GRA

GIBRALTAR REGULATORY AUTHORITY

(10) Getting ready for a "no-deal" Brexit

Guidance on the General Data Protection Regulation

20th December 2018

Guidance Note IR05/18

CONTENTS

1. INTRODUCTION

This document provides guidance for organisations to prepare for a "no-deal" Brexit.

In the event of a no-deal Brexit, the General Data Protection Regulation ("GDPR")[1] will be absorbed into Gibraltar law, so there won't be any substantive changes to data protection in Gibraltar.

However, the uninterrupted free flow of data between Gibraltar and the European Economic Area (the "EEA") may be affected. This is because the GDPR provides for the free flow of personal data within the EEA but imposes conditions on transfers outside the EEA. In the event of Brexit without a deal, transfers to Gibraltar would need to comply with said conditions. Although developments are ongoing, it is recommended that organisations prepare for a "no deal" scenario and contingency plans are implemented to ensure the continued flow of data across borders.

Her Majesty's Government of Gibraltar ("HMGoG") is planning to include mechanisms in law for the uninterrupted transfer of personal data between Gibraltar and the UK, so these data flows should not be affected. HMGoG is also looking to implement mechanisms in law that will allow the uninterrupted flow of data from Gibraltar to the EEA, and so these data transfers will not affected. However, organisations that receive data from the EEA would need to meet the GDPR conditions.

This guidance note provides advice on "international transfers", "six key steps that organisations should take", and "advice on the use of standard contractual clauses" (likely to be a popular mechanism to protect the ongoing transfer of data to and from Gibraltar).

[1] Regulation (EU) 2016/679

2. OVERVIEW

This guidance is relevant to you if you are an organisation based in Gibraltar, which -

- operates in the EEA (which includes the EU); or
- sends personal data outside Gibraltar; or
- receives personal data from the EEA.

Firstly, it is important to note that the GDPR is an EU regulation with "direct effect". This means that it became law in all member states of the EU (including Gibraltar), without the need for Gibraltar to introduce new legislation. It also applies to the EEA states.

When the UK and Gibraltar exit the EU, the EU GDPR will no longer be law in Gibraltar. HMGoG intends to write the GDPR into Gibraltar law, with the necessary changes to tailor its provisions for Gibraltar (the "Gibraltar GDPR").

Similar to the EU GDPR's territorial scope, HMGoG intends that the Gibraltar GDPR will also apply to controllers and processors based outside Gibraltar, where their processing activities relate to:

- offering goods or services to individuals in Gibraltar; or
- monitoring the behaviour of individuals taking place in Gibraltar.

3. INTERNATIONAL TRANSFERS UNDER THE GDPR

This section is of particular importance if:

- you are a Gibraltar-based business or organisation; and
- you send personal data outside Gibraltar; or
- you receive personal data from the EEA; or
- you receive personal data from countries or territories which are covered by an adequacy decision.

This section does <u>not</u> apply to you if:

- you never transfer personal data outside Gibraltar and never receive personal data from outside Gibraltar; or
- you only transfer personal data outside Gibraltar to consumers or only receive personal data from outside Gibraltar directly from consumers.

Examples

A hairdressers in Gibraltar has a client database which it uses for bookings and marketing. It stores this database on its office computer. It has never sent any of its client data outside of Gibraltar and has no intention of doing so. The hairdressers does not need to consider this section on international transfers.

A hotel in Gibraltar takes direct bookings from individuals across Europe, which includes their names, addresses and other personal information. It receives personal data from those individuals and sends personal data back to them. Neither transfer is restricted under the GDPR nor the Gibraltar GDPR, as it is made directly with a consumer. The hotel does not need to consider this section on international transfers.

However, if either business uses a cloud IT service which stores and/or processes their data (including personal data) anywhere outside Gibraltar, (including in the EEA), it should review this section on international transfers.

The GDPR provides rules setting out when and how a transfer of personal data outside the EEA may take place.

If you transfer personal data outside the EEA now, you should already have in place arrangements for making a restricted transfer under the GDPR.

On exit date there will be two sets of rules to consider:

- first, if you are making a restricted transfer outwards from Gibraltar; and
- second, if you are receiving personal data from outside Gibraltar (including from the EEA) into Gibraltar.

You can make a restricted transfer if it is covered by an adequacy decision[2], an appropriate safeguard[3] or an exception[4].

The European Data Protection Board (EDPB) is currently working on its guidance regarding International Transfers, and we will update our guidance as this is published.

What are the key points if we are making transfers from Gibraltar?

You are making a restricted transfer outwards from Gibraltar if:

- the Gibraltar GDPR applies to the processing of the personal data you are transferring;
- the Gibraltar GDPR does not apply to the importer of the data, usually because they are located outside Gibraltar (which may be in the EU, the EEA or elsewhere); and
- you, the sender of the personal data, and the receiver of the data are separate organisations (even if you are both companies within the same group).

[2] EDPB, 'Adequacy' < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en > Accessed 19 December 2019

[3] See Article 46 of the GDPR

[4] See Article 49 of the GDPR

Example

A Gibraltar company passes employee information to a centralised group human resources service provided by its parent company in Germany. After the UK and Gibraltar exit the EU, this will be a restricted transfer under the Gibraltar GDPR.

As mentioned in the foregoing, Gibraltar law will allow unrestricted transfers to the UK to continue.

