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

Guidance on International Data Transfers (under *The Data Protection (Bailiwick of Guernsey) Law, 2017*)

BACKGROUND:
The Data Protection (Bailiwick of Guernsey) Law, 2017 (the "**Law**") provides protection for data subjects[1] whose personal data is processed by controllers and processors in the Bailiwick of Guernsey (with some limited exceptions).

ISSUE:
Individuals risk losing the Law's protection where their personal data is **transferred outside** of the Bailiwick.

On that basis, Part X of the Law **restricts** the transfer of personal data to countries outside the Bailiwick where the transfer is to an "**unauthorised jurisdiction**" – which is broadly any jurisdiction other than the ones listed here:

- The Bailiwick of Guernsey;
- A Member State of the European Union or European Economic Area;
- A jurisdiction which is the subject of an adequacy finding by the European Commission (as at April 2022: Andorra, Argentina, Canada (in respect of commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan (private sector only), Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom and Uruguay.

We refer in this guidance to a transfer of personal data to a jurisdiction outside the Bailiwick as a "**restricted transfer**".

WHAT YOU NEED TO THINK ABOUT:
This guidance sets out **seven steps** you need to consider when thinking about making a restricted transfer.

Please note that this guidance is inevitably quite technical, so please use the details on the ODPA 'Contact Us' page if you need help, or speak to your Data Protection Officer or legal advisor.

Step 1 – Know your transfers
Step 2 – Can you achieve your purpose without transferring personal data?
Step 3 – Is the recipient jurisdiction either (a) a Member State of the European Union or European Economic Area or (b) any country, any sector within a country, or any international organisation which the European Commission has found to be "adequate" for the purposes of the protection of personal data?
Step 4 - Are you putting in place one of the 'available safeguards' referred to in the Law?
Step 5 - Have you undertaken a 'Transfer Impact Assessment'?
Step 6 – Having undertaken a Transfer Impact Assessment, are you satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the Bailiwick data protection regime?

[1] 'data subjects' are *the living human beings* that any given set of personal data is *about* or *related to*.

Step 7 – Is the transfer otherwise authorised under the Law?

Step 1 – Know Your Transfers

One of the key things for any controller or processor to establish is what transfers it is *currently* making and those it *intends* to make. You are making a restricted transfer where **all** the following apply:

- **The Law applies to your processing**. The scope of the Law is set out in Section 2 of the Law which provides that the Law applies to the processing of personal data only where conditions A and B are satisfied.
    - **Condition A** is that –
        - the processing is wholly or partly by automated means;
        - if the processing is other than by automated means, the personal data forms or is intended to form part of a filing system.
    - **Condition B** is that –
        - the processing is in the context of a controller or processor established in the Bailiwick; **or**
        - the personal data is that of a Bailiwick resident, and it is processed in the context of:
            - the offering of goods or services (whether or not for payment) to the resident; or
            - the monitoring of the resident's behaviour in the Bailiwick.
- **You are sending personal data to a receiver outside the Bailiwick** – whilst there are some exceptions to this rule, sending personal data outside the Bailiwick will generally require you to consider the provisions of Part X of the Law. You should note that transferring personal data will include *making it available to access* from outside the Bailiwick – so if you enable remote access to your Bailiwick systems for someone in another jurisdiction and personal data becomes accessible as a result, this will constitute a transfer.
- **You are sending personal data to someone else –** for the transfer restrictions to apply, the receiver needs to be legally distinct from the Guernsey exporter of personal data – so it needs to be a separate company, organisation or individual. It should be noted that this *includes* a transfer to *another entity in the same corporate group*. However, if you are sending personal data to someone employed by you or by your company or organisation, this is *not* a restricted transfer. The transfer restrictions only apply if you are sending personal data *outside* your company or organisation.

