BREXIT NO DEAL: IMPLICATIONS FOR GIBRALTAR BUSINESSES DOING CROSS-BORDER TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

PART I

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

Michael Adamberry
Associate
ISOLAS LLP

Introduction

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

In the first part, the authors discuss the general GDPR regime regarding international data transfers and the added complexity surrounding 'third country' data transfers, exploring preparatory steps organisations can take to mitigate against a 'no deal' Brexit that could result in Gibraltar and UK instantly becoming third countries for the purposes of the pan-European (GDPR) privacy regime.

The second part shall explore the gateways under which personal data may be validly transferred to and from third countries.

GDPR and international transfers (overview)

Given the growth of a rapidly ever-evolving international market it has become increasingly part of business requirements for organisations to transfer data internationally. However, where these transfers involve *personal* data it is necessary to ensure that the data is adequately protected and the transfer complies with the requirements of the Data Protection Act 2004 (DPA) as well as the General Data Protection Regulation (GDPR); in particular, Chapter V of the GDPR and the data protection principles in Art. 5 GDPR.

GDPR applies a much stricter regime where personal data are transferred to 'third countries' and international organisations (i.e. countries and international organisations outside of the European Economic Area (EEA)). However, it also provides various 'gateways' to allow transfers of this nature, which for convenience we shall refer to as 'third country transfers'. Conversely, transfers within the EEA are not subject to such stringent requirements or what the law refers to as 'appropriate safeguards'.

Consequently, data controllers may only transfer personal data to third countries by using one of the gateways, which we have summarised 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 Art. 49(1) GDPR.
4. Transfer is an 'exempted transfer' under the specific derogations in the second sub-paragraph of Art. 49(1) GDPR.

Whenever there is a need for third country transfers, it is imperative that organisations ensure a similar degree of protection is afforded to protect the rights and freedoms of data subjects as regards the processing of personal data.

Transfers on the basis of an 'adequacy decision' under the first gateway are least problematic, as additional steps do not need to be taken by the data controller in order to introduce appropriate safeguards. The current list of *adequate* countries or territories can be downloaded from the website of the European Commission (EC), and at the time of writing includes Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework).

Brexit No Deal – What does this mean for Gibraltar businesses?

As most will be aware, Gibraltar benefits from the UK's current membership of the EU, and therefore is not currently considered a 'third country' for GDPR purposes. As a result, transfers to/from the UK and/or Gibraltar do not currently require any of the gateways mentioned above, and it is notable that the UK and Gibraltar have neither required nor obtained an 'adequacy ruling' for this reason.

The logical question follows: "will the UK (and by extension, Gibraltar) become a third country for GDPR purposes on Brexit?"

On a 'no deal' Brexit, the answer is undoubtedly a resounding "Yes!"

For this reason, there are growing concerns among businesses; and quite rightly so.

Presently, organisations or businesses that process personal data (as *controllers* or *processors*) need to comply with Gibraltar's data protection regime, which is contained in the DPA. Our DPA is substantially similar to the UK's Data Protection Act 2018 (UK DPA), which was drafted in anticipation of Brexit. Accordingly, amendments were made to the DPA in Gibraltar on 25 May 2018 in order to ensure that it remains *'fit for purpose'* following Brexit and also takes account of the special relationship between the UK and Gibraltar. This means we do not expect a significant amount of changes to our DPA post-Brexit.

(Spoiler alert! After Brexit, a future article will explore how the DPA works in conjunction with GDPR, and the four regimes contained therein in further detail)

Given the DPA and the UK DPA incorporate the GDPR, one would expect the EU will be able to consider Gibraltar and the UK as having an adequate level of data protection rights in their legislative regimes, ensuring the fundamental rights and freedoms of natural persons are guaranteed. In other words, the DPA aims to meet the EU's 'GDPR standard' (and go even further if need be).

A further practical question asks: ***"how long will the EU take to make that (formal) decision on adequacy?"*** and the answer is that on a 'no deal' Brexit it might be **"too long"**.

Her Majesty's Government of Gibraltar (HMGoG) is working to include further mechanisms and changes as may be required in law for the uninterrupted transfer of personal data between Gibraltar and the UK; accordingly, such transfers should remain unaffected, regardless of a no deal Brexit.

However, on a no deal Brexit and in the absence of an adequacy decision (which involves a formal process made at EC level and is not expected to be a decision made overnight), transfers (i) from Gibraltar to the EEA; and (ii) received from the EEA to Gibraltar, will still require the receiving EEA entity to demonstrate there are appropriate safeguards in place, which could lead to Gibraltar businesses having to agree to GDPR audits and/or being asked to confirm their compliance status.

Okay…there's a potential problem – what's the solution?

Should the UK leave the EU without a deal there are measures which your business or organisation can take and put in place to ensure data protection compliance.

Being prepared is key, and the best preparation is to ensure that your organisation or business is at present, effectively complying with the GDPR (and the DPA) which will continue to apply post-Brexit. The reason for this is not only that GDPR is directly applicable in Gibraltar, but also that EEA-based international businesses will not be able to transfer personal data to a Gibraltar business or organisation (in the absence of an adequacy decision) unless it demonstrates effective GDPR compliance.

Due consideration must also be given to the requirement to appoint a representative in the EEA, if you are a data controller or processor which is not established in the EU (i.e. a Gibraltar international business with head office in Gibraltar or the UK in a post-Brexit context, and no EEA offices). It should be ascertained whether it is apparent that your business or organisation envisages offering services to or monitoring behaviour of data subjects in one or more Member States in the Union[1].

