JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

GUIDANCE NOTE

International Transfers

Transfers of personal data to third countries and international organizations.

DEC 2022 • V4.1 • WWW.JERSEYOIC.ORG

OVERVIEW

Flows of personal data to and from the European Union (the **EU**) (including Iceland, Liechtenstein and Norway who are members of the European Economic Area) and to other countries with an adequacy decision from the European Commission (including the UK) are essential for Jersey in terms of international trade and international co-operation.

Transfers to third countries (any country or territory outside the 'EEA') are restricted unless the rights of individuals are protected in another or, one of a limited number of exceptions applies and must be done in full compliance with Part 8 of the Data Protection (Jersey) Law 2018 (the **DPJL 2018**).

However, the transfer of such personal data from Jersey to controllers and processors located in third countries must not undermine the level of protection of the individuals concerned as individuals risk losing the protection of Jersey data protection laws if their personal data is transferred outside of Jersey.

These types of transfer are commonly referred to as a "restricted transfer" and that is how they will be referred to in this guidance note.

This guidance note provides summary guidance on the provisions in Part 8 of the DPJL 2018, as well as links to more detailed information and guidance, about what you must consider when deciding whether to make a restricted transfer.

COMMON DEFINITIONS

Adequacy:	a jurisdiction that has been awarded adequacy status by the European Commission (i.e. a jurisdiction that has been found to offer an equivalent level of protection to that afforded by European data protection legislation
BCRs:	binding corporate rules (i.e. internal guidelines used by international companies setting out how the group will approach data protection matters and which have been approved by a data protection supervisory authority
Data exporter:	the entity sending/transferring the personal data
Exceptions:	these are the exceptions to the adequacy requirements or appropriate safeguards i.e. the other ways in which a controller is allowed to make a restricted transfer and as set out in Schedule 3 of the DPJL 2018
Data importer:	the entity ultimately receiving the personal data from the data exporter
Restricted transfer:	a transfer of personal data from Jersey to a third country that falls within scope of Art.66 of the DPJL 2018
SCCs:	standard contractual clauses issued by the European Commission
Third country:	a country outside of the EEA

DO I NEED TO MAKE A "RESTRICTED TRANSFER"?

One question to ask before making any transfer under Art.66 of the DPJL 2018 is whether there are any alternatives to sending the data out of Jersey.

A controller/processor engaging in an international transfer must always be able to demonstrate why they consider it necessary to deal with data in a particular way and so will need to justify why personal data needs to be sent off-island. This decision making should be carefully documented.

You may wish to consider the following alternatives:

1. Can you anonymise the data before it is sent? If that is possible, then the data to be transferred will no longer fall within the definition of 'personal data' and so the DPJL 2018 will not apply to it. (You must be able to anonymise the data completely; if it can only be pseudonymized the DPJL 2018 will continue to apply to it and you will need to comply with the requirements of Art.66.)

2. Do you actually need to transfer the data at all? The DPJL 2018 requires controllers to apply to the principle of data minimization i.e. to minimize the extent to which personal data is processed and to have processes in place that are proportionate for the purposes of processing.

3. Could you use a supplier based in Jersey instead?

AM I MAKING A "RESTRICTED TRANSFER"?

A transfer of personal data falls within the definition of 'processing' under the DPJL 2018:

> *"means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*

You will be making a restricted transfer if:

1. The DPJL 2018 applies to the processing of the personal data you are transferring

2. You will be sending personal data, or making it accessible, to an entity (the data importer) which is located in a third country (including by allowing the data importer remote access to your systems/storage locations in Jersey)

3. The data importer is legally distinct from you i.e. it is a separate company (including a company within the same corporate group), organisation or individual.

If you are sending data to someone employed by your organization, this will not count as a restricted transfer even if they are situated in a so-called third country.

If information simply transits through a third country (e.g. passes through servers to an end recipient), so long as the end recipient is not in a third country, this will not count as a restricted transfer. For data to be classed as 'in transit' only, it must not be accessed or manipulated in any way whilst in transit.