Once you have identified whether a restricted transfer is taking place (or is proposed), you should document the parameters of the transfer, which jurisdiction the transfer is to and the nature of the recipient – and what you intend to transfer (or are already transferring)

Example 1: Controller in a third country collects data directly from a data subject in Guernsey

Martha, living in Guernsey, inserts her personal data by filling a form on an online clothing website in order to complete her order and receive the dress she bought online at her residence in Guernsey. The online clothing website is operated by a company established in Singapore with no presence in Guernsey. In this case, the data subject (Martha) passes her personal data to the Singaporean company, but this does not constitute a transfer of personal data since the data are not passed by an exporter (controller or processor), since they are passed directly and on her own initiative by the data subject herself. This is **not a restricted transfer and Part X Law does not apply**. Nevertheless, the Singaporean company will need to check whether its processing operations are subject to the Law.

Example 2: Controller in Guernsey sends data to a processor in a third country

Company X established in Guernsey, acting as controller, provides personal data of its employees or customers to a Company Z established in Mexico, which processes the data as processor on behalf of X. In this case, data are provided from a controller which, as regards the processing in question, is subject to the Law, to a processor in a third country. Hence, the provision of data will be considered as a transfer of personal data to a third country. This **is a restricted transfer and Part X of the Law applies.**

Example 3: Employee of a controller in Guernsey travels to a third country on a business trip

Alf, employee of A, a company based in Guernsey, travels to India for a meeting. During his stay in India, Alf turns on his computer and accesses remotely personal data on his company's databases to finish a memo. This remote access of personal data from a third country, does **not qualify as a transfer of personal data**, since Alf is not another controller, but an employee, and thus an integral part of the controller (company A). Therefore, the disclosure is carried out within the same controller (A). The processing, including the remote access and the processing activities carried out by Alf after the access, are performed by the Guernsey company, i.e. a controller established in Guernsey.

Step 2 – Can you achieve your purpose without transferring personal data?

Sending personal data to any recipient will entail a certain level of risk (although it is often the right thing to do).

Before making a restricted transfer you should consider whether you can achieve your aims without actually sending personal data (or making it available in the case of remote access).

Explore whether it is possible to make the data anonymous so that it is not possible to identify individual data subjects, as anonymous data is not personal data and therefore the Law's transfer restrictions will not apply, and you can make the transfer without restriction.

Anonymising data also accords with the third data protection principle (**data minimisation**) and the sixth data principle (**integrity and confidentiality (security)**).

Step 3 – Is the recipient jurisdiction either (a) a Member State of the European Union or European Economic Area or (b) any country, any sector within a country, or any international organisation which the European Commission has found to be "adequate" for the purposes of the protection of personal data?

You may make a restricted transfer if the receiver is located in a third country or territory or is an international organisation and is:

(a) within the European Union (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden) or a member of the European Economic Area (the EU Member States plus Iceland, Liechtenstein and Norway); or

(b) the recipient of a European Commission "adequacy" finding, which is a formal finding by the European Commission that the legal framework in that country, territory, sector or international organisation has been assessed as providing 'adequate' protection for individuals' rights and freedoms for their personal data. (Andorra, Argentina, Canada (commercial organisations), Faroe Islands, the Bailiwick of Guernsey, Israel, Isle of Man, Japan (private sector only), Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom and Uruguay).

It should be noted that:

- Japan – the adequacy finding only covers private sector organisations.
- Canada - the adequacy finding only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For more details please see the EU Commission's FAQs on the adequacy finding on the Canadian PIPEDA.

If the answer to the question at Step 3 is "Yes" then you do not need to go any further – you may make the transfer subject to the other provisions of the Law.

If the answer to the question at Step 3 is "No" then you should proceed to Step 4.

Step 4 - Are you putting in place one of the 'available safeguards' referred to in the Law?

If the answer to the question at Step 3 is "no" and you are (or are considering) transferring personal data to a country, any sector within a country, or any international organisation which is not on the list of adequate jurisdictions then you will need to consider one of the "**available safeguards**" referred to in the Law.

In order to utilise an available safeguard, you will generally need to undertake a 'Transfer Impact Assessment'.

There is a list of available safeguards in the Law. Each ensures that both you and the receiver of the restricted transfer are legally required to protect individuals' rights and freedoms in respect of their personal data. The key ones are as follows:

1. A legally binding and enforceable instrument between public authorities or bodies

You can make a restricted transfer if it is covered by a legal instrument between public authorities or bodies containing 'available safeguards'. The 'available safeguards' must include enforceable rights and effective remedies for the individuals whose personal data is transferred.

