GRA

GIBRALTAR REGULATORY AUTHORITY

(11) International Transfers

Guidance on the General Data Protection Regulation

13th March 2019

Guidance Note IR11/18

CONTENTS

SUMMARY

The General Data Protection Regulation (the "GDPR") primarily applies to data controllers and processors located in the European Economic Area (the "EEA"), with some exceptions. Individuals risk losing the protection of the GDPR if their personal data is transferred outside of the EEA. On that basis, the GDPR restricts transfers of personal data outside the EEA, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies. This Guidance Note aims to assist organisations identify the most appropriate mechanism available under Article 45 or 46 of the GDPR to make a restricted transfer.

Article 45 of the GDPR

- Transfers on the basis of an Adequacy Decision

Article 46 of the GDPR

- Standard data protection clauses adopted by the European Commission
- Standard data protection clauses adopted by a supervisory authority and approved by the European Commission.
- Binding corporate rules
- Approved codes of conduct
- Approved certification mechanisms
- A legally binding and enforceable instrument between public authorities or bodies
- Administrative arrangements between public authorities or bodies that include enforceable and effective rights for the individuals, which have been authorised by a supervisory authority

Article 49 of the GDPR Derogations (exceptions)

- The data subject has given explicit consent to the restricted transfer.
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- The restricted transfer is being made from a public register.
- It is a one-off restricted transfer and it is in your compelling legitimate interests pursued by the controller.

1. INTRODUCTION

Flows of personal data to and from the European Union (the "EU") are necessary for international trade and international co-operation. However, if personal data is transferred from the EU to data controllers and processors located outside the EU in third countries, a third country being any country outside the European Economic Area (the "EEA"), individuals risk losing the protection of the General Data Protection Regulation ("GDPR"). For this reason, the GDPR 'restricts' transfers of personal data outside the EEA, unless certain provisions in Chapter V of the GDPR are met. It is important to note that in a "no-deal" Brexit scenario, Gibraltar will no longer be a member of the EU. Instead, it will become a third country, outside of the EEA. Therefore, under the GDPR, transfers of personal data to Gibraltar will also be 'restricted'.

The purpose of this document is to provide summary guidance on the provisions in Chapter V of the GDPR regarding transfers of personal data to third countries or international organisations. The guidance is useful to a data controller in Gibraltar, as a territory within the EU, to understand its obligations when transferring data outside of the EEA. In the event of a "no-deal" Brexit, this guidance will also be useful to a data controller or processor in Gibraltar as it identifies the mechanisms that may be used to maintain ongoing data flows from the EU/EEA, for example by using '**standard contractual clauses**'. However, for further guidance on preparing for a "no-deal" Brexit please refer to Guidance Note IR05/18[1].

Please note that the European Data Protection Board (the "EDPB") is currently working on its guidance regarding 'international transfers'. Therefore, the Information Commissioner[2] (the "Commissioner") will update this document as and when the guidance is published.

Acknowledgements

Where appropriate Gibraltar's Information Commissioner will seek to ensure that locally published guidance notes are consistent with others made available by fellow Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the guidance from the European Data Protection Board, the UK's Information Commissioner's office and the Irish Data Protection Commissioner's office.

[1] See Guidance Note IR05/18 Guidance on the General Data Protection Regulation: (10) Getting ready for a "no-deal" Brexit <https://www.gra.gi/gdpr-10-getting-ready-for-brexit> Accessed 15 February 2019.

[2] The Chief Executive Officer of the Gibraltar Regulatory Authority.

2. ARTICLE 45 OF THE GDPR: TRANSFERS ON THE BASIS OF AN ADEQUACY DECISION

The first thing to consider when transferring personal data to a third country is if there is an 'adequacy decision'. An adequacy decision means that the European Commission has decided that a third country or an international organisation (outside the EEA) ensures an adequate level of data protection.

When assessing the adequacy of the level of protection, the European Commission takes into account elements such as the laws, respect for human rights and freedoms, national security, data protection rules, the existence of a data protection authority and binding commitments entered into by the country in respect of data protection.

The effect of such an adequacy decision is that personal data can flow from the EEA to that third country, without restriction.

It is important to note that adequacy decisions made prior to the GDPR remain in force, unless there is a further European Commission decision which decides otherwise. The European Commission plans to review these decisions at least once every four years.

All European Commission adequacy decisions to date also cover restricted transfers made from EEA states.

An up to date list of the countries which have an adequacy finding can be viewed on the European Commission's data protection website[3]. These should be checked regularly for any changes.