Transfer restrictions apply to transfers from both controllers and processors and both to an initial transfer, and to any onward transfers i.e. it applies if personal data is transferred from Jersey to a country in the EEA and then onward transferred to a further recipient in a third country.

Example

Jersey Company A has an employee located in America. The employee logs onto Jersey Company A's cloud servers that are hosted in Jersey. This is not a restricted transfer.

Example

Jersey Company A owns Company B, which is incorporated in Australia. They each have their own servers in their respective jurisdictions. Company A has a client who wants to do some work with Company B and so Company A needs to send certain information about that client to Company B. Even though Company A and Company B are part of the same corporate group, because Company A is a separate legal entity in a third country, any transfer of the client's information would be classed as a restricted transfer.

Example

Jersey Company A needs to send some information to Guernsey Company A and is going to route the information through its servers in China. This is not a restricted transfer.

ARTICLE 66

Article 66 of the DPJL 2018 sets out the three ways data controllers can make a restricted transfer;

- Adequacy.
- Appropriate safeguards (See Article 67 of the DPJL 2018).
- Schedule 3 exceptions (see Schedule 3 of the DPJL 2018).

Transfers on the basis of an adequacy decision

What is 'adequacy'

An adequacy decision means that the European Commission has decided that a third country ensures an adequate level of data protection to those within the European Union.

The Bailiwick of Jersey is a third country itself (being a Crown Dependency territory outside the EEA) and it enjoys 'adequacy' status as a result of a decision of the **European Commission dated 8 May 2008.**

When assessing adequacy and level of protection afforded by the third country territory, the European Commission takes into account elements such as the laws, respect for human rights and freedoms, national security, data protection rules, the existence of a data protection authority and binding commitments entered into by the country in respect of data protection.

The adoption of an adequacy decision involves:

- A proposal from the European Commission;
- An opinion of the European Data Protection Board (**EDPB**);
- An approval from representatives of EU countries; and
- The adoption of the decision by the European Commissioners.

The effect of such a decision is that personal data can flow from the EEA to that third country, or vice versa, without any further safeguard being necessary. In other words, it's classed as if the transfer was carried out within the EU itself.

A list of countries with an adequacy decision can be found **here**. The European Commission can revoke adequacy decisions and the European Court of Justice can also strike down adequacy decisions previously granted so it is important to check the list of adequate jurisdictions, in case of any changes.

Can I transfer data to a country with 'adequacy' status

Yes.

Are there any additional safeguards I need to put in place before I transfer information to a country with adequacy?

No; if a jurisdiction is "adequate" for the purposes of Art.66 of the DPJL 2018 you can make the transfer without putting in place any of the other safeguards mentioned in that article (NB if you a transferring to Canada it only has partial adequacy status relating to data that is subject to Canada's Personal Information and Electronic Documents Act (**PIPEDA**) – not all data is – so you will need to check the intended recipient of the data and whether it falls within the scope of the adequacy assessment. Similarly, Japan's adequacy finding only covers private organizations).

However, you must remember that even if you are sharing data to an entity in a country with adequacy, you must still comply with the DPJL 2018. You should:

- Think about whether the sharing of the data in this way is actually necessary (or could you achieve the same outcome without transferring the data?)
- Have a lawful basis for the data sharing
- Be transparent about the data sharing (you may need to review your privacy policy, for example)
- Consider whether a formal data sharing agreement is necessary/desirable and if you already have such an agreement in place, check whether it needs updating
- Make sure the data sharing takes place in a safe and secure way (including being satisfied that the data will be dealt with securely by the data importer)

ARTICLE 67

Transfers subject to appropriate safeguards

In the absence of an adequacy decision, the DPJL 2018 also allows a restricted transfer to take place if the controller or processor has provided 'appropriate safeguards' and on condition that enforceable data subject rights and effective legal remedies for data subjects comparable to those under the DPJL 2018 are available in that third country or organisation.

In practice, this means that data subjects should have essentially equivalent protection in the country to which the data is being transferred i.e. the ability to enforce their rights and have access to a regulatory authority and a court system.