If your restricted transfer is not to the EEA, then you should already have considered how to comply with the GDPR. You will continue to be able to rely on the same mechanisms. In particular, an adequacy decision, an appropriate safeguard or an exception, as identified in the foregoing.

1. Adequacy decisions:

- You will be able to make the restricted transfer if it is covered by an adequacy decision made by HMGoG. An adequacy decision confirms that a particular country or territory (or a specified sector in a country or territory) or international organisation, has an adequate data protection regime.
- HMGoG intends to recognise the EU adequacy decisions[5] which have been made by the European Commission prior to the exit date. This will allow restricted transfers to continue to be made to those organisations, countries, territories or sectors covered by an EU adequacy decision. The only exception is in relation to the EU adequacy decision for the EU/US Privacy Shield, as this is an EU/US specific arrangement. HMGoG intends to pursue arrangements for its continued application to restricted transfers from Gibraltar to the USA.

2. Appropriate safeguards:

- If there is no adequacy decision which covers your restricted transfer, you should consider putting in place one of a list of appropriate safeguards to cover the restricted transfer.
- For most businesses, a convenient appropriate safeguard is the use of standard contractual clauses[6] (see section 5). HMGoG intends to recognise European Commission-approved standard contractual clauses as providing an appropriate safeguard for restricted transfers from Gibraltar.
- Over the coming weeks, the Commissioner will publish template contracts for organisations to use, for both -
    - controller to controller transfers; and
    - controller to processor transfers.

Example:

A Gibraltar travel company organises educational visits overseas for schools. It sends personal data of those going on the trips to hotels in Spain, Uruguay and Mexico. The travel company, the schools and each hotel are separate controllers as each is processing the personal data for its own purposes and making its own decisions. The personal data of students is passed from the schools to the Gibraltar

[5] EU Commission, 'Adequacy' < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en > Accessed 19 December 2019

[6] EU Commission, 'International data transfers using model clauses' < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en > Accessed 19 December 2019

company and then to the hotels. The travel company is making a restricted transfer to the hotels. It does not need to take additional steps when transferring personal data to:

- the Spanish hotel (as HMGoG will recognise EEA countries as ensuring adequate level of data protection under Gibraltar law); and
- the Uruguayan hotel (as the Gibraltar government will recognise the adequacy decision made by the European Commission in respect of Uruguay).

In order to transfer personal data to the Mexican hotel it will need to take additional steps to comply with the provisions on restricted transfers in the Gibraltar GDPR.

3. Exceptions

If there is no European Commission adequacy decision in relation to Gibraltar and no appropriate safeguards, but one of the list of EU GDPR exceptions applies, you will be able to make the restricted transfer. These exemptions will continue under the Gibraltar GDPR.

What are the key points if we are receiving transfers from the EEA into Gibraltar?

The EU GDPR will continue to apply to an EEA sender of personal data. Chapter V of the EU GDPR sets out the obligations on the EEA sender of the personal data to you in Gibraltar. You should bear in mind that on exit date Gibraltar will be a third country outside the EEA.

The EDPB are still finalising detailed guidance on this area and we advise that you take a broad interpretation of a restricted transfer, which is that you are receiving a restricted transfer if you are a controller or processor located in Gibraltar and an EEA located controller or processor sends you personal data.

Under the GDPR, an EEA controller or processor will be able to make a restricted transfer of personal data to Gibraltar if any of the following apply:

1. Adequacy decisions

The EEA controller or processor will be able to make a restricted transfer to Gibraltar if it is covered by an adequacy decision by the European Commission.

At exit date there may not be an adequacy decision by the European Commission regarding Gibraltar. We will keep you updated as to any plans or developments regarding an adequacy decision.

2. Appropriate safeguards

If there is no European Commission adequacy decision in respect of Gibraltar, but the EEA sender has put in place one of the EU GDPR list of appropriate safeguards, the EEA sender will be able to make the transfer to you.

For most businesses a convenient appropriate safeguard is standard contractual clauses (see section 5). Over the coming weeks, the Commissioner will publish template contracts for organisations to use, for both -

- controller to controller transfers; and

- controller to processor transfers.

For restricted transfers from an EEA public body to a Gibraltar public body, where one of the parties is unable to enter into a contract, an appropriate safeguard may be provisions inserted into an administrative arrangement[7] between these bodies. This will need to be authorised by the data protection supervisory authority with oversight of the EEA public body.

Example

A Gibraltar regulator makes a request to an EEA counterparty for information about the good standing of an individual who has moved to Gibraltar. The EEA regulator is not able to enter into contracts. The two regulators could agree to an appropriate administrative arrangement, which would need to be approved by the EEA supervisory authority of the EEA counterparty.

If you have in place binding corporate rules[8] covering a Gibraltar-based entity, which are authorised under the EU process **before** the exit date, this will continue to provide an appropriate safeguard for personal data transfers from the EEA to Gibraltar.

Those binding corporate rules would need to be updated, with effect on the exit date, to recognise the UK as a third country outside the EEA for the purposes of the EU GDPR.

3. Exceptions:

If there is no European Commission adequacy decision in relation to Gibraltar and no appropriate safeguards, but one of the list of EU GDPR exceptions applies, your EEA sender will be able to transfer personal data to you.

What are the key points if we are receiving transfers into Gibraltar from countries, territories or sectors covered by a European Commission adequacy decision?

In order to have received and to maintain an adequacy decision, the country or territory is likely to have its own legal restrictions on making transfers of personal data to countries outside of the EEA. This will include Gibraltar on its exit from the EU.

