Version 1: June 2022
For more information please visit odpa.gg/data-transfer

Transfer Impact Assessments
relating to *The Data Protection (Bailiwick of Guernsey) Law, 2017* ("the Law")

This document is in two parts:

- **Part 1**: is a self-assessment tool for you to use whenever you need to do a Transfer Impact Assessment.
- **Part 2**: helps you use the self-assessment tool effectively by guiding you through each step of the Transfer Impact Assessment process.

Part 1: Self-assessment tool for you to use when you need to do a Transfer Impact Assessment

This tool is for you to use before you transfer people's data outside the Bailiwick of Guernsey, to prompt you to:

- document detailed answers to the seven questions below and
- take any steps necessary that arise from the seven questions.

These seven questions are intended to be used as a tool to help you make a self-assessment of the risk posed by a transfer of someone's data outside of the Bailiwick of Guernsey.

1. QUESTION 1: Which data protection law(s) are you subject to?
2. QUESTION 2: What are the details of the data transfer in question?
3. QUESTION 3: What transfer tool are you using?
4. QUESTION 4: What are the laws and practices of the country where the data is going to?
5. QUESTION 5: Have you identified any 'supplementary measures' needed to protect the data, where necessary?
6. QUESTION 6: Have you identified what formal steps the 'supplementary measures' require and how you will put them in place?
7. QUESTION 7: Have you assessed when it's appropriate to re-evaluate whether the data is still adequately protected?

In addition to the above questions, you may find it a useful exercise to produce a '**data transfer map**' (a simple visual representation showing the path of the data transfer). You could add key details to the map based on your responses to the above questions.

THE OFFICE OF THE Data Protection Authority

Version 1: June 2022
For more information please visit odpa.gg/data-transfer

PART 2: What you need to know about Transfer Impact Assessments

Introduction

The Law was adopted in the Bailiwick of Guernsey in order to bring the Bailiwick's data protection regime up to the standards of the EU General Data Protection Regulation ("**GDPR**").

In its July 2020 judgment C-311/18 ("**Schrems II**") the Court of Justice of the European Union ("**CJEU**") emphasised that the protection granted to personal data in the European Economic Area (EEA) (and by extension the Bailiwick) must travel with the data wherever it goes.

Transferring personal data to third countries cannot be a means to undermine or water down the protection it is afforded in the Bailiwick.

Where you rely on one of the "**available safeguards**" under the Law, the CJEU in Schrems II stated that controllers or processors, acting as exporters, are responsible for verifying, on a **case-by-case basis** and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the relevant transfer tools.

In those cases, the CJEU still leaves open the possibility for exporters to implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU/ Bailiwick law.

The CJEU did not specify which measures these could be. However, the Court underlines that exporters will need to identify them on a case-by-case basis.

You may wish to consider guidance published by the European Data Protection Board (the "**EDPB**"), including its guidance on supplementary measures.

You should undertake a Transfer Impact Assessment as follows:

Section 1 – Which law are you subject to?

In common with the Law, the GDPR and its UK equivalent (the "**UK GDPR**") have extra territorial effect (i.e. they apply beyond the jurisdiction they were made in). It is therefore possible that you may be dealing with international transfers under the Law and other laws (such as the GDPR).

Whilst the rules applicable to such transfers are similar, they are not the same and you should satisfy yourself that you understand the applicable law(s) in your situation.

Section 2 – Know Your Transfers

A critical part of being able to transfer information lawfully (and identifying when you should not undertake a transfer) is mapping and understanding your transfers.

Mapping all transfers of personal data to third countries can be a difficult exercise. Being aware of where the personal data goes is however necessary to ensure that it is afforded an essentially equivalent level of protection wherever it is processed.

You should also bear in mind that you will need to consider the Law's other provisions before you make a transfer.

You should also satisfy yourself as to:

- What capacity you are acting in – controller, joint controller or processor?
- What capacity the recipient is acting in – controller, joint controller or processor?

If you are acting as a **controller** or a **joint controller,** you should ensure that you have considered the lawful basis for your transfer and that the data to be transferred is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Section 3 – Verify your transfer tool

A next step is to verify the transfer tool your transfer relies on, amongst those listed under the Law.

Please review the international data transfer guidance which sets out the options for transfer tools.

If the European Commission has already declared the country, region or sector to which you are transferring the data as 'adequate', through one of its adequacy decisions under Article 45 of the GDPR or under the previous Directive 95/46 as long as the decision is still in force, you will not need to take any further steps, other than monitoring that the adequacy decision remains valid.

In the absence of an adequacy decision, you need to rely on one of the transfer tools listed under the Law, these are detailed in the international data transfer guidance.

This guidance also includes details what to do if you are unable to rely on a transfer tool, as you may be able to make use of one of the exceptions listed in the Law– although their use is restricted to specific situations.