There is a list of appropriate safeguards set out at Art.67 of the DPJL 2018:

- **Standard data protection clauses:** For the majority of organizations, the most relevant alternative legal basis to an adequacy decision would be these clauses, also known as 'Standard Contractual Clauses' or 'SCCs'. They are model data protection clauses that have been **approved by the European Commission** and enable the free flow of personal data when embedded in a contract. The clauses contain contractual obligations on the Data Exporter (the sender of the information) and the Data Importer (organisation receiving the information), and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the Data Importer and the Data Exporter.

  The Jersey Data Protection Authority has formally adopted the **updated SCCs** and issued a Jersey addendum.

  If you wish to rely on SCCs to make a restricted transfer from Jersey you MUST include the Jersey Addendum as part of your contract.

  If your agreement is intended to govern transfers under the GDPR and the DPJL 2018, you should make it clear that the terms of the Jersey Addendum apply only to transfers governed by the DPJL 2018.

  (Please note that UK International Data Transfer Agreements do not fall within the scope of Art.66 and are not recognised as an 'appropriate safeguard' in this context)

- **Binding corporate rules 'BCRs'**: BCRs form a legally binding internal code of conduct operating within a multinational group, which applies to transfers of personal data from the group's Jersey entities to the group's non-EEA entities. This group may be a corporate group, or a group of undertakings engaged in a joint economic activity, such as franchises or joint ventures.

  BCRs are legally binding data protection rules with enforceable data subject rights contained in them, which are approved by the Jersey Data Protection Authority or another competent supervisory authoriy under Article 46 of the GDPR.

  There are two types of BCRs which can be approved – BCRs for Controllers which are used by the group entity to transfer data that they have responsibility for such as employee or supplier data; and BCRs for Processors which are used by entities acting as processors for other controllers and are normally added as an addendum to the Service Level Agreement or Processor contract.

  Further provisions on the use of BCRs as an appropriate safeguard for personal data transfers are set out in **Schedule 4** of the DPJL 2018.

- **Approved Codes of Conduct:** The use of Codes of Conduct as a transfer tool, under specific circumstances, has been introduced by the Article 67(d) of the DPJL 2018.

  (d) A code or any other code approved by another competent supervisory authority under Article 40 of the GDPR or equivalent statutory provisions, together with binding and enforceable commitments of the controller, processor or recipient in the third country or international organization to apply the appropriate safeguards, including as regards data subjects' right.

  Codes are voluntary and set out specific data protection rules for categories of controllers and processors. They can be a useful and effective accountability tool, providing a detailed description of what is the most appropriate, legal and ethical behaviour within a sector.

  From a data protection viewpoint, codes can therefore operate as a rulebook for controllers and processors who design and implement compliant data processing activities that give operational meaning to the principles of data protection set out in local, European and national law.

- Approved certification mechanisms: There is no definition of certification in the DPJL 2018. Certification is defined by the International Organisation for Standardization (ISO) as 'the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements'.

  Article 80 of the Data Protection (Jersey) Law 2018. Regulations establishing certification mechanism; Regulations may provide for the establishment of mechanisms, seals or marks to certify or signify –

  (a) that particular processing operations by controllers or processors comply with this Law; or

  (b) the existence of appropriate safeguards for the protection of personal data provided by controllers or processors established in a third country for the purposes of personal data transfers to third countries or international organizations as provided for by Article 66.

  Therefore, as introduced in Article 80 of the DPJL 2018, certification mechanisms may be developed to demonstrate the existence of appropriate safeguards provided by controllers and processors in third countries but no Regulations have yet been put in place by the States of Jersey.

  These controllers and processors would also make binding and enforceable commitments to apply the safeguards including provisions for data subject rights.

- **A legally binding and enforceable instrument between public authorities or bodies:** An organisation can make a restricted transfer if it is a public authority or body and is transferring to another public authority or body, and with both public authorities having signed a contract or another instrument that is legally binding and enforceable **(Article 67 (1) of the DPJL 2018).**

  This contract or instrument must include enforceable rights and effective remedies for individuals whose personal data is transferred. This is not an appropriate safeguard if either the transferring organisation or the receiver is a private body or an individual.