We anticipate that HMGoG will pursue mechanisms with these countries and territories in order to make alternative arrangements for transfers to Gibraltar. We will provide further guidance on this in due course.

Otherwise, if you wish to continue receiving personal data from these countries or territories, you and the sender of the data will need to consider how to comply with local law requirements on transfers of personal data.

How can we prepare?

- The first thing to do is to take stock. Understand your international flows of personal data, so that you know if any of your transfers are or will become restricted transfers under Gibraltar or EU data

[7] See Article 46 of the GDPR

[8] See Article 47 of the GDPR

protection law on exit date. While all transfers have to be considered, you may want to prioritise transfers of large volumes of data, transfers of special category data or criminal convictions and offences data, and your business critical transfers.

- Consider how you may continue to make and receive those transfers lawfully after exit date, and without an adequacy decision by the European Commission in relation to Gibraltar. Key transfers to consider will be from the EEA to Gibraltar.
- Often a relatively simple way to provide an appropriate safeguard for a restricted transfer is to enter into standard contractual clauses between the sender and receiver of personal data (see section 5).
- Multinational corporate groups should also consider their use of existing EEA approved binding corporate rules to make transfers into and out of the Gibraltar. These will need updating to reflect that, under the EU GDPR, Gibraltar becomes a third country on exit date.
- If as a result of exit you will be making transfers of personal data from Gibraltar that will become restricted transfers (e.g. transfers between Gibraltar and the EEA which were previously permitted as transfers between EU Member States), you should also update your documentation[9] and privacy notice[10] to expressly cover those transfers.
- If you are receiving personal data from a country, territory or sector covered by a European Commission adequacy decision, the sender of the data will need to consider how to comply with its local laws on international transfers.

3.1 EUROPEAN REPRESENTATIVES

This section is of particular importance if you are a Gibraltar-based controller or processor:

- without any offices, branches or other establishments in the EEA; and
- you are offering goods or services to individuals in the EEA or monitoring the behaviour of individuals located in the EEA.

You do not need to read this section if you are a Gibraltar-based controller or processor:

- with one or more offices, branches or other establishments in the EEA; or
- you do not offer goods or services to individuals in the EEA and you do not monitor the behaviour of individuals located in the EEA.

If you are based in Gibraltar and do not have a branch, office or other establishment in any other EU or EEA state, but you either:

- offer goods or services to individuals in the EEA; or
- monitor the behaviour of individuals located in the EEA,

then you will still need to comply with the EU GDPR regarding this processing even after Gibraltar leaves the EU.

As you will not be an EEA-based controller or processor after exit date, the EU GDPR requires that you must appoint a representative within the EEA. This representative will need to be set up in an EU or EEA state where some of the individuals whose personal data you are processing in this way are located.

You will need to authorise the representative, in writing, to act on your behalf regarding your EU GDPR compliance, and to deal with any supervisory authorities or data subjects in this respect.

[9] See Article 30 of the GDPR
[10] See Articles 13 and 14 of the GDPR

Your representative may be an individual, or a company or organisation established in the EEA, and must be able to represent you in respect of your obligations under the EU GDPR (e.g. a law firm, consultancy or private company). In practice, the easiest way to appoint a representative may be under a simple service contract.

You should provide EEA-based individuals whose personal data you are processing with the details of your representative. This may be done by including them in your privacy notice or in the upfront information provided to individuals when you collect their data. You must also make it easily accessible to supervisory authorities – for example by publishing it on your website.

Your appointment of your representative must be in writing and should set out the terms of your relationship with them. Having a representative does not affect your own responsibility or liability under the EU GDPR.

Example:

A Gibraltar law firm does not have offices in other EEA countries, but has a regular client base in Sweden and Norway (only). The firm will be required to appoint a European representative to act as its direct contact for data subjects and EU and EEA supervisory authorities. This European representative may be based in either Sweden or Norway, but not any other EU or EEA member state.

The firm will have to include the name of its European representative in the information it provides to the data subjects, for example in its privacy notice. It is not required to inform the supervisory authorities in either Sweden or Norway, or indeed the Commissioner, of this, although the details should be easily accessible to those supervisory authorities.

You do not need to appoint a representative if either:
- you are a public authority; or
- your processing is only occasional, of low risk to the data protection rights of individuals and does not involve special category or criminal offence data on a large scale.

The EDPB has published guidelines on territorial scope which are out for consultation. These contain more guidance on appointing a representative. The view of the EDPB is that supervisory authorities are able to initiate enforcement action (including fines) against a representative in the same way as they could against the controller or processor which appointed them.

HMGoG intends that after Gibraltar and the UK exit the EU, the Gibraltar version of the GDPR will require that a controller or processor located outside of Gibraltar, but which must still comply with the Gibraltar GDPR, will be required to appoint a Gibraltar representative.

How to prepare?

If you do not have any EEA offices, branches or other establishments, you should consider whether you are processing personal data of individuals in the EEA which relates to either:
- offering goods or services to individuals in the EEA; or
- monitoring the behaviour of individuals located in the EEA.

If you are carrying out such processing, and intend to continue after exit date, you will need to consider whether you must appoint a European representative.

You will need to consider in which EU or EEA state your representative will be based and put in place an appropriate written mandate for that representative to act on your behalf. Information about the representative should be provided to data subjects, for example, in your privacy notice. It should also be made easily accessible to supervisory authorities, for example, by publishing it on your website.

