GRA
GIBRALTAR REGULATORY AUTHORITY

UK-US Data Bridge: Guidance for Gibraltar Businesses

21st September 2023

Further guidance in relation to Guidance Note IR11/18

FOREWORD

Gibraltar's data protection law consists of both the Gibraltar General Data Protection Regulation ("Gibraltar GDPR") and the Data Protection Act 2004 ("DPA").

The legislation in Gibraltar maintains the data protection standards that applied in Gibraltar as a result of EU Law i.e., the EU General Data Protection Regulation 2016/679 and the Law Enforcement Directive 2016/680, prior to Brexit and the end of the transition period.

Organisations involved in the processing of personal data need to be aware of the obligations that the Gibraltar GDPR and/or the DPA impose on them.

The Gibraltar Regulatory Authority, as the Information Commissioner, regularly publish guidance notes that aim to –

• raise awareness amongst controllers and processors of their data protection obligations; and,

• assist them in ensuring compliance.

Guidance notes also aim to promote public awareness of the risks to personal data that may arise from data processing activities.

CONTENTS

1. INTRODUCTION

From **12 October 2023**, businesses in Gibraltar can start to transfer personal data to US organisations certified to the "UK Extension to the EU-US Data Privacy Framework" (the "UK Extension") without the need for further safeguards such as those set out in Articles 46 and 49 of the Gibraltar General Data Protection Regulation (the "Gibraltar GDPR").[1]

The EU-US Data Privacy Framework (the "DPF") is a bespoke, opt-in certification scheme for US organisations, enforced by the Federal Trade Commission (the "FTC") and Department of Transportation ("DoT"), and administered by the Department of Commerce.

The DPF includes a set of enforceable principles and requirements that must be certified to, and complied with, in order for organisations to be able to join said framework. These principles take the form of commitments to data protection and govern how an organisation uses, collects, and discloses personal data. US organisations who have been certified to the DPF can opt in to receiving data from Gibraltar.

Once a US organisation has been certified and is publicly placed onto the DPF list (the "DPF List") on the DPF website, they can receive personal data from Gibraltar through a UK-US data bridge (the "Data Bridge").

2. WHAT TYPES OF ORGANISATIONS ARE INCLUDED AND EXCLUDED UNDER THE DPF?

Unlike some other adequacy regulations, Gibraltar-based organisations cannot simply transfer personal data to any data importer/recipient in the US - for the data to flow freely, the relevant recipient **must** be certified to the UK Extension and appear on the DPF List.

Only US organisations subject to the jurisdiction of the US FTC or the US DoT are currently eligible to participate in the DPF program. Those organisations not subject to the jurisdiction of either the FTC or DoT — for example, banking, insurance, and telecommunications companies — are unable to participate in the DPF program at this time.

[1] See Article 45(1)(a) of the Gibraltar GDPR and UK's Data Protection (Adequacy) (United States of America) Regulations 2023 here: https://www.legislation.gov.uk/uksi/2023/1028/introduction/made.

3. WHAT CATEGORIES OF DATA ARE EXCLUDED FROM TRANSFER UNDER THE DPF?

Journalistic data defined by Supplemental Principle 2(b) of the DPF is not subject to the requirements of the DPF. Therefore, such data **cannot** be transferred under the Data Bridge.

For information, the Journalistic Exceptions Supplemental Principle 2(b) states that:

> *Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Principles.*

4. SHOULD SPECIAL CATEGORY OR SENSITIVE DATA BE SHARED UNDER THE DATA BRIDGE?

Special category[2] and sensitive data can be shared with certified US organisations, **however**, this must correctly be identified by Gibraltar-based organisations as such when it is being shared.

The Choice principle 2(c) sets out that:

> *Personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual*

are considered *sensitive information* under the DPF. Organisations under the DPF are also required to treat as *sensitive*, any information received which has been identified and previously been treated as sensitive.

[2] See Article 9(1) of the Gibraltar GDPR which specifies the special categories of personal data that are prohibited from being processed unless one of the conditions under Article 9(2) of the Gibraltar GDPR are met, in addition to a lawful basis under Article 6(1) of the Gibraltar GDPR. In accordance with Section 12(2) and (3) of the Data Protection Act 2004 (the "DPA"), some of these conditions also require organisations to meet additional conditions and safeguards set out in Schedule 1 of the DPA. For further guidance, see sections 3 and 5 of the Information Commissioner's Guidance Note (6) Identifying the 'Lawful Basis' available here: https://www.gra.gi/data-protection/guidance.

