CROSS-BORDER TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS – THE GATEWAYS EXPLAINED

PART II

Authors:
Gloria Ophar-George
CEO & Founder
WESTFIELD & HERENT

Michael Adamberry, Associate
ISOLAS LLP

Introduction

This article is the second of a two-part series.

In the first part, the authors discussed a "no deal" Brexit scenario where Gibraltar would become a third country for GDPR purposes and offered recommended steps in mitigation of this.

This second part explores the gateways under which personal data may be validly transferred to and from third countries,

Third country transfers under the GDPR

Art. 44 of the GDPR provides a general principle applicable to all third country transfers as follows:

"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of [GDPR], the conditions laid down in [Chapter V] are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. "

Our previous article summarised what we refer to as the 'gateways' under which third country transfers (also referred to as "*restricted transfers*") are allowed as follows:

1. Transfer is to a third country that is deemed "adequate" by the European Union.
2. Transfer is subject to "appropriate safeguards" under Art. 46 GDPR.
3. Transfer is an "exempted transfer" under the specific derogations in the first sub-paragraph of Article 49(1) GDPR.
4. Transfer is an "exempted transfer" under the specific derogations in the second sub-paragraph of Article 49(1) GDPR.

What's excluded?

It is important to note that GDPR only covers *personal data*, so if you are sending non-personal data anywhere, these restrictions do not apply.

Similarly, GDPR doesn't *always* apply. In general, the GDPR applies if you are processing personal data in the EEA (i.e. you are established there), and may apply in specific circumstances if you are outside the EEA and processing personal data about individuals in the EEA (offering goods to them or monitoring their behaviour). You should always seek suitable professional advice when in doubt as to whether GDPR applies.

Finally, it should also be borne in mind that

restricted transfers cover transfers to different corporate entities across borders, but that any transfers to employees/consultants within the same entity are not subject to restriction (otherwise, how could we send emails or share files whilst abroad?)

Gateways

Adequacy decision

A transfer may take place where an adequacy decision have been granted by the EC, ensuring adequate data protection is in place to facilitate such transfer but more importantly protects the personal data of those data subjects in question whose data it is that is being transferred.

To ascertain whether a country inside or outside the EEA or EU has been granted an adequacy decision, a copy of such list of countries is available and can be downloaded from the Official Journal of the EU published on the EC website[1]. Our previous article listed the countries and territories that had received an adequacy decision at the time of writing.

Appropriate safeguards

There are numerous appropriate safeguards listed in Art. 46(2) GDPR. Given that legally binding instruments between public authorities or bodies will not apply to most data controllers, and that approved codes of conduct and certification mechanisms are still in early stages of development in most cases, the most pertinent appropriate safeguards are binding corporate rules (BCRs) and the standard contractual clauses (SCCs).

Standard Contractual Clauses (SCCs)

There are currently three sets of SCCs (sometimes referred to as the 'model clauses'). 4 sets of SCCs have been approved, but only 3 of these can be used after 2010. The EC plans to update the SCCs for GDPR but at the moment organisations can use:

- Controller-Controller '2001' model clauses contained Commission Decision of 15 June 2001;
- Controller-Controller '2004' model clauses contained Commission Decision of 27 December 2004; and
- Controller-Processor '2010' model clauses contained Commission Decision of February 2010.

It is important to bear in mind that you are restricted from making any amendment to the SCCs and must use them in their entirety; you can however add any additional business-related clauses that may be required (or use an addendum in addition to the SCC). When doing the later, you may wish to seek appropriate professional advice to ensure that any additional things added do not compromise the validity of the SCCs as an appropriate safeguard. If your organisation is receiving personal data from the EEA, then consider the use of SCCs and put these in place.

Binding Corporate Rules (BCRs)

What are they?

BCR are internal rules adopted by multi-national corporate groups and companies which define their global policy with regard to the international transfers of personal data within the same corporate

[1] Official Journal of the EU

group to entities located in countries which do not provide an adequate level of protection.

What is their purpose?
Established under pre-GDPR European legislation, BCRs have historically been used by multi-national companies in order to adduce appropriate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals.

BCR are designed to allow multi-national companies to transfer personal data from the EEA to their affiliates located outside of the EEA.

To that extent, BCRs ensure that all transfers made within a group benefit from an adequate level of protection. This is an *alternative* to the company having to sign SCCs each time it needs to transfer data to a new member of its group and may be preferable where it becomes too onerous to sign SCCs to cover each respective data flow made within a group (to the extent third countries are involved).

Once approved under the EU cooperation procedure, BCRs provide a sufficient level of protection to companies to get authorisation of transfers by national data protection supervisory authorities. It should be noted that the BCRs do not provide a basis for transfers made outside the group.

How do I get authorisation for my BCRs?
An applicant must demonstrate that their BCRs put in place appropriate safeguards for protecting personal data throughout the organisation in line with the requirements of the *Article 29 Working Party papers on Binding Corporate Rules.*

The procedure is designed to avoid organisations having to approach each individual supervisory authority separately.

Your business or organisation needs to choose a supervisory authority to be a lead authority. Your choice of lead authority depends on the location of the EU headquarters of your business or the location within Europe of that part of your business best placed to take responsibility for global data protection compliance.

If the lead authority is satisfied as to the adequacy of the safeguards put in place in your BCRs, that authority's decision is binding across the other supervisory authorities in Europe (with the caveat that other member states may have additional requirements to consider).

Derogations for specific situations

GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain *specific situations*. These are sub-divided into the first two sub-paragraphs of Art. 49(1) GDPR. They are not to be confused with appropriate safeguards. In fact, they are properly understood as exempted transfers, as they allow restricted transfers to happen where there are no appropriate safeguards in place (e.g. no SCCs have been entered into).