3.2 ONE STOP SHOP

You should read this section if you are a Gibraltar-based controller or processor currently carrying out cross-border processing of personal data, across member state borders, but still within the EEA.

You do not need to read this section if you are only based in Gibraltar and your processing of personal data is unlikely to affect individuals in any other EU or EEA state.

Under the GDPR, organisations with several establishments in the EU only have to report to one supervisory authority i.e. the Lead Supervisory Authority. This is also known as the "one-stop-shop" mechanism. This is a new system, so the EDPB is still working out how it will operate in practice. We are waiting for it to have settled its views on this.

In brief, you currently may be carrying out cross-border processing if you have an office, branch or other establishment in Gibraltar and your processing is likely to affect individuals in another EU or EEA state, because either:

1. You are processing the same set of personal data in the context of the activities of both your Gibraltar establishment and one or more EEA offices, branches, or other establishments; or

Example

A fashion retailer:
- has a head office in Gibraltar which handles all its customer data;
- has a distributor in Paris for French sales; and
- sells only in Gibraltar and France.

Before Gibraltar exits the EU: the fashion retailer is cross-border processing its French customer personal data. It is processing that data in the context of both its Gibraltar head office and Paris distributor.

2. You only have offices, branches or other establishments in the Gibraltar, but your processing of personal data is likely to substantially affect data subjects in one or more other EU or EEA states.

Example

A fashion retailer:

- has a single office in Gibraltar which handles all of its customer data; and
- it sells via its website to Gibraltar, France and Italy.

Before Gibraltar exits the EU, the fashion retailer is cross-border processing in Gibraltar, France and Italy, to the extent the Gibraltar office's processing of the customer data substantially affects data subjects in France and Italy.

If you are carrying out cross-border processing, you benefit from the GDPR One-Stop-Shop system. This means a single supervisory authority will act as the lead on behalf of the other EEA supervisory authorities.

It should mean that, regarding your cross-border processing only, you deal with a single lead supervisory authority, which is responsible for regulating your cross-border processing and enforcing the GDPR (including issuing fines), acting on behalf of the other interested EEA authorities. So, if you breach the GDPR regarding your cross-border processing, you are only investigated by one supervisory authority and only receive one fine across the EEA.

There are exceptions to this. For example, the lead supervisory authority may agree that another supervisory authority can take its own enforcement action if complaints only come from within the other authority's jurisdiction.

Examples:

Following the example above, the lead supervisory authority for the fashion retailer is Gibraltar's Commissioner, as its head office is in Gibraltar.

If (prior to Gibraltar exiting the EU) there is a data security breach of the fashion retailer relating to Gibraltar, French and Italian customers, the Commissioner would investigate and bring enforcement action, such as a fine.

The French and Italian supervisory authorities would provide input into the Commissioner's investigation and enforcement action, but **they would not be able to carry out their own investigation or take independent enforcement action.** This means the fashion retailer would only receive a single fine, albeit reflecting the impact of the breach on individuals in Gibraltar, France and Italy. This is a key benefit of the One-Stop-Shop.

If (prior to Gibraltar exiting the EU) a French citizen has a complaint against the fashion retailer regarding a failure to respond to a subject access request, the French citizen may make his/her complaint to the French supervisory authority. The French supervisory authority will contact the Commissioner, and the Commissioner may choose to investigate the complaint itself or agree to the French supervisory authority investigating the matter.

If you are currently established in Gibraltar and carry out cross-border processing (as described above), then four scenarios may apply to you:

<u>Scenario 1</u>

- You are currently cross-border processing in relation to two establishments: one in Gibraltar and one in another EU or EEA state.
- Your processing **is not likely** to substantially affect individuals in any other EU or EEA state.

After exit date:
- You will no longer be cross-border processing. You will no longer be processing personal data in the context of the activities of establishments located in two or more EU or EEA states.
- The One-Stop-Shop and lead authority arrangements will no longer apply to your processing. You will have to deal with both the Commissioner and the supervisory authority in the other EU or EEA state where you are established.

Example:

A fashion retailer:
- has a head office in Gibraltar which handles all its customer data;
- has a distributor in Paris for French sales; and

sells only in Gibraltar and France.

Before Gibraltar exits the EU:
- The fashion retailer is cross-border processing its French customer personal data. It is processing French customer data in the context of both its Gibraltar head office and Paris distributor.

After Gibraltar exits the EU:
- The fashion retailer is no longer cross-border processing. It will only have a single EEA establishment (the Paris distributor) and that distributes to customers only in France.

If there is a security breach of the retailer's customer database impacting Gibraltar and French customers, it will be investigated by the Commissioner under Gibraltar data protection law and the French supervisory authority under the EU GDPR, and it could be fined by both.

Scenario 2

- You are currently cross-border processing in relation to two establishments: one in Gibraltar and one in another EU or EEA state.
- Your processing in the context of the activities of both the Gibraltar and EEA establishment **is likely** to substantially affect individuals in other EU or EEA states.

After exit date:
- Processing in the context of your Gibraltar establishment is no longer cross-border processing.
- Processing in the context of your EEA establishment, which substantially affects data subjects in other EU or EEA states, will continue to be cross-border processing. Its local supervisory authority will be the lead supervisory authority in the EEA in respect of that cross-border processing.
- You will have to deal with both the Commissioner and the EEA lead supervisory authority.