Section 4 – Assess the laws and practices within the Recipient Country

The fourth step is to assess if there is anything in the law and/or practices in force in the third country to which you wish to transfer data that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer.

You will need to pay specific attention to any laws which lay down requirements to disclose personal data to public authorities or granting such public authorities powers of access to personal data (for instance for criminal law enforcement, regulatory supervision or national security purposes).

Laws and practices in the third country will be considered to be incompatible with transfer tools if they exceed what is necessary in a democratic society for the following purposes (set out in Article 23(1) of the GDPR):

a. National security;

b. Defence;

c. Public security;

d. The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

e. Other important objectives of general public interest of the Bailiwick of Guernsey, in particular an important economic or financial interest of the Bailiwick of Guernsey, including monetary, budgetary and taxation matters, public health and social security;

f. The protection of judicial independence and judicial proceedings;

g. The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

h. A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

i. The protection of the data subject or the rights and freedoms of others;

j. The enforcement of civil law claims.

In making your assessment, you should ensure that you take into account:

- The purposes for which the data are to be transferred and processed (e.g. marketing, HR, storage, IT support, clinical trials);
- The types of entities involved in the processing and their respective roles (public/private; controller/processor);
- The sector in which the transfer occurs (e.g. adtech, telecommunication, financial, etc);
- Categories of personal data transferred;
- Whether the data will be stored in the third country or whether there is remote access to data stored within the Bailiwick;
- Format of the data to be transferred (i.e. in plain text/ pseudonymised or encrypted);
- Any possibility that the personal data may be subject to onward transfers from the third country to another third country.

You will need to ensure that you engage the data importer in your assessment. You (and/or the importer) may also need to obtain legal advice in the third country.

You may use external sources of information for your assessment. Such sources must be:

- **Relevant** to the specific transfer;
- **Objective** and supported by empirical evidence, based on knowledge gained from the past, not assumptions about potential events and risks;
- **Reliable** both in terms of its source and in terms of the information itself;
- **Verifiable**: information and conclusions should be verifiable or contrastable with other types of information or sources;
- **Publicly available or otherwise accessible**: information should preferably be public or at least accessible to facilitate the verification of the criteria made above and ensure its possible sharing with supervisory authorities, judicial authorities and, ultimately, data subjects.

Useful sources of information in relation to the practices applicable to third country jurisdictions might include:

- Case-law of the CJEU and of the European Court of Human Rights (ECtHR) as referred to in the European Essential Guarantees recommendations;
- Adequacy decisions in the country of destination if the transfer relies on a different legal basis;
- Resolutions and reports from intergovernmental organisations, such as the Council of Europe, other regional bodies and/or UN bodies and agencies (e.g. UN Human Rights Council, Human Rights Committee);
- Reports and analysis from competent regulatory networks, such as the Global Privacy Assembly (GPA);
- National case-law (including the Royal Court of Guernsey and/or the Royal Court of Jersey) or decisions taken by independent judicial or administrative authorities competent on data privacy and data protection of third countries;
- Reports of independent oversight or parliamentary bodies;
- Reports based on practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, from entities active in the same sector as the importer;
- 'Warrant canaries' of other entities processing data in the same field as the importer;
- Reports produced or commissioned by chambers of commerce, business, professional and trade associations, governmental, diplomatic, trade and investment agencies of the exporter or other third countries exporting to the third country to which the transfer is made;
- Reports from academic institutions, and civil society organisations (e.g. NGOs);
- Reports from private providers of business intelligence on financial, regulatory and reputational risks for companies;
- 'Warrant canaries' of the importer itself – e.g. the documented practical experience of the importer. You will only be able to use the experience of the importer as an additional source of information if the legal framework of the third country does not prohibit the importer to provide information on requests for disclosure from public authorities or on the absence of such requests (and you should also document such an assessment);
- Transparency reports, on the condition that they expressly mention the fact that no access requests were received. Transparency reports merely silent on this point would not qualify as sufficient evidence as these reports most often focus on access requests received from law enforcement authorities and provide figures only on this aspect while remaining silent on access requests for national security purposes received. This does not mean that no access requests were received but rather that this information cannot be shared;
- Internal statements or records of the importer expressly indicating that no access requests were received for a sufficiently long period; and with a preference for statements and records engaging the liability of the importer and/or issued by internal positions with some autonomy such as internal auditors, DPOs, etc.

The fundamental question to ask is whether the data importer's commitments enabling data subjects to exercise their rights as provided in the transfer tool (such as access, correction and deletion requests for transferred data, as well as judicial redress) can be effectively applied in practice, and are not thwarted by the laws and/or practices in the third country of destination.

In doing so, you will need to consider whether the relevant law or practice contravenes Article 47 of the EU Charter of Fundamental Rights (Right to an Effective Remedy and to a fair trial) or Article 52 (which provide for limitations on rights only where necessary).

You should use the EDPB European Essential Guarantees ("**EEG**") recommendations[1] which set out standards for surveillance measures.