  If a public authority or body does not have the power to enter into legally binding and enforceable arrangements, it may consider an **administrative arrangement** that includes enforceable and effective individual rights instead **(Article 67(3)(b) of the DPJL 2018).**

  The above methods of transfer do not require any specific authorization from the Jersey Data Protection Authority at point of transfer.

What do I need to do if I want to rely on an 'appropriate safeguard'?

Before you can rely on any of the above appropriate safeguards, you must be satisfied that the data subjects of the data you want to transfer continue to have a level of protection in the country of the anticipated recipient which is essentially equivalent to the DPJL 2018.

You should work this out by carrying out a risk assessment relating to the proposed transfer and this is sometimes referred to as a "transfer impact assessment" (**TIA**) or "transfer risk assessment" (**TRA**). We will refer to TIAs in this guidance note.

What is a TIA?

A TIA will help you ensure that when you make a restricted transfer, you do so in a way that provides appropriate safeguards in respect of individual's data and provides them with effective and enforceable rights.

By completing a TIA this will help you to consider all the circumstances of the restricted transfer, the apparent risks that present in the country to which you are transferring the data and what safeguards will be in place to protect the interests of affected data subjects and the information being transferred.

How do I undertake a transfer impact assessment?

We have produced a TIA checklist at the end of this document to help you focus on the things you need to consider when deciding whether to make a restricted transfer.

You will need to consider:

1. Risks to individual rights in the importing country including whether their information could be subject to access by third parties e.g. government agencies or police authorities;
2. Risks to individuals regarding their ability to effectively enforce their rights e.g access to legal advice, an effective court/tribunal system etc.

You should go through each of the questions to assess the risk of transferring the data to the third country and once you've assessed the level of risk, you should consider whether there are any additional safeguards that need to be put in place to reduce the risks you've identified.

You should document your analysis and make sure that you keep details of this should you ever need to explain to the JOIC why you sent information to a particular place. Whilst the JOIC may not ultimately agree that a transfer should have been made, the fact that you carried out a thorough and careful risk analysis would be taken into account by the JOIC when deciding upon any enforcement action.

The European Data Protection Board (**EDPB**) has published a document on supplementary measures which deals with transfers, transfer impact assessments and supplementary measures you may wish to consider putting in place.

What other safeguards can I put in place?

Any safeguards should address and be able to minimise the risks identified: what is the worst that could happen if the data is breached and what can be put in place to either reduce the chances of a breach occurring or to ensure that if a breach does occur, any impact on affected data subjects are minimised?

The type of safeguard that is appropriate will depend on the nature of the data being transferred i.e. basic information such as a name and an email address may not need the same level of protection as full identifying and financial details about an individual, or medical records.

You could deploy additional technical controls e.g. password protection of the data (keeping password separate to the data itself), encryption or pseudonymization and/or you could put in place additional contractual obligations such as mandating that the importer submit to regular testing from a third party.

So, can I make the restricted transfer?

Ultimately, you can make the restricted transfer if:

1. You're satisfied that the third country/international organization offers data subjects an essentially equivalent level of protection to their rights under Jersey law;
2. The transfer is not high risk/complex;
3. You're satisfied that you will be able to enforce any contractual provisions against the data importer, should you need to and will have access to a legal system that allows this and to courts that can make appropriate orders/give appropriate remedies;
4. Any identified risks have been identified and minimised to the extent possible and any residual risks to data subjects are low.

What if the restricted transfer is not covered by appropriate safeguards?

If the restricted transfer is not covered by appropriate safeguards, then you need to consider whether the restricted transfer is covered by an exception set out in Schedule 3 of the DPJL 2018.

SCHEDULE 3

Exceptions to adequacy requirements

Schedule 3 of the DPJL 2018 provides exceptions from the general principle that personal data may only be transferred to a third country if an adequate level of protection is provided for in that third country.