There are conditions on when a derogation / exemption might apply. The first sub-paragraph of Art 49 (1) lists seven distinct situations, two of which we summarise immediately below as they are usually most relevant:

- the transfer is made with the data

subject's *explicit consent* (i.e. after having been informed of the risks);
- the transfer is necessary for the *performance of a contract* between the data subject and the controller or for pre-contractual steps taken at the data subject's request.

When relying on these, it is highly recommended that decisions are well *documented* so that the controller/processor can show evidence as to its rationale in applying the derogation.

The second sub-paragraph of Art 49 (1) provides a final *'last resort'* exemption; it states that where there is no adequacy decision applicable, and no appropriate safeguards, and none of the seven derogations in Art 49 (1)(a) to (g) apply, then a restricted transfer may still take place, but only if *all* the below conditions are fulfilled:

- transfer is *not repetitive*
- concerns only a *limited number* of data subjects
- is *necessary for the purposes of compelling legitimate interests*
- controller has *assessed* all the circumstances and provided suitable safeguards
- controller *informs the supervisory authority* of the transfer.
- Controller *provides Art. 13/14 GDPR info* (i.e. Privacy Notices/Policies)
- controller (or processor) *documents the assessment* as well as the suitable safeguards referred to above in accordance with Art. 30 GDPR (i.e. Data Mapping)

Other gateways

Can I rely on an exemption under the Data Protection Act 2004 (DPA)?

Member States can introduce exemptions from GDPR's transparency obligations and individual rights, but only where the restriction "respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" to safeguard and for reasons of national or public security; defence; the prevention, investigation, detection or prosecution of criminal offences and otherwise[2].

Due regard must also be given to whether any of the exemptions under the DPA apply to and can be relied upon by your business or organisation in exceptional "one off" transfers.

In the normal scheme of things appropriate steps should be taken to protect personal data, rather than place reliance on any exemption. Any transfer must also comply with the other seven data protection principles of Art. 5 GDPR.

EU-US Privacy Shield (applies to transfers to the USA only)

The Privacy Shield Framework was deemed adequate by the European Commission. Participating organisations are deemed to provide "adequate" privacy protection, Compliance requirements of the Privacy Shield Framework are clearly laid out and can be implemented by small and medium-sized enterprises.

[2] See GDPR Arts 6, 9, 23, 85-91.

If you are transferring personal data to an organisation in the USA, provided this organisation is a member of the Safe Harbour Scheme (SHS) (now EU-US Privacy Shield which superseded SHS)[3], then such transfer will be in compliance with GDPR.

The list of Privacy Shield organisations can be found on the US Department of Commerce website[4]. The relevant URL must be included in an organisation's privacy policy to meet the Framework requirement[5].

Conclusion

- Compliance with privacy laws and data protection regulation is complex and multi-layered and will continue to present challenges for a number of businesses or organisations.

- Businesses must continue to be compliant with their data protection responsibilities and obligations. The DPA and GDPR requirements will remain. Therefore, continue to apply standards of GDPR and be guided by current GRA guidance. The guidance issued by the UK's Information Commissioner's Office (ICO) is also extremely useful.

- Personal data may be transferred with very limited restrictions to countries that have been deemed to provide an adequate level of protection for personal data by the EC or countries within the EEA. Conversely, you should always ensure a relevant gateway applies for *restricted transfers* to *third countries.* It would also be advisable to document why a gateway is deemed applicable in case this is ever questioned by a relevant supervisory authority.

- Appointing an EU Representative if you are based in Gibraltar, and not in any other EU/EEA state, but offer goods/services to or monitor behaviour of individuals in the EEA, please bear in mind that, for the organisations who have appointed a data protection officer (DPO), this is separate from your DPO obligations. This means that your Representative cannot be your DPO or one of your processors.

- The good news is that, if you are a public authority there is no requirement to appoint a Representative, or if you undertake the occasional processing, low-risk and no special category or criminal offence data on a large scale is involved.

- Where your organisation or business uses certain service providers, it may use appropriate safeguards such as SCCs or BCRs. You can create your own contractual clauses, but an assessment will need to be made and for practical purposes it is far more

[3] Withdrawal from Safe Harbor requires recertification from Privacy Shield.

[4] (see http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list)

[5] https://www.privacyshield.gov

straightforward to use the SCCs and supplement these further by adding them to an agreement as an addendum.

- Consider any derogations made by Gibraltar laws (e.g. DPA) which could be used to guarantee the protection of the personal data to be transferred, and that matters outside of GDPR scope (e.g. national security, defence) would fall under a different (albeit similar) regime.

- Where your business uses providers, who are based in the United States of America (USA), you may transfer data to them if they form part of the Privacy-Shield.

About the authors:

Gloria Ophar-George
CEO & Founder
WESTFIELD & HERENT,

Gloria LLB is CEO & Founder of WESTFIELD & HERENT, a Gibraltar-based specialist data protection compliance service, helping local businesses understand and comply with complex Data Protection Laws and their privacy obligations. She commands a unique combination of training and experience as a GDPR expert delivering training and providing in-house consultancy for various international organisations in risk, corporate governance and data protection. During her recent tenure at IT Governance Ltd, she was the trainer of choice for the House of Commons as well as numerous organisations in the private and public sectors. She is a Certified EU GDPR Practitioner (2017), and has worked at executive level, advising at board and senior management level.

Michael Adamberry
Associate
ISOLAS LLP

Michael is an Associate at ISOLAS LLP, and specialises in Data Protection & Privacy Law, offering advice to a wide range of clients ranging from sole traders and SMEs, to large multi-national corporates, public authorities, financial institutions, and insurance companies. He is a Certified EU GDPR Practitioner (2018) and has significant experience in advising on implementation and compliance with GDPR.