Example:

A fashion retailer:
- has a head office in Gibraltar, which handles all its customer data;

- has a European distribution centre in Paris; and
- sells online to Gibraltar, France, Italy and Spain.

Before Gibraltar exits the EU:
- The fashion retailer is cross-border processing its customer data in the context of both the Gibraltar office and Paris distributor. The Commissioner is likely to be the lead authority.

After Gibraltar exits the EU:
- The fashion retailer is no longer cross-border processing in the context of the Gibraltar office.
- The fashion retailer is cross-border processing in the context of the Paris distributor, for French, Italian and Spanish customer data.
- The French supervisory authority is the lead authority as the fashion retailer only has an establishment in France.
- If there is a security breach of the retailer's customer database impacting French, Italian and Spanish customers, it will be investigated by the Commissioner under Gibraltar data protection law and the French supervisory authority under the EU GDPR and could be fined by both.

Scenario 3

- You are currently cross-border processing in relation to three or more establishments: one in Gibraltar and two or more in other EU or EEA states.
- Your processing may or may not substantially affect individuals in any other EU or EEA state.

After exit date:
- The Gibraltar establishment is no longer cross-border processing.
- Your EU or EEA establishments will still be cross-border processing. You will have to deal with both the Commissioner and your EEA lead supervisory authority. You should review the EDPB guidance to work out which is your lead authority.

Example:

A fashion retailer:
- has a head office in Gibraltar, which handles all its customer data;
- has a global distribution centre in Paris and a global marketing office in Milan; and
- sells online across the world.

Before Gibraltar exits the EU:
- The fashion retailer is cross-border processing in the context of the Gibraltar office, the Paris distributor and Milan office, in relation to its customer database. The Commissioner is likely to be the lead authority.

After Gibraltar exits the EU:
- The fashion retailer is no longer cross-border processing in the context of its Gibraltar office.
- The fashion retailer continues cross-border processing in the context of its Paris and Milan offices. Its lead authority would be decided based on EDPB guidance. If the largest customer base was in Italy, the Italian supervisory authority would probably be the lead authority.

- If there is a security breach of the retailer's customer database it will be investigated by the Commissioner under Gibraltar data protection law and the Italian supervisory authority (if it is the lead authority) under the EU GDPR, and could be fined by both.

Scenario 4

- You are currently cross-border processing with an establishment only in Gibraltar, and no establishment in any other EU or EEA state.
- Your processing is likely to substantially affect individuals in one or more other EU or EEA state.

After exit date:
- you will not be carrying out cross-border processing under the EU GDPR as you have no office, branch or other establishment in the EEA.
- You may still need to comply with the EU GDPR to the extent that your processing relates to the offering of goods or services to, or the monitoring of the behaviour of, individuals in the EEA.
- You may have to deal with the Commissioner and with the supervisory authorities in all EU and EEA states where individuals are located whose personal data you process in connection with those activities.

Example

A fashion retailer:
- has a head office in Gibraltar which handles all customer data; and
- markets and sells online across Europe.

Before Gibraltar exits the EU:
- The fashion retailer is cross-border processing across the EEA.

After Gibraltar exits the EU:
- The fashion retailer is no longer cross-border processing as it has no office, branch or other establishment in the EEA.
- All the fashion retailer's processing of personal data will be subject to the Gibraltar GDPR and the oversight of the Commissioner.
- All the fashion retailer's marketing activities targeting EEA customers will also be subject to the EU GDPR.
- If there is a security breach of the fashion retailer's customer database it will be investigated by the Commissioner under Gibraltar data protection law. It may also be investigated by any of the EEA authorities if it has impacted customers in their member state. In theory, they could be fined by the Commissioner and the supervisory authority in every EU and EEA state where customers have been impacted.
- This could be a key change for your business, and you may want to consider how to minimise any risks. For example, you should consider what resources may be needed to deal with enquiries from various EU and EEA supervisory authorities.

After the exit date, the Commissioner may no longer be part of the One-Stop-Shop. But we will still co-operate and collaborate with European supervisory authorities, as we did before GDPR and the One-Stop-Shop system, regarding any breaches of GDPR that affect individuals in Gibraltar, the UK, the EU and EEA states.

HMGoG and the Commissioner will continue to work towards maintaining the close working relationships between the Commissioner, the UK and the EU supervisory authorities once Gibraltar and the UK have left the EU.

How can we prepare?

- You should consider whether any of your processing of personal data involves cross-border processing under the GDPR, and if so who your lead supervisory authority is.

- Consider whether you will continue to carry out cross-border processing after exit date.

- If you will continue to carry out cross-border processing, and your current lead authority is the Commissioner, review the EDPB guidance, and consider which other EU and EEA supervisory authority will become lead authority on exit date (if any). You may want to contact them closer to exit date.

- If you will no longer carry out cross-border processing after exit date, but your processing will continue to be within the scope of the EU GDPR (for example, if you are "targeting" individuals in the EEA), this could be a key change for your business and you may want to consider its impact.