When might your transfer be problematic?

1. Legislation in the third country formally meeting the required standards is manifestly not applied/complied with in practice;
2. There are practices incompatible with the commitments of the transfer tool where relevant legislation in the third country is lacking;
3. Your transferred data and/or importer falls or might fall within the scope of problematic legislation (i.e. impinging on the transfer tool's contractual guarantee of an essentially equivalent level of protection and not meeting EU standards on fundamental rights, necessity and proportionality).

In the first two situations, you will have to **suspend** the transfer or **implement adequate supplementary measures** if you wish to proceed with it.

In the third situation, in light of uncertainties surrounding the potential application of problematic legislation to your transfer, you may decide to:

- suspend the transfer;
- implement supplementary measures to proceed with it; or
- alternatively, you may decide to proceed with the transfer without implementing supplementary measures if you consider and are able to demonstrate and document that you have no reason to believe that relevant and problematic legislation will be interpreted and/or applied in practice so as to cover your transferred data and importer.

You must document your assessment set out above.

[1] Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 of the GDPR, and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations022020-european-essential_en

Example:

The CJEU held that Section 702 of the Foreign Intelligence Surveillance Act of 1978 ("**FISA**") does not respect the minimum safeguards resulting from the principle of proportionality under EU law and cannot be regarded as limited to what is strictly necessary.

This means that the level of protection of the programs authorised by Section 702 FISA is not essentially equivalent to the safeguards required under EU law.

Assessment: If your assessment of the relevant U.S. legislation leads you to consider that your transfer might fall within the scope of Section 702 FISA, but you are unsure if it falls within its practical scope of application, you may decide either:

1. To stop the transfer;

2. To adopt appropriate supplementary measures that ensure effectively a level of protection of the data transferred essentially equivalent to that guaranteed in the Law; or

3. To look at other objective, reliable, relevant, verifiable and preferably publicly available information (which may include information provided to you by your data importer) to clarify the scope of application in practice of Section 702 FISA to your particular transfer. This information should provide answers to some relevant questions, such as the following:

- Does publicly available information show that there is a legal prohibition of informing about a specific request for access to data received and wide restrictions on providing general information about requests for access to data received or the absence of requests received?
- Has your data importer confirmed that it has received requests for access to data from U.S. public authorities in the past?
- Has your data importer confirmed that it has not received requests for access to data from U.S. public authorities in the past and that it is not prohibited from providing information about such requests or their absence?
- Does publicly available information you obtained on U.S. case law and reports from oversight bodies, civil society organisations, and academic institutions reveal data importers of the same sector as your importer have received requests for access to data for similar transferred data in the past?

The answers to these questions that you obtain through your overall assessment lead you to conclude either that:

- Section 702 FISA applies in practice to your particular transfer and therefore, impinges on the effectiveness of your Law transfer tool. Consequently, if you wish to proceed with the transfer, you must consider, where appropriate in collaboration with the importer, if you can adopt supplementary measures that ensure effectively a level of protection of the transferred data essentially equivalent to that guaranteed in the EEA. If you cannot find effective supplementary measures, you must not transfer the personal data.
  Or
- Section 702 FISA does **not** apply in practice to your particular transfer and therefore, does not impinge on the effectiveness of your Law transfer tool. You may then proceed with the transfer without any supplementary measures.

Section 5 - Identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the required standard of essential equivalence

This step is only necessary if your assessment reveals that the third country legislation and/or practices impinge on the effectiveness of the transfer tool you are relying on, or you intend to rely on, in the context of your transfer.

The types of supplementary measures which may satisfy the need bring the level of protection of the data transferred up to the required standard of essential equivalence are set out in Annex 2 of the EDPB Guidance on Supplementary Measures[2], which sets out a non-exhaustive list of examples of supplementary measures with some of the conditions they would require to be effective.

You are responsible for assessing their effectiveness in the context of the transfer, and in light of the third country law and practices and the transfer tool you are relying on.

You should also **document your assessment.**

Section 6 - Take any formal procedural steps the adoption of your supplementary measure may require, depending on the Law transfer tool you are relying on

You may need to consult your competent supervisory authorities on the formal procedural steps you have selected. For example, if you intend to utilise **binding corporate rules**, you will need to seek the approval of the Bailiwick of Guernsey's Data Protection Authority under Section 58 of the Law.

The use of **EU Standard Contractual Clauses,** with or without the Bailiwick of Guernsey Addendum, requires no Authority approval.

Section 7 - re-evaluate at appropriate intervals the level of protection afforded to the personal data you transfer to third countries and monitor if there have been (or there will be) any developments that may affect it

The principle of accountability requires continuous vigilance of the level of protection of personal data.

The Authority will take action to ensure that controllers and processors comply and continue to comply with their obligations under Part X of the Law.

[2] See Annex 2 of edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (europa.eu)