This agreement or legal instrument could also be entered into with an international organisation.

2. Binding Corporate Rules (BCRs)
The concept of using 'Binding Corporate Rules' (BCRs) to provide adequate safeguards for making restricted transfers was developed under EU law and is incorporated into the Law by Section 58.

BCRs are intended for use by multinational corporate groups, groups of undertakings or a group of enterprises engaged in a joint economic activity such as franchises, joint ventures or professional partnerships.

BCRs must be approved by a competent supervisory authority before they can be relied upon for transfers. The ODPA recognises BCRs approved by EEA data protection authorities and is empowered to approve BCRs submitted by local controllers. Schedule 4 of the Law outlines what needs to be covered in a set of BCRs submitted to the Authority for approval.

It is advisable to refer to the European Data Protection Board's guidance in relation to supplementary measures to accompany international transfer tools, as this will assist with the assessment of the jurisdiction's legal redress mechanisms.

3. Standard Data Protection Clauses, also known as standard contractual clauses ('SCCs') or model clauses
Standard data protection clauses contain contractual obligations on the data exporter (based in the Bailiwick) and the data importer (based outside the Bailiwick and the EEA) and rights for the individuals whose personal data is to be transferred. These clauses are approved by the European Commission, available on their website, and recognised by the ODPA for transfer purposes.

As a result of a case in the European Court of Justice in 2020, it is now necessary to ensure that the individuals whose data is transferred will be afforded legal redress in the jurisdiction of the data importer if their rights or freedoms are infringed. Controllers need to assess whether this is achievable and not enter into such an arrangement where such redress is not available.

A new set of SCCs have been approved by the European Commission under the auspices of the GDPR and taking on board the CJEU's "Schrems II" judgment that an assessment of legal redress is needed and should be used for any new contracts between data exporters and data importers.

Any Bailiwick business engaging in new transfers will need to utilise the new EU SCCs. If you are still utilising the previous EU SCCs for transfers the deadline to transfer these to the new EU SCCs is **27 December 2022**.

It is advisable to refer to the European Data Protection Board's guidance in relation to supplementary measures to accompany international transfer tools, as this will assist with the assessment of the jurisdiction's legal redress mechanisms.

For more information please see our more detailed technical update on SCCs.

Note: The Authority have produced a Bailiwick of Guernsey Addendum to the new EU SCCs which make them more appropriate for use under the Bailiwick Law.

4. An "approved code"
You can make a restricted transfer if the receiver has signed up to a code of conduct, which has been

approved by the Authority or by a Supervisory Authority in the EU. The code of conduct must include appropriate safeguards to protect the rights of individuals whose personal data is transferred, with a binding and enforceable commitment by the receiver to apply those appropriate safeguards.

No approved codes of conduct are yet in use, but any sector bodies and associations who wish to produce some should contact the Authority in the first instance for discussion.

5. An "Approved Mechanism"
You can make a restricted transfer if the receiver has a certification, under a mechanism approved by the Authority or by a Supervisory Authority in the EU. The certification mechanism must include appropriate safeguards to protect the rights of individuals whose personal data is transferred, with a binding and enforceable commitment by the receiver to apply those appropriate safeguards.

No such certification mechanisms exist at present, however, questions about this mechanism should be directed to the Authority.

6. Contract authorised by the Authority
You can make a restricted transfer if you and the receiver have entered into a bespoke contract governing a specific restricted transfer which has been individually authorised by the Authority.

This means that if you are making a restricted transfer from Guernsey, the Authority will have had to have approved the contract *before* it goes into effect.

If you want the Authority to consider such an arrangement, you should involve them at an early planning stage.

7. Administrative arrangements between public authorities or bodies
You can make a restricted transfer using an administrative arrangement (usually a document, such as a memorandum of understanding) between public authorities.

The administrative arrangement must set out which include enforceable and effective rights for data subject rights.

The administrative arrangement must be individually authorised by the Authority *before* it goes into operation.