3.3 OTHER RELEVANT MATTERS

- Privacy notices[11] – the information required in your privacy notice is unlikely to change. However, you may need to review your privacy notice to reflect changes to international transfers, review references to your lawful bases or conditions for processing if any refer to 'Union law' or other terminology changed in the Gibraltar GDPR, and to identify your EU representative (if you are required to have one).
- Rights of data subjects – as a reminder, if the Gibraltar GDPR applies to your processing of personal data, it doesn't matter where in the world the individuals whose data you process are located.
- Documentation – the information required in your record of processing activities is unlikely to change. You may need to review it to reflect changes regarding international transfers. If you have chosen to record the lawful basis or conditions for any of your processing, you need to review any references to "Union law" or other terminology changed in the Gibraltar GDPR.
- Data Protection Impact Assessments (DPIAs) – existing assessments may need to be reviewed in the light of the Gibraltar GDPR; for example, if they cover international data flows which on exit date become restricted transfers.
- Data Protection Officers (DPOs) – if you are currently required to have a DPO, on exit date that requirement will continue, whether under the Gibraltar GDPR or the EU GDPR. You may continue to have a DPO who covers Gibraltar, the UK and EEA. The Gibraltar, UK and EU GDPRs will all require that your DPO is "easily accessible from each establishment" in the EEA, UK and Gibraltar.
- Codes of conduct and certification – the EDPB is working on guidance regarding codes of conduct and certification, and how those schemes may be used for transfers. We do not expect there will be any codes of conduct or certification schemes which are authorised before exit date. The

[11] See articles 13 and 14 of the GDPR.

Commissioner's work on introducing codes of conduct and certification schemes within Gibraltar will continue after Gibraltar and the UK have left the EU.

4. LEAVING THE EU – CHECKLIST

The following checklist highlights six steps you can take now to start preparing for data protection compliance if Gibraltar leaves the EU on the 29th March 2019 without a deal.

If you only operate within Gibraltar, you may not need to do much to prepare for data protection after we leave the EU. Locally, we are committed to the high standards of data protection as set out in the GDPR and the Data Protection Act 2004 (the DPA"), and such standards will remain even after Brexit. Therefore, your best preparation for the future data protection regime is to ensure that you are effectively complying with the GDPR and the DPA now.

You may, however, need to ensure adequate safeguards are in place to maintain any data flows from the EEA, which includes the EU.

If you operate in the EEA, you may need to comply with both Gibraltar's data protection regime and the EU regime after we exit the EU. You may also need to appoint a representative in the EEA. You can use the checklist to work out whether you will be affected once we leave the EU, and take some key steps now, to help you prepare.

We will continue to update our guidance and develop other tools to assist you.

The six steps to take:

1 Continue to comply

Continue to apply GDPR standards and follow current guidance. If you have a DPO, they can continue in the same role for both Gibraltar and Europe.

2 Transfers to Gibraltar

Review your data flows and identify where you receive data into Gibraltar from the EEA. Think about what GDPR safeguards you can put in place to ensure that data can continue to flow once we are outside the EU.

3 Transfers from Gibraltar

Review your data flows and identify where you transfer data from Gibraltar to any other country, as these will fall under new local transfer and documentation provisions.

4 European operations

If you operate across Europe, review your structure, processing operations and data flows to assess how Gibraltar's exit from the EU will affect the data protection regimes that apply to you.

5 Documentation

Review your privacy information and your internal documentation to identify any details that will need updating when Gibraltar leaves the EU.

6 Organisational awareness

Make sure key people in your organisation are aware of these key issues. Include these steps in any planning for leaving the EU and keep up to date with the latest information and guidance.

1 CONTINUE TO COMPLY

You should continue to implement GDPR/DPA compliance standards and follow the current guidance published by the Commissioner.

The DPA will remain in place in Gibraltar and HMGoG intends to further incorporate the GDPR directly into Gibraltar law on exit, to sit alongside it. There will be some technical adjustments to the local version of the GDPR – for example, amending provisions referring to EU law and enforcement cooperation.

Most GDPR requirements will remain the same. This means that the first and most important step is to ensure you comply with GDPR principles, rights and obligations. Our current guidance remains relevant and can help you comply, and we will continue to update it regularly.

If you have a DPO, they may continue in this role. They can combine their future responsibilities with any ongoing EU responsibilities, as long as they have expert knowledge of both local data protection law and the EU regime, and are "easily accessible" from both locations.

2 TRANSFERS TO GIBRALTAR

Review your data flows and identify where you receive data from the EEA, including from suppliers and processors. Think about what GDPR safeguards you can put in place to ensure that data can continue to flow once we are outside the EU.

If you receive data from organisations in the EEA, the sender will need to comply with the transfer provisions of the EU regime. This means the sender needs to make sure there are adequate safeguards in place, or one of the exceptions listed in the GDPR applies.

If the EU issues a formal adequacy decision that the Gibraltar regime offers an adequate level of protection, there will be no need for specific safeguards. However, on exit date there may not be such a decision in place, so organisations should plan to implement adequate safeguards.

The HMGoG has however, made clear its intention to seek adequacy decisions for Gibraltar. An adequacy agreement would recognise Gibraltar's data protection regime as essentially equivalent to those in the EU. It would allow data flows from the EEA and avoid the need for organisations to adopt any specific measures. But any such adequacy decisions will not be in place before the UK and Gibraltar leave the EU (and will take time to conclude). Therefore, organisations need to carefully consider their circumstances and what alternative transfer mechanisms are appropriate to maintain data flows.

You may want to consider putting standard contractual clauses ("SCCs") in place if you are receiving data from the EEA (see section 5).

If you are a multinational group with existing binding corporate rules ("BCRs") that cover the EEA and locally-based group companies, with appropriate changes to show the new status of Gibraltar as a third country, these BCRs are likely to permit the transfer from the EEA to Gibraltar.