Gibraltar personal data which is considered to be sensitive, and which is not covered by the list set out within the Choice principle, must be appropriately **identified** as sensitive to US organisations when transferred under the Data Bridge to ensure it receives appropriate protections under the DPF. This will include -

- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning sexual orientation.

5. SHOULD CRIMINAL OFFENCE DATA BE SHARED UNDER THE DATA BRIDGE?

Where criminal offence data[3] is proposed to be shared under the Data Bridge as part of a human resources ("HR") data relationship, recipient organisations in the US are required to indicate that they are seeking to receive such data under the DPF.

HR data is clarified under Human Resources Data Supplemental principle 9(a)(i) as:

> *…personal information about its employees (past or present) collected in the context of the employment relationship* [transferred] *to a parent, affiliate, or unaffiliated service provider in the United States participating in the EU-U.S. DPF…*

Alternatively, if criminal offence data is shared outside of a HR relationship, it should be indicated to the US recipient organisation that it is sensitive data requiring additional protections, in line with protections for special category or sensitive data set out above.

[3] Personal data relating to 'criminal convictions and offences or related security measures' covers information about offenders or suspected offenders in the context of criminal activity, allegations, investigations, and/or proceedings. In order to process such data under the general processing regime set out in the Gibraltar GDPR (i.e., under Part II of the DPA and not under the law enforcement processing regime under Part III of the DPA), organisations must meet a lawful basis under Article 6(1) of the Gibraltar GDPR and ensure that the processing is authorised by Gibraltar law as per Article 10(1) of the Gibraltar GDPR. Section 12(5) of the DPA makes provision about when the requirement at Article 10(1) of the Gibraltar GDPR is met. For further guidance, see sections 3 and 6 of the Information Commissioner's Guidance Note (6) Identifying the 'Lawful Basis' available here: https://www.gra.gi/data-protection/guidance.

6. HOW CAN YOU CHECK WHICH SPECIFIC BUSINESSES HAVE CERTIFIED TO THE UK EXTENSION?

Before sending personal data to the US, you must confirm that the recipient is self-certified with the DPF (and when transferring HR data specifically, US organisations must have highlighted this on their certification). More precisely, you must:

1. Confirm whether an organisation is an active DPF participant, go to the DPF List[4] and search alphabetically or by typing in the organisation name in the search bar.

2. Confirm that said organisation has signed up to the UK Extension to the DPF program.

3. If wishing to transfer HR data, confirm that HR data is covered by the organisation's DPF commitments -

    - click on the organisation's name within the DPF List[5];
    - within the organisation's DPF program record, click on the link to the relevant privacy policy or policies (for HR data and/or non-HR data) under the "Privacy Policy" section of the record.

4. Review the privacy policy that applies to the covered information:

    - Within the organisation's DPF program record, click on the link to the relevant privacy policy or policies (for HR data and/or non-HR data) under the "Privacy Policy" section of the record.

If you cannot rely on the UK Extension to transfer personal data to the US, your organisation will have to revert to one of the pre-existing appropriate safeguards (e.g., the International Data Transfer Agreement[6] or the Gibraltar Addendum to the EU Standard Contractual Clauses[7]) or rely on one of the available derogations under Article 49 of the Gibraltar GDPR for international data transfers. You may also need to carry out a transfer risk assessment to validate your transfers.

[4] DPF participant search available here: https://www.dataprivacyframework.gov/s/participant-search.

[5] Ibid.

[6] See the document entitled 'INTERNATIONAL DATA TRANSFER AGREEMENT' under section (11) International Transfers on the Information Commissioner's website available here: https://www.gra.gi/data-protection/guidance.

[7] See the document entitled 'ADDENDUM' under section (11) International Transfers on the Information Commissioner's website available here: https://www.gra.gi/data-protection/guidance .

7. FURTHER GUIDANCE

- EU-US Data Privacy Framework: https://www.dataprivacyframework.gov/s/european-businesses

- Gibraltar Information Commissioner (Gibraltar Regulatory Authority)[8]: https://www.gra.gi/uploads/documents/data-protection/Documents/Guidance/GDPR11.pdf

[8] See the Information Commissioner's Guidance Note (11) International Transfers, available here: https://www.gra.gi/data-protection/guidance.

IMPORTANT NOTE

This document is purely for guidance and does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the Gibraltar GDPR and the DPA may apply directly to them. The responsibility to become familiar with the Gibraltar GDPR and the DPA and comply with its provisions where applicable lies with the organisation.

Where necessary, the Information 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 Gibraltar GDPR and the DPA, the Gibraltar GDPR and the 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