What actions need to be taken by businesses?

Whilst we await an adequacy ruling for the UK (which it is hoped will include Gibraltar), or a 'deal' scenario where the UK negotiates this, we are left with the other appropriate safeguards, and the exempt transfer scenarios. We do not propose to deal with all of these in this article, but feel it is important to highlight Binding Corporate Rules (BCRs), and the approved EU standard contractual clauses (SCCs).

Given the complexity and timescales involved with BCRs, which require formal approval by a supervisory authority, SCCs are the more commonly adopted mechanism to ensure

[1] Art. 27 and Recital 23 GDPR

efficient transfers. But the SCCs are not *one-size-fits-all* and nor do they arrive with all the blanks filled in. The SCCs require fact-specific business decisions as well as considering the practicalities of how international transfers will operate.

The next article in this series will cover BCRs and SCCs in more detail, as well as the other gateways that allow third country transfers.

SCCs aside, your organisation or business needs to have a plan to implement appropriate safeguards. A two-phased approach is suggested below which focuses on preliminary steps to take, before shifting focus to how the organisation exports and imports personal data to/from Gibraltar.

Phase 1 – Implementing your compliance plan

(1) Think about what GDPR safeguards your organisation can put in place to ensure continuance of data flows, following departure from the EU.[2]

(2). Review existing contracts that are in place and/or amend as appropriate in line with any data sharing initiatives (e.g. data processing and/or sharing agreements.

(3). Review your privacy notices and other privacy information (data subjects have a right to know where their data is being transferred) and identify details that will need updating once we leave the EU.

(4). Review your internal documentation and appropriate policy documents, including data protection impact assessments for transfer between Gibraltar and the EEA and Risk Registers (if these are in place) to identify any details which will need to be updated when Gibraltar leaves the EU.

(4). Review lawful basis on which processing activities are being done and start to map internal and external data flows within your organisation if you have not already done so.

(5) Raise organisational awareness about these key issues and the importance of GDPR compliance in your businesses – i.e. obtain '*management buy-in*' and train staff accordingly. Keep abreast of guidance and latest information from the Gibraltar Regulatory Authority (GRA).

Phase 2 – Review your international transfers and implement appropriate safeguards.

(1). Discussions need to be held with any pan European partners if you operate across Europe (e.g. have offices, branches or other establishments in the EEA). Assuming this to be the case, then EU regime will apply to these European processing activities even after we leave the EU.

(2). The EU regime may equally apply where you offer goods or services to individuals in the EEA or monitor the behaviour of individuals in the EEA, if you are only based in Gibraltar for instance.

(3). You may need to appoint a representative in the EEA to act on your behalf if your

[2] ICO, March 2019 'Leaving the EU – six steps to take'.

organisation does not have a presence in any other EEA or EU member state. Apart from data protection officer (DPO) obligations of your organisation or business, your representative cannot be your DPO or one of your processors. If your organisation is a public authority, processing is occasional, low-risk and does not consist of special category or criminal offence data on a large scale, there is no need to appoint a representative[3].

(4). Review your data flows, structures and processing operations to assess (a) whether you will continue to have a Lead Supervisory Authority (LSA)[4] and take advantage of the one-stop-shop; (b) if you no longer have a LSA how you could be at a disadvantage from the one-stop-shop which could significantly impact on your businesses in addition to the resources you may require in dealing with EU data protection authorities enquiries and (c) how Brexit will affect the data protection regimes that apply to your business or organisation as you may have to deal with both the GRA and EU supervisory authorities in each EEA or EU member state where the processing of personal data relative to those activities has effect on the fundamental rights and freedoms of individuals[5].

(5). In view of transfers to Gibraltar, undertake a review of your data flows to identify where (locations) you receive data into Gibraltar from the EEA. If your business or organisation is in receipt of data from organisations in the EEA, the organisation transferring that data to your business will need to comply with the transfer provisions of the EU regime and may ask you to enter into the SCC to ensure that there are sufficient safeguards in place or that one of the exceptions of GDPR applies.

(6) Equally, a review is required where you transfer data from Gibraltar to any country outside of Gibraltar, as these will undoubtedly fall under new transfer and documentation provisions of Gibraltar. In particular, establish whether the country to which the personal data is being transferred to is within a third country, is within the EEA, or is otherwise deemed adequate.

(7) If your organisation forms part of a multi-national group and there are existing BCRs already in place (quite rare at the moment) that cover EEA and Gibraltar group companies, you may rely on these for transfers from the EEA to Gibraltar (showing relevant changes to Gibraltar as a third country).

For additional information on the current requirements on transfers outside of Gibraltar, refer to guidance issued by the GRA[6] or ICO on international transfers.

[3] For further guidance on appointing a representative, see EDPB 'Guidelines on Territorial Scope'.

[4] GRA 'Guidance on GDPR: (2) Lead Supervisory Authority'(Guidance Note IR02/17 of 24 May 2017). See also Article 29 Working Party, 'Guidelines for identifying a controller or processor's lead supervisory authority' (5 April 2017).

[5] See European Data Protection Board (EDPB) guidelines for identifying your lead supervisory authority.

[6] See GRA 'Guidance on GDPR: (10) 'Getting ready for a "no deal" Brexit' (Guidance Note IR05/18 of 20 December 2018); GRA 'Guidance on GDPR: (11) 'International Transfers' (Guidance Note IR11/18 of 13 March 2019)

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 is a Certified EU GDPR Practitioner (2017) and 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, 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.