3 TRANSFERS FROM GIBRALTAR

Review your data flows and identify where you transfer data from Gibraltar to the EEA, or to countries outside the EEA, as these will fall under new transfer provisions and documentation requirements.

Transfers from Gibraltar to the EU

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

Transfers from Gibraltar to countries outside the EEA

Rules on transfers to countries outside the EEA are likely to remain similar, however, at this stage you do not need to take any specific steps. The Commissioner expects HMGoG to confirm that Gibraltar will reflect existing EU adequacy decisions, approved EU SCCs and BCRs.

4 EUROPEAN OPERATIONS

If you operate across Europe, you should review your structure, processing operations and data flows to assess how Gibraltar's exit from the EU will affect the data protection regimes that apply to you.

Data protection regimes

As an organisation established in Gibraltar, you will need to comply with Gibraltar's data protection regime after exit, and the Commissioner is responsible for regulating this regime.

If you also have offices, branches or other establishments in the EEA, the EU regime will still apply to your European activities even after Gibraltar leaves the EU. The Commissioner, however, will no longer regulate the EU regime.

If you are ONLY based in Gibraltar, but you offer goods or services to individuals in the EEA or you monitor the behaviour of individuals located in the EEA, then the EU regime will also apply to your processing of personal data in relation to those activities. You may have to liaise with the Commissioner and with European supervisory authorities in every EEA and EU state where individuals are affected by these activities.

Lead authority and One-Stop-Shop

If Gibraltar is currently your lead supervisory authority, you should review the structure of your European operations to assess whether you will continue to be able to have a lead authority and benefit from the "One-Stop-Shop".

The "One-Stop-Shop" means you can generally deal with a single European supervisory authority taking action on behalf of the other European supervisory authorities. It avoids your having to deal with regulatory and enforcement action from every supervisory authority in every EEA and EU state where individuals are affected.

After Gibraltar exits from the EU, if you no longer have a lead authority and cannot benefit from the One-Stop-Shop, this could significantly affect your business and the resources you need to deal with enquiries from various European data protection authorities.

The EDPB has published guidelines for identifying your lead supervisory authority.

Appointing a European representative

If you are based in Gibraltar, and not in any other EU or EEA state, but you offer goods or services to individuals in the EEA, or you monitor the behaviour of individuals located in the EEA, then to comply with the EU regime you will need to appoint a suitable representative within the EEA.

This person will act as your local representative with individuals and data protection authorities in the EEA. This is separate from your DPO obligations, and your representative cannot be your DPO or one of your processors. You do not need to appoint a representative if you are a public authority, or if your processing is only occasional, low-risk, and does not involve special category or criminal offence data on a large scale.

5 DOCUMENTATION

Review your privacy information and your documentation to identify any details that will need updating when Gibraltar leaves the EU.

The requirements regarding privacy notices and documentation are unlikely to change but you need to identify any references to EU law or other EU terminology and be ready to make the necessary changes to reflect the relevant terminology by the exit date. You also need to review what you say about international transfers and reflect any changes, especially for data transfers between Gibraltar and EEA.

You may also need to review existing data protection impact assessments ("DPIAs") if they involve data transfers between Gibraltar and the EEA.

6 ORGANISATIONAL AWARENESS

Make sure that key people in your organisation are aware of these key issues. Include these steps in any business planning for leaving the EU and keep up to date with the latest information and guidance.

Key people in your organisation need to be aware of the ongoing importance of GDPR compliance, as well as specific implications for any European operations and data flows. If you have significant operations or relationships in Europe, you can plan ahead. You may find it more difficult to ensure continuity if you leave your preparations until the last minute. It would also be useful to review your organisation's risk register, if you have one.

5. STANDARD CONTRACTUAL CLAUSES

Notwithstanding HMGoG's intention to pursue an adequacy decision for Gibraltar, said decision may not be in place before the UK and Gibraltar leave the EU. In this scenario, SCCs can provide a solution to many organisations wanting to continue the transfer of personal data to and from Gibraltar. The guidance below aims to assist you through this process by helping you decide if SCCs are relevant.

WHAT ARE THE SCCS?

If someone in the EEA sends personal data to someone else who is outside the EEA, they must comply with the GDPR's rules on international transfers of personal data. The SCCs are one of a number of 'safeguards' which can be used to comply.

The SCCs are standard sets of contractual terms and conditions which the sender and the receiver of the personal data both sign up to. They include contractual obligations which help to protect personal data when it leaves the EEA and the protection of the GDPR.

It is the EEA sender of the personal data which must comply with the GDPR rules, but Gibraltar receivers may want to assist those senders in complying, to make sure data continues to flow if we leave the EU without a deal.

Questions

1. **Do I need to use SCCs for transfers from the EEA to Gibraltar (if we leave the EU with no deal)?**

   If you are in Gibraltar, the answer may be yes, SCCs may suit your needs.

2. **Who is sending you the data?**
   The GDPR transfer rules do not apply if -
   - the person sending you the data is the data subject, that is the individual that the personal data relates to;
   - an individual is sending the data for purely personal family or household reasons (e.g. personal correspondence or personal social media activity); or
   - the data is being sent within your own company or organisation (e.g. from an employee or partner).
   - The GDPR transfer rules do apply to -
     - transfers to another company within the same multinational corporate group; and
     - sole traders or individual contractors or consultants, which count as a separate business.