Step 5 - Have you undertaken a 'Transfer Impact Assessment'?

When you are seeking to rely on an available safeguard you must still carry out a **'transfer impact assessment'**. This is to make sure that the *actual* protection provided by the available safeguard, given the actual circumstances of the restricted transfer, is sufficiently similar to the principles of the Law to provide data subjects of the transferred data with a level of protection **essentially equivalent** to that under the Law.

You should do this by undertaking a risk assessment, which takes into account the protections contained in that appropriate safeguard and the legal framework of the destination country (including laws governing public authority access to the data).

If your assessment is that the appropriate safeguard does not provide the required level of protection, you may include **additional measures**.

There is a template Transfer Impact Assessment and associated guidance available here.

Step 6 – Having undertaken a Transfer Impact Assessment, are you satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the Bailiwick data protection regime?

If **yes**, you can make the transfer.

If **no**, go to Step 7.

Step 7 – Is the transfer otherwise authorised under the Law?

If **Yes**, you can make the transfer. Please review the eight most common of the specific scenarios in which transfers are authorised by the Law listed below. Transfers using these scenarios should only be used in exception circumstances, and are not for regular transfers.

If **No**, you cannot make the transfer in accordance with the Law.

Scenario 1 – Court Orders

You may make a restricted transfer if you are required to make the transfer as a result of:

- an order or a judgment of a court or tribunal having the force of law in the Bailiwick;
- a decision of a public authority of the Bailiwick based on an international agreement imposing an international obligation on the Bailiwick; or
- where the order has the force of law in the Bailiwick, and is based on an international agreement imposing an international obligation on the Bailiwick:
    - an order or a judgment of a court or tribunal of a country other than the Bailiwick; or
    - a decision of a public authority of any country other than the Bailiwick.

Scenario 2 - Explicit Consent of the Data Subject

'**Explicit consent**' can be used to make a restricted transfer provided you meet all these conditions: the data subject must be able to consent freely, only to specific processing, via an affirmative (opt-in) mechanism, which must be unambiguous, and the data subject must be able to be withdraw this consent at any time. Explicit consent has the same requirements as consent, with the extra safeguard that it must be conveyed in an express written statement. For example, through a signed written statement, or by filling in an electronic form, or by sending an email.

Note: 'Consent' and 'Explicit Consent' are different to each other in ways that are difficult to summarise. But in essence it boils down to the difference between actions the person may take to indicate their consent, and a written statement where they give their explicit consent.

As a valid explicit consent must be both **specific** and **informed**, you must provide the individual with *precise* details about the restricted transfer. You cannot obtain a valid consent for restricted *transfers in general*.

You should tell the individual:

- the identity of the receiver, or the categories of receiver;
- the country or countries to which the data is to be transferred;
- why you need to make a restricted transfer;
- the type of data that will be transferred;

- that they can withdraw consent; and
- the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other appropriate safeguards[2] in place. For example, you might explain that there will be no local supervisory authority, and no (or only limited) individual data protection or privacy rights.

Given the high threshold for a valid explicit consent, and that it can be withdrawn at any time this may mean that it is not advisable to rely on it where an alternative exists.

Public authorities are not permitted to transfer to unauthorised jurisdictions using explicit consent.

Scenario 3: Contract with the data subject or for the benefit of the data subject

You may make a transfer where necessary:

- for the conclusion or performance of a contract –
  - to which the data subject is a party; or
  - made between the controller and a third party in the interest of the data subject;
- to take steps at the request of the data subject prior to entering into such a contract.

The transfer must be **necessary**, (i.e. you *cannot perform the core purpose* of the contract or the core purpose of the steps needed to enter into the contract, *without* making the restricted transfer).

For example, this does not cover a transfer for you to use a cloud-based IT system.

Public authorities cannot rely on contracts with data subjects to make transfers.

Scenario 4: Legal Proceedings or Legal Advice

You may make a restricted transfer where necessary:

- for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
- for the purpose of obtaining legal advice; or
- otherwise for the purposes of establishing, exercising or defending legal rights.