A Data Exporter (should first endeavour to frame transfers with one of the mechanisms guaranteeing adequate safeguards listed above, and only in their absence seek to utilise one of the exceptions provided in **Schedule 3 of the DPJL 2018.**

These exceptions allow transfers in specific situations. Full details can be found in Schedule 3 of the DPJL 2018, but in summary are listed below:

- Court Order, or order from a Public Authority outside of Jersey;
- Explicit consent from data subject;
    - » Valid consent must be freely given, specific and informed. That means that a data subject must be given explicit and precise details about the intended restricted transfer.
      * Specifically, the data subject must be told:
        - » Who will be receiving their information
        - » Where the data is being transferred to and the risks of the receiving jurisdiction in relation to the provision of data protection.
        - » Why the restricted transfer needs to be made
        - » What data is to be transferred
        - » That they can withdraw their consent at any time (although this may mean that depending on the reason for the transfer, that consent is not an appropriate basis for making the restricted transfer).
- Contract between a data subject or a Controller or third-party contract in the interest of the data subject; The DPJL 2018 says that the transfer must be **necessary**. This means that unless you are able to make the restricted transfer, you will not be able to fulfil the obligations of the contract.
- Transfer on behalf of the Jersey Financial Services Commission ('**JFSC**');
- Transfers necessary for the purpose of legal proceedings, obtaining of legal advice and establishing, exercising or defending legal rights;
- Transfers necessary to protect the vital interests of the data subject or any other person;
    - » In these circumstances, the person whose vital interests you are intending to protect must not be capable (i.e. not have the physical ability or mental capacity) to give their consent to the transfer. A transfer under this provision would usually only be appropriate in a medical emergency and where the imminent risk of serious harm outweighs the data protection rights of the individual.
- Transfers of information from a public register.

In all cases where transfers are made under the exceptions in Schedule 3, a full assessment must be carried out and documented.

There is one final exception available if the restricted transfer cannot take place under any other provision of the DPJL 2018. This exception should only be relied upon in truly exceptional circumstances and must be:

a. Not repetitive (it can happen more than once, but must be occasional rather than routine).

b. Limited number of data subjects.

Necessary for purposes if compelling legitimate interests pursued by the data controller, which are not overridden by the interest rights and freedoms of data subjects.

In addition the Controller must have assessed all the circumstances where the transfer is to take place under this paragraph and must inform the Authority of the transfer as soon as practicable. We will ask to see full details of all the steps you have taken in deciding why it was necessary to make the restricted transfer under this provision. You must also tell the data subject about the transfer and of the compelling legitimate interests pursued.

The EDPB **guidance** document on these derogations should always be consulted to ensure that they could be relied upon for the specific scenarios that organizations are dealing with.

TRANSFER IMPACT ASSESSMENTS CHECKLIST

A: Questions about the transfer

1. Who are the parties to the restricted transfer

a. Who is the data exporter (the one sending the information)?

b. Who is the data importer (the one receiving the information)?

   i. What type of organization are they (e.g. Government, third party or inter-company/within the same group of companies)?

   ii. Where are they located?

   iii. What is their reputation? Are they reputable and/or long-established e.g. an international banking entity or IT provider.

   iv. Are they a controller, processor, joint-controller or sub-processor?

   v. Is the importer going to be sharing that information with anyone else?

   vi. If so, who, why and where are they located?

   vii. Is the importer subject to any professional standards/code of conduct e.g. accountant, lawyer, medic?

2. Details of proposed restricted transfer

a. What is the purpose of the transfer? Why is the data being transferred?

b. What will the importer be doing with the data?

c. What data is being transferred?

   i. Does this include special category data?

   ii. How much data is being transferred?

   iii. With what frequency?

   iv. Is it about children or vulnerable individuals?

d. What technological and organisational security measures does the importer have in place to ensure the security of the data entrusted to it? Do you have evidence of these measures being in place?

e. Will the data be secure in transit and how is it being transferred? Is it by secure access into data held in Jersey, by email, or by secure download link for example?

f. What format will the data be in whilst in transit e.g. will it be pseudonymization/encrypted?

3. What is your lawful basis for transferring the personal data (Sched 2 Part 1 of the DPJL 2018)?

- ☐ Consent
- ☐ Contractual performance
- ☐ Compliance with a legal obligation
- ☐ Vital interests
- ☐ Performance of a task carried out in the public interest or exercise of official authority
- ☐ Legitimate interests

If you're relying on legitimate interests have you carried out a legitimate interest assessment? (If not, you will need to do one BEFORE completing the transfer impact assessment.)

