GRA
GIBRALTAR REGULATORY AUTHORITY

(12) Data Protection & Brexit for Law Enforcement Authorities

Guidance on Part III of the Data Protection Act 2004 (transposing the Law Enforcement Directive)

13th March 2019

Guidance Note IR12/18

CONTENTS

1. INTRODUCTION

This checklist highlights five steps Law Enforcement Authorities ("LEAs") can take to prepare for data protection compliance if Gibraltar leaves the EU without a deal.

As per sections 39 and 40 of the Data Protection Act 2004 (the "DPA"), the processing of personal data by a LEA (referred to as a "competent authority" in the DPA) for "law enforcement purposes" is regulated by Part III of the "DPA", not the General Data Protection Regulation ("GDPR").

If you are not a competent authority, or you are a competent authority processing for non-law enforcement purposes (e.g. HR records), refer to our separate Guidance Note "Getting Ready for Brexit".

The relevant law enforcement processing regime in Part III of the DPA will continue to apply after Gibraltar leaves the EU. Therefore, your best preparation is to ensure you are already complying with current data protection law.

You may however need to ensure 'appropriate safeguards' are in place to maintain any data flows to you from the EU.

The checklist that follows may be used to help you work out whether you will be affected once we leave the EU and take some key steps to prepare.

DATA PROTECTION AND BREXIT

LAW ENFORCEMENT PROCESSING

FIVE STEPS TO TAKE:

1

CONTINUE TO COMPLY

Continue to comply with Part III of the DPA and follow guidance published by the Information Commissioner ("the Commissioner").

2

TRANSFERS TO GIBRALTAR

Review your data flows and identify where you receive data into Gibraltar from the EU. Talk to your European partners about whether they need you to incorporate any additional safeguards to ensure data can continue to flow.

3

TRANSFERS FROM GIBRALTAR

Review your data flows and identify where you transfer data from Gibraltar to the EU, so that you can document the new basis for those transfers.

4

DOCUMENTATION

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

5

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

There will be some minor technical amendments to the transfers provisions of Part III to reflect the fact that Gibraltar would no longer be part of the EU after exit day, but these changes will not affect your day-to-day domestic processing.

This means the first and most important step is to ensure you continue to comply with the principles, rights and obligations set out in Part III of the DPA. Our current guidance remains relevant and can help you to comply. We will continue to review and update it regularly to reflect any changes or developments in practice.

2 TRANSFERS TO GIBRALTAR

Review your data flows and identify where you receive data from the EU. Keep an open communication line with your European partners about whether they want you to employ any additional safeguards to ensure data can continue to flow.

Once we leave the EU, we will become a 'third country' for EU data protection purposes. If you receive personal data from a law enforcement partner in the EU, this means the sender will need to comply with the transfer provisions under their national data protection law (which are likely to be similar to the provisions in Part III of the DPA).

If the EU makes a formal 'adequacy decision' that the Gibraltar regime offers an adequate level of protection, there will be no need for specific safeguards. However, if we leave the EU on the 29 March 2019 without a deal, there will not yet be such a decision in place. Therefore, in practice, this means the EU sender needs to make sure there are other appropriate safeguards in place – either through a contract or other binding legal instrument, or by making their own assessment of appropriate safeguards. The sender may take into account the protection provided by the DPA itself when making this assessment.

If you receive personal data from other types of organisations in the EU or EEA who are subject to the GDPR, the sender will need to comply with the transfer provisions of the GDPR. You may want to consider putting standard contractual clauses (SCCs) in place to ensure adequate safeguards in these cases.

3 TRANSFERS FROM GIBRALTAR

Review your data flows and identify where you transfer data to the EU, so that you can document the new basis for those transfers.

Transfers from Gibraltar to the EU

The Gibraltar government has confirmed that there will be a transitional adequacy decision in place to cover transfers to EU member states and the UK.

This means that you will be able to continue to send personal data from Gibraltar to your law enforcement partners in the EU, as long as you can show the transfer is necessary for law enforcement purposes. You can also transfer personal data to non-law enforcement bodies in the EU if you can meet some additional conditions, but you will need to notify the Information Commissioner.

Transfers from Gibraltar to countries outside the EU

Rules on transfers to other countries outside the EU will remain the same in practice. At this stage you don't need to take any specific additional steps.

4 DOCUMENTATION

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

The requirements for privacy notices, documentation and logging are unlikely to change but you need to review what you say about international transfers and make sure it includes details of transfers to the EU. You may also need to identify any references to EU law, EU membership or other EU terminology, and be ready to make changes to reflect Gibraltar's status outside the EU by exit date.

You may also need to review existing Data Protection Impact Assessments (DPIAs) if they involve data transfers between Gibraltar and EU.

5 ORGANISATIONAL AWARENESS

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

Key people in your organisation need to be aware of the ongoing importance of data protection compliance, as well as specific implications for data flows. If you have significant data transfers to and from the EU, you can plan ahead. You may find it more difficult to ensure continuity if you leave your preparations until the last minute.

We will keep this guidance under review and update it if anything changes, or more details become available.

IMPORTANT NOTE

The 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