)

- Approved certification mechanism (with the same commitment as immediately above) – still not developed.

At the risk of stating the obvious, you don't need ICO approval for the above. However, you could use alternative methods provided these have been approved by the ICO. These are:

- Contractual clauses (i.e. between UK Data Controller/Data Processor and 3rd Country Data Controller/Data Processor/recipient)
- Provisions in administrative arrangements between public authorities or bodies (which include enforceable Data Subject rights)

- Pre-existing ICO authorisations (based on the existing legislation) until these are amended, replaced or repealed.

Where do we stand with the USA?

This falls under the last bullet point above. The EU-USA now operate what is known as the Privacy Shield (and used to be known as Safe Harbor) for US companies which sign up. You can transfer data provided that the US receiving entity adheres to certain conditions.

The EU-US Privacy Shield decision was adopted on 12 July 2016 and the Privacy Shield framework became operational on 1 August 2016. This framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States for commercial purposes. The framework also brings legal clarity for businesses relying on transatlantic data transfers.

The new arrangement includes

- strong data protection obligations on companies receiving personal data from the EU
- safeguards on US government access to data
- effective protection and redress for individuals
- an annual joint review by EU and US to monitor the correct application of the arrangement.

The first annual review took place in September 2017 and, on that basis, the Commission published on 18 October 2017 a report on the functioning of the Privacy Shield.

For those who wish to delve into this a little more, see https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

In summary, it is currently being re-assessed as the US has failed to meet a number of the conditions required by the EU. In other words, it is currently authorised, but may suffer the same fate as the Safe Harbor provisions which were struck down as inadequate by the CJEU.

Ultimately it is up to you. You may take the view, depending on the nature of the data involved, that it is not worth the risk to your clients and your business, to rely solely on the Privacy Shield adequacy decision.

So, can I store my data in a US based cloud system?

To comply with GDPR you need to look to see whether the company concerned is one of the 2,400 or so registered under the Privacy Shield. But you also need to be aware that the USA is one of a number of countries which may take enforcement measures to obtain access to data stored in the cloud (without informing you). If you are storing data in the "special categories" – as we have previously defined this technical term - or data which includes allegations of criminal activity and convictions, consider using a non-US company which uses servers located outside the USA, or a company which provides zero knowledge encryption of data stored in the cloud.

Other alternatives?

In the event that

(a) There is no adequacy decision from the EU (Art 45(3)) OR
(b) Appropriate safeguards ***of the kinds specified in*** Art. 46

you can <u>still</u> transfer data if one of the following conditions in Art. 49 is met.

- The Data Subject has explicitly agreed to this AND been told of the potential risks
- The data transfer is required to perform a contract between Data Subject and Data Controller (or for the implementation of pre-contractual measures)
- The transfer is between a Data Controller and a third party and is required in the Data Subject's interest for the conclusion or performance of a contract to which he is party
- The transfer is for important reasons of public interest
- **The transfer is necessary to establish, exercise or defend legal claims**
- The transfer is necessary to protect the vital interests of the Data Subject (or others) and the Data Subject is physically or legally incapable of giving consent
- The transfer is from an open public register (this does not mean the entirety of the register or entire categories of personal data contained in it)

There is one final provision in Art.49. If you cannot transfer data on the basis of the Arts.45 or 46 and none of the conditions above can be satisfied you can still transfer data to a third country, if the following cumulative conditions can be satisfied:

- The transfer is not repetitive
- The number of Data Subjects is limited
- It is necessary for the Data Controller's "compelling legitimate interests" and these are not overridden by the interests or rights and freedoms of the Data Subject

- The Data Controller has assessed all of the circumstances surrounding the transfer and has provided suitable safeguards for the protection of personal data
- The Data Controller has told the ICO of the proposed transfer
- The Data Controller has told the Data Subject of the transfer and what the "compelling legitimate interests" actually are, as well as providing all the information required by Arts. 13 and 14 [this was discussed in Chapter 3 here].
- The assessments and the safeguards employed for the transfer must all be documented.

And if I ignore all of the above….

……..you are on risk for a big fine; the €20 M category. See Article 85(5)(c). Best not to do it…..

So what does the DPA 2018 have to say about all of this? Precious little as it turns out at this point in time. DPA 2018 s.18 allows the Government to make regulations

- ***for the purposes of GDPR Art. 49(1)(d) – the transfer of data for important reasons of public interest – the circumstances in which such a transfer is necessary***
- ***to restrict the transfer of data to a third country where there is no adequacy decision as contemplated above under GDPR Art.45(3).***

Otherwise, what we have said above is still relevant.

For the ICO's guidance on international transfers see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/.

Bar Council IT Panel