If you are transferring special category data, what is your lawful basis (Sched 2 Part 2 of the DPJL 2018)

- ☐ Explicit consent
- ☐ Other legal obligations
- ☐ Employment and social fields
- ☐ Vital interests
- ☐ Non-profit associations
- ☐ Information made public
- ☐ Legal proceedings, etc.
- ☐ Public functions
- ☐ Public interest
- ☐ Medical purposes
- ☐ Public health
- ☐ Archiving and research
- ☐ Avoidance of discrimination
- ☐ Prevention of unlawful acts
- ☐ Protections against malpractice and mismanagement
- ☐ Counselling
- ☐ Insurance and pensions

4. What safeguards are in place in the third country

a. Does the third country have a dedicated data protection/privacy law in force at the proposed time of transfer? If so;
    i. Is it based on a data protection law/regime from another country e.g. is it based on GDPR
    ii. Is there evidence of it being followed/applied/enforced in practice?

b. Is there an appropriate data protection regulatory authority in place in the third country?
    i. If so, does that authority have appropriate powers of enforcement?
    ii. Is it able to deal with complaints from data subjects about how their personal data has been handled by organizations in that country?
    iii. Can it deal with complaints against all sectors i.e. Governmental and private sector? Would it be able to deal with a complaint against the data importer.
    iv. What does their enforcement/sanction regime look like? Can they order remedial action, take enforcement action and/or issue fines, for example?
    v. Is there evidence of the regulatory authority actually utilising its powers and carrying out its mandated functions?

c. Can you enforce any contractual obligations between you and the importer in the third country?
    i. Is there an established legal system and access to court process?
    ii. How easy is it for those overseas to:
        - Access relevant legal advice
        - Access the court system including to initiate proceedings/seek enforcement of foreign judgments
    iii. Are any judgments robust? Do they provide effective remedies and are they capable of being enforced?
    iv. Are there any current circumstances making court access/enforcement difficult/unlikely e.g. war/civil unrest?

d. Do data subjects have rights under local data protection legislation essentially equivalent to those provided for under the DPJL 2018 e.g. rights of access, rectification, erasure?
    i. If so, what can they do if their rights have been breached and who can they complain to?
    ii. Is there evidence of those complaints being dealt with?

e. Are there any surveillance regimes in the third country that may impact on the data subject whose information is being transferred?
    i. If so, what rights do data subjects have in those circumstances?
    ii. Are there any rules in place relating to the exercise of those surveillance powers? If so, what are they and who has oversight.
    iii. Could the information subject to the restricted transfer be of potential interest to surveillance authorities?

f. Are there any human rights issues that you need to take into account e.g. could the transfer increase the risk for people of a human rights breach in the country of the importer? What are the human rights that could be infringed and what would the likely impact of that breach be on the affected individual?The key human rights you may want to consider are:

- Right to life
- Prohibition of torture
- Prohibition of slavery and forced labour
- Right to liberty and security
- Right to a fair trial
- Right to marry
- Right to be an effective remedy
- No discrimination

CONCLUSION

It is important to bear in mind that SCCs (and indeed any of the other mechanisms used to facilitate the lawful transfer of data out of Jersey) are not an end in themselves. Care is required to ensure that, operationally, transfers are conducted and managed in a way that ensures that personal data is at all times protected to the level contemplated by the DPJL 2018 and that the obligations assumed by the parties under the terms of their SCCs contract are in fact discharged in practice. Like all other elements of the data processing arrangements of a business, planning is required to ensure compliance with the requirements of the DPJL 2018 generally.

MORE INFORMATION

Should you have any questions on this guidance or require further information, please visit our website, or contact the Jersey Office of the Information Commissioner:

Jersey Office of the Information Commissioner
2nd Floor
5 Castle Street
St Helier
Jersey JE2 3BT

Telephone number: +44 (0) 1534 716530
Email: enquiries@jerseyoic.org