IN THE EVENT OF BREXIT

In regard to data transfers to Gibraltar from the EEA –

1. Her Majesty's Government of Gibraltar ("HMGoG") has made clear its intention to seek adequacy decisions for Gibraltar to ensure the ongoing free flow of data to Gibraltar. However, at exit date adequacy decisions regarding Gibraltar may have not been finalised;
2. Organisations should therefore plan to implement appropriate safeguards (see section 3).

In regard to data transfers from Gibraltar –

1. HMGoG has confirmed that, when Brexit takes place, transfers to the EEA and the UK from Gibraltar will not be restricted. This means you will able to continue to send personal data from Gibraltar to the EEA and the UK without any additional requirements.

[3] See EU Commission, 'Adequacy decisions' <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en> Accessed 15 February 2019.

2. Rules on transfers to countries other than the UK or EEA countries are likely to remain similar. The Commissioner expects HMGoG to confirm that Gibraltar will reflect existing European Commission adequacy decisions.

3. ARTICLE 46 OF THE GDPR: TRANSFERS SUBJECT TO APPROPRIATE SAFEGUARDS

In the absence of an adequacy decision, the GDPR does allow a restricted transfer if the data controller or processor has provided 'appropriate safeguards'. The safeguards may include:

Standard data protection clauses adopted by the European Commission

For the majority of organisations, the most relevant alternative legal basis to an adequacy decision would be these clauses. They are model data protection clauses that have been approved by the European Commission and enable the free flow of personal data when embedded in a contract. The clauses contain contractual obligations on the organisation sending the personal data (the "Data Exporter") and the organisation receiving the personal data (the "Data Importer"), and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the Data Exporter and the Data Importer. These are known as the '**standard contractual clauses**' ("SCCs").

The SCCs published by the European Commission are the following:
- 2001 controller to controller
- 2004 controller to controller
- 2010 controller to processor

The Commissioner has produced template contracts, which include explanatory notes and guidance:

- controller to controller transfers
- controller to processor transfers

For most businesses, a convenient and appropriate safeguard would be to use SCCs.

It is important to note that the European Commission has advised the EDPB that it plans to update the existing SCCs for the GDPR. Until then, EU-based data controllers can still enter into contracts that include the standard contractual clauses based on the EU Directive 95/46/EC, which pre-dated the GDPR.

Please check the Commissioner's and the European Commission websites regularly for any updates.

IN THE EVENT OF BREXIT
In regard to the transfer of personal data to Gibraltar from the EEA –
1. in the absence of an Adequacy Decision for Gibraltar, data controllers in the EEA could use the SCCs to maintain the flow of data to Gibraltar.

In regard to the transfer of personal data from Gibraltar –
1. SCCs can continue to be used for transfers to countries other than the UK or EEA jurisdictions.
2. SCCs are not required for transfers to the EEA or the UK.

Standard data protection clauses adopted by a supervisory authority and approved by the European Commission

Personal data may also be transferred to a third country if organisations enter into a contract incorporating standard data protection clauses adopted by the Commissioner. However, neither the Commissioner nor any other EEA supervisory authority has yet adopted any standard data protection clauses. They are likely to be similar to those adopted by the European Commission (above), but will be first adopted by the supervisory authority and then approved by the European Commission.

Please check the Commissioner's website as more details about using this option will be added in due course.

Binding corporate rules

Binding Corporate Rules ("BCRs") form a legally binding internal code of conduct operating within a multinational group, which applies to transfers of personal data from the group's EEA entities to the group's non-EEA entities. This group may be a corporate group or a group of undertakings engaged in a joint economic activity, such as franchises or joint ventures. BCRs are legally binding data protection rules with enforceable data subject rights contained in them, which are approved by the competent supervisory authority.

There are two types of BCRs that can be approved:

- BCRs for controllers - used by the group entity to transfer data that they have responsibility for, such as employee or supplier data. These can be found on the European Commission's data protection website[4].
- BCRs for processors - used by entities acting as processors for other controllers and are normally added as an addendum to the Service Level Agreement or Processor contract. These can be found on the European Commission's data protection website[5].

[4] See EU Commission, 'Working Document on Binding Corporate Rules for Controllers' <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109> Accessed 15 February 2019.

[5] See EU Commission, 'Working Document on Binding Corporate Rules for Processors' <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110> Accessed 15 February 2019.

Further provisions on the use of BCRs as an appropriate safeguard for personal data transfers are set out in Article 47 of the GDPR.