The transfer must be **necessary**, so there must be a close connection between the need for the transfer and the relevant legal claim and/or the advice.

A claim must have a basis in law, and a formal legally defined process, but it is not just judicial or administrative procedures. This means that you can interpret what is a legal claim quite widely, to cover, for example:

- all judicial legal claims, in civil law (including contract law) and criminal law. The court procedure does not need to have been started, and it covers out-of-court procedures. It covers formal pre-trial discovery procedures.

[2] For available safeguards see: Step 4 of this document.

- administrative or regulatory procedures, such as to defend an investigation (or potential investigation) in competition law or financial services regulation, or to seek approval for a merger.

You **cannot** make a restricted transfer on the basis that there is a *possibility* that a legal claim or other formal proceedings may be brought in the future. It could be possible to use this scenario when seeking legal advice and the justification for doing so should be documented. You may wish to speak to your legal advisor for their guidance on this point.

Public authorities can make restricted transfers on this basis, in relation to the exercise of their powers.

Scenario 5: You need to make the restricted transfer to protect the vital interests of the data subject or another individual.

This applies in a medical emergency where the transfer is needed in order to give the medical care required or in an equivalent situation where the vital interests of the individual are engaged. **"Vital interests"** are defined in the Law as (in relation to any individual) including the life, health or safety of the individual. The imminent risk of serious harm to the individual must outweigh any data protection concerns.

You cannot rely on this scenario to carry out *general* medical research.

If the individual is physically and legally capable of giving consent, then you cannot rely on this scenario unless you can demonstrate that you *cannot be reasonably expected to obtain* such consent.

Scenario 6: You are making the restricted transfer from a public register.

The register must be created under Bailiwick law and must be open to either:

- the public in general; or
- any person who fulfils conditions set down in law for such access.

For example, registers of companies, associations, land registers or public vehicle registers. The whole of the register cannot be transferred, nor whole categories of personal data.

The transfer must comply with any general laws which apply to disclosures from the register.

Scenario 7: you are making a one-off (or a non-repetitive) restricted transfer and it is in your compelling legitimate interests.

If you cannot rely on any of the other scenarios, there is one other scenario to consider. This should not be relied on lightly and never routinely as it is only for exceptional circumstances.

For this scenario to apply to your restricted transfer:

- You are unable to use any of the other appropriate safeguards. You must give serious consideration to this.
- None of the other scenarios outlined above apply. Again, you must give this serious consideration. It may be that you can obtain explicit consent with some effort or investment.
- Your transfer must not be repetitive – that is it may happen more than once but not regularly or routinely.

- The personal data must only relate to a limited number of individuals. There is no absolute threshold for this. The number of individuals involved should be part of the balancing exercise you must undertake below.
- The transfer must be necessary for your compelling legitimate interests. Demonstrating such interests is a similar exercise to identifying and documenting lawful processing based on legitimate interests but a higher standard applies – the legitimate interests must be "compelling". An example is a transfer of personal data to protect a company's IT systems from serious immediate harm. You must document the compelling legitimate interests which you identify.
- On balance your compelling legitimate interests outweigh the rights and freedoms of the individuals. You must document this balancing exercise.
- You have made a full assessment of the circumstances surrounding the transfer and provided suitable safeguards to protect the personal data. Suitable safeguards might be strict confidentiality agreements, a requirement for data to be deleted soon after transfer, technical controls to prevent the use of the data for other purposes, or sending pseudonymised or encrypted data. This must be recorded in full in your records of your processing activities.
- You have informed the Authority of the transfer. You will be asked to provide full details of all the steps you have taken as set out above.
- You have informed the individual of the transfer and explained your compelling legitimate interest to them.

Scenario 8: Where you are authorised to make a transfer by regulations made in the public interest.
The Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018 permit certain transfers made by Guernsey Financial Services Commission or the International Stock Exchange.

Conclusion

If after following the seven steps detailed above you find that none of the circumstances fit, and/or you would like to talk to the Authority about a transfer please visit the ODPA 'Contact Us' page. You can speak to a member of staff over the phone (anonymously, if needs be) or you can attend one of the regular in-person drop-in sessions.