   IMPORTANT NOTE: If you are part of a multinational corporate group and are making an intra-group transfer, SCCs may not be suitable for you. You may still be able to use SCCs but you may wish to consider BCRs.

3. **If your answer to the above indicates that the GDPR transfer rules do apply and you are not signed up to BCRs, you should consider this next question: Is the person sending you the data acting as controller?**

   Please note that an organisation is a controller if they decide what personal data they collect and why. In such cases, the organisation is best placed to advise whether or not they are a controller.

   The sender may be acting as a controller where:
   - They have confirmed that they are the controller.
   - They are sending you the data for you to provide a service to the sender, for the sender's business purposes.
   - The data is about people and the sender holds the relationship with, for example:
     - the sender's staff, customers or clients (including visitors to their website);
     - the sender's suppliers, service providers, advisers, consultants or other professional experts; or
     - the sender's members, supporters, shareholders, complainants, correspondents, enquirers, patients, students, pupils, or anyone else the sender deals with for its business purposes.
   - The sender is a professional consultant or adviser with professional or regulatory obligations when they process personal data (e.g. a lawyer or accountant), even if they are acting for you.
   - The sender is sending papers or notes to you for data entry, electronic storage or structured filing services in Gibraltar, even if this is not structured data when they send it.
   - The sender may not be acting as a controller where:
     - The sender is your service provider and holds the data only on your behalf, therefore providing its services to you.
     - Where they are acting only on your instructions and is therefore known as a 'processor'.
     - They are a processor acting on behalf of another company or organisation and acting only on the instructions of that other company or organisation.

   IMPORTANT NOTE: You can only use the SCCs if the sender of the data is acting as a controller. If the sender is acting as your processor or someone else's processor, you cannot use SCCs. However, you can contact the controller (on whose behalf the processor is acting) to see if they will enter into SCCs with your organisation.

4. **If your answer to the above indicates that the sender is a controller, you should consider this next question: Is the sender in the EEA?**

   The EEA is made up of all the EU member states plus the EEA states (not including the UK and Gibraltar). The EU member states are:

Austria	France	Malta
Bulgaria	Germany	Netherlands
Belgium	Greece	Poland
Croatia	Hungary	Portugal
Cyprus	Ireland	Romania
Czech Republic	Italy	Slovakia

Denmark	Latvia	Slovenia
Estonia	Lithuania	Spain
Finland	Luxembourg	Sweden

The EEA states are:

Iceland	Norway	Liechtenstein

If you your answer is no, the sender is outside the EEA – you do not need to use SCCs.

IMPORTANT NOTE: The GDPR transfer rules mainly apply to senders in the EEA. The GDPR also applies to organisations outside the EEA that offer goods or services to individuals located in the EEA, or which monitor individuals located inside the EEA. If you think this may apply to your sender, you or the sender may need to seek professional advice about how the GDPR and the GDPR rules on transfers apply.

5. If your answer to the above indicates that the sender is outside the EEA, you need to consider this next question: Is there an urgent reason why you need to receive this data?

If you and the sender of the data think there is an urgent reason why you should go ahead without waiting to put SCCs in place, the sender may be able to rely on an exception:

a) If there is a medical emergency and you need the data 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 you will be able to rely on an exemption[12]. The sender may go ahead and make the transfer.

b) The other exceptions are very limited in scope. Broadly, they 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.

Based on the above, if there is an urgent reason for a one-off or occasional transfer and you don't have time to put SCCs in place, you may be able to rely on an exception.

6. If your answer to the above indicates that there is no urgent reason why you need to receive this data, then you will need to consider this next question: is there a realistic alternative transfer safeguard that can be used?

There may be an alternative transfer safeguard where:

- You are a public authority receiving the data from another public authority, you may still use the SCCs, if both you and the sender are able to enter into contracts. However, there other options for transfer between public authorities - you may be able to enter into your own contract or (if

[12] Article 49(1)(f) of the GDPR

one or both public authorities are unable to enter into a contract) an administrative arrangement to ensure individuals rights and remedies.
- If you are making a transfer within a multinational group of companies, you may not need SCCs if your group has approved BCRs in place.

However, please note that if you are a small or medium sized business or third sector organisation, then SCCs are often your best option. You are unlikely to have a realistic alternative.

7. **If your answer to the above does not provide you with a realistic alternative transfer safeguard and you require using SCCs, then you will need to consider this last question: Which version of SCCs do you need?**

   There are two different sets of SCCs. Which version to use depends on whether you are receiving the data as a controller or as a processor.

   You will need a 'controller to controller' SCC if:

   - You decide how and why to use the data you receive for your own business purposes, it's about your staff, customers, members or business contacts, or if you consider yourself to be the "owner" of the data once you have it.

   - If you are a professional consultant or adviser with professional or regulatory obligations when you process personal data (e.g. a lawyer or accountant), even if you are acting for the sender.

   You will need a 'controller to processor' SCC if:

   - You are providing services to the sender of the data and handling the data on the sender's behalf in accordance with their instructions.

   - If the sender is sending papers or notes to you for data entry, electronic storage or structured filing services in Gibraltar, even if this is not structured data when they send it.

   If you are in any doubt about whether you are acting as a controller or a processor, read guidance on controllers and processors before you consider this question.

   Current SCCs approved by the EU Commission, which organisations can use are available here. Over the coming weeks, the Commissioner will publish his own templates for organisations to use.

CONTACT US

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

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