Approved codes of conduct

The use of codes of conduct ("Codes") as a transfer tool, under specific circumstances, was introduced in Article 46.2(e) of the GDPR. Codes are voluntary and set out specific data protection rules for categories of controllers and processors. They can be a useful and effective accountability tool, providing a detailed description of what is the most appropriate, legal and ethical behaviour within a sector. From a data protection viewpoint, Codes can operate as a rulebook for controllers and processors who design and implement GDPR-compliant data processing activities that give operational meaning to the principles of data protection set out in European and national law.

Therefore, personal data may be transferred to a third country if the Data Importer (data receiver) has signed up to a Code, which has been approved by a supervisory authority. The Code must include appropriate safeguards to protect the rights of individuals whose personal data has been transferred, and which can be directly enforced.

It is important to note that approved codes of conduct are not yet in use and the EDPB is planning to issue separate specific guidance relating to this, at a later date. Please check the Commissioner's website as more details about using this option will be added in due course.

Approved certification mechanisms

As introduced in Article 46.2(f) of the GDPR, certification mechanisms may be developed to demonstrate the existence of appropriate safeguards provided by controllers and processors in third countries. These controllers and processors would also make binding and enforceable commitments to apply the safeguards including provisions for data subject rights. Therefore, personal data may be transferred to a third country if the Data Importer (data receiver) has a certification, under a scheme approved by a supervisory authority.

It is important to note that approved certification schemes are not yet in use and the EDPB is also planning to issue separate specific guidance relating to this, at a later date. Please check the Commissioner's website as more details about using this option will be added in due course.

A legally binding and enforceable instrument between public authorities or bodies

An organisation can make a restricted transfer if it is a public authority or body and is transferring to another public authority or body, and with both public authorities having signed a contract or another instrument that is legally binding and enforceable (Article 46 (2)(a) of the GDPR). This contract or instrument must include enforceable rights and effective remedies for individuals whose personal data is transferred. However, this mechanism is not an appropriate safeguard if either the transferring/sending organisation (Data Exporter) or the receiving organisation (Data Importer) is a private body or an individual.

Administrative arrangements between public authorities or bodies that include enforceable and effective rights for the individuals, which have been authorised by a supervisory authority

If a public authority or body does not have the power to enter into legally binding and enforceable arrangements (as noted above), it may consider an administrative arrangement ("Administrative Arrangement") that includes enforceable and effective individual rights, to make a restricted transfer (Article 46(3)(b) of the GDPR). However, this is not an appropriate safeguard for restricted transfers between a public and private body.

Further, the administrative arrangement must be individually authorised by the supervisory authority in the country (or countries) from which the transfer is being made. If the restricted transfer is to be made from Gibraltar, the Commissioner must approve it.

It is important to note that Administrative Arrangements are not yet in use and the EDPB is currently working on updated guidance in relation to this transfer mechanism. Please check the Commissioner's website as more details about using this option will be added in due course.

4. ARTICLE 49: DEROGATIONS FOR SPECIFIC SITUATIONS

Derogations under Article 49 of the GDPR are exemptions from the general principle that personal data may only be transferred to a third country if an adequate level of protection is provided for in that third country. A Data Exporter (data sender) should first endeavour to frame transfers with one of the mechanisms guaranteeing adequate safeguards listed in the foregoing, and only in their absence use the derogations provided in Article 49(1) of the GDPR. The following derogations or exceptions allow restricted transfers in specific situations:

a) If there is a medical emergency and the data is needed to give medical care, or risk serious harm to the individual, and the individual is (physically or legally) unable to give his or her consent, then an organisation can rely on an exemption to make the restricted transfer (Article 49(1)(f) of the GDPR).

b) The other exceptions are very limited in scope and broadly cover –
   - the individual's explicit consent;
   - an occasional transfer to perform a contract with an individual;
   - an occasional transfer for important reasons of public interest;
   - an occasional transfer to establish, make or defend legal claims;
   - transfers from public registers; or
   - a truly exceptional transfer for a compelling legitimate interest.

It is important to note that the EDPB guidance document[6] on these derogations should always be consulted to ensure that they can be relied upon for the specific scenarios that organisations are dealing with.

[6] See EU Commission, 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679' <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en> Accessed 15 February 2019.

IMPORTANT NOTE

This document does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the GDPR and the Data Protection Act 2004 ("DPA") will apply directly to them. The responsibility to become familiar with the GDPR and the DPA and comply with its provisions lies with the organisation.

Where necessary, the Commissioner will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR and the DPA, the GDPR and DPA will take precedence.

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi