INTRODUCTION
1. The DPJL is based around six principles of 'good information handling'. These principles give people (the data subjects) specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

2. The Data Protection Authority (Jersey) Law 2018 (AL) establishes the Data Protection Authority (the Authority) which will replace the Office of the Information Commissioner. The Information Commissioner (the Commissioner) is the Chief Executive Officer of the Authority.

3. This is part of a series of guidance to help organisations fully understand their obligations, as well as to promote good practice.

GUIDANCE NOTE

International Transfers

Transfers of personal data to the European Union, third countries and international organisations.

This document is purely for guidance and does not constitute legal advice or legal analysis. It is intended as a starting point only, and organisations may need to seek independent legal advice.
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 are essential for Jersey in terms of international trade and international co-operation.

However, the transfer of such personal data from Jersey to the EU and to controllers and processors located outside the EU in third countries should not undermine the level of protection of the individuals concerned.

A third country is defined as any country or territory outside the ‘EEA’. Therefore, transfers to third countries or international organisations outside this area should be done in full compliance with Part 8 of the Data Protection (Jersey) Law 2018 (the ‘Law’).

The Bailiwick of Jersey is a Crown Dependency territory outside the EEA and is therefore technically categorised as a third country itself albeit that it enjoys ‘adequacy’ status as a result of a decision of the European Commission dated 8 May 2008. (Countries with ‘adequacy’ status are deemed to provide essentially equivalent levels of protection in data protection terms to those within the EU and data may be sent to Jersey from an EU country without the need for further measure or restrictions.)

This document provides summary guidance on the provisions in Part 8 of the Law, as well as links to more detailed information and guidance, about what you must consider when deciding whether to transfer personal data from Jersey to another jurisdiction.
ARTICLE 66

Transfers on the basis of an adequacy decision

Article 66 sets out the three ways data controllers can transfer personal information into a third country;

• Adequacy.
• Appropriate safeguards (See Article 67).
• Schedule 3 exceptions (see Schedule 3).

Firstly, consider when transferring personal data to a third country whether there is an ‘adequacy decision’ in place for that country. An adequacy decision means that the European Commission has decided that a third country or an international organisation ensures an adequate level of data protection to those within the European Union.

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, the transfer is the same as if it was carried out within the EU.

A list of countries with an adequacy decision can be found here.
ARTICLE 67

Transfers subject to appropriate safeguards

In the absence of an adequacy decision, the Law also allows a transfer to a third country 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 Law are available in that third country or organisation. These safeguards may include:

- **Standard data protection clauses**: For the majority of organisations, 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.

Currently, there are two sets of **standard contractual clauses** for restricted transfers between a controller and controller, and one set between a controller and processor.

The European Commission has advised the European Data Protection Board (EDPB) that it plans to update the existing standard contractual clauses for the General Data Protection Regulation (GDPR) and an updated set of SCCs are currently out for consultation and may be found [here]. Until then, EU-based data controllers can still enter into contracts that include the standard contractual clauses based on the EU Directive 95/46/EC, which pre-dates the GDPR. This guidance note will be updated in due course.

(*Please see the additional note at the end of this guidance regarding transfers to the US post-Schrems II, and to the UK post-Brexit transitional period*)

- **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 (‘the Authority’). There are two types of BCRs which can be approved - BCR for Controllers which are used by the group entity to transfer data that they have responsibility for such as employee or supplier data; and BCR 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 Law.
**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 Law.

(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 Law. 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 organisations as provided for by Article 66.

Therefore, as introduced in Article 80 of the Law, 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 Law).

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 Law).

The above methods of transfer do not require any specific authorisation from the Jersey Data Protection Authority at point of transfer.
**SCHEDULE 3**

**Exceptions to adequacy requirements**

**Schedule 3** of the Law 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 (the entity transmitting the data from Jersey) should first endeavour to frame transfers with one of the mechanisms guaranteeing adequate safeguards listed above, and only in their absence use the exceptions provided in **Schedule 3 of the Law**.

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

- Court Order, or order from a Public Authority outside of Jersey;
- Explicit consent from data subject;
  - Must be freely given.
  - Must be informed.
  - The data subject must be made aware of the risks of the receiving jurisdiction in relation to the provision of data protection.
  - Article 11 of the DPJL covers consent.
- Contract between a data subject and a Controller;
- Third-party contract in the interest of the data subject;
- 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;
- 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.

It is also possible to transfer to a third country organisation if it cannot take place under any other provision of the DPJL, if:

a. Not repetitive.

b. Limited number of data subjects.

c. 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.

d. Controller has assessed all the circumstances where the transfer is to take place under this paragraph must inform the Authority of the transfer as soon as practicable.

The EDPB guidance document on these derogations should always be consulted to ensure that they could be relied upon for the specific scenarios that organisations are dealing with.
Additional guidance following the CJEU invalidation of the EU-US Privacy Shield mechanism

Background

In August 2020, the Court of Justice of the European Union (CJEU) (in what is known as the ‘Schrems II’ judgment) invalidated the EU-US Privacy Shield mechanism for data transfers between the EU and the US. Given the invalidation of this transfer mechanism, this may cause issues for Jersey organisations that had been using the Privacy Shield to transfer personal data to the US, or use Processors based in the US.

The EU-US Privacy Shield, however, is not the only mechanism for transfers of personal data. Other mechanisms may be available to Jersey-based Controllers and Processors who are, or are considering transferring personal data to the US.

What does this mean for local businesses?

Privacy Shield:

The CJEU found that domestic laws in the US dealing with access and use of personal data by US authorities to the data they hold does not provide sufficient protection of that data in line with GDPR requirements. Their biggest concern was in respect of the lack of protection for non-US individuals who may be targeted by US Government surveillance programmes, and the potential lack of recourse of those individuals against those US authorities.

The CJEU judgment means it is therefore no longer acceptable to use the Privacy Shield as a data transfer mechanism for transfers of personal data between the EU and the US. Given that the Law is based on the GDPR, and aims to offer an essentially equivalent standard of protection, the Authority will unlikely consider that transfers based on the Privacy Shield mechanism alone are lawful.

Standard Contractual Clauses (‘SCCs’):

Firstly, SCCs are not directly binding on Jersey-based businesses receiving personal data as part of a data transfer. However, their validity will be assessed on their ability to ensure compliance with the Law, which is based upon the provisions of the GDPR. As long as the levels of protection afforded in the agreement meet that standard, then the likelihood is the SCCs will be considered, on the face of it, a valid mechanism for transferring personal data.

Notwithstanding the above, transfers will need to be assessed on a case-by-case basis and must examine any surveillance regime that the recipient company may be subject to. It is worth noting that you will need to look at whether such regimes have the capability to access the data you are transferring, not just whether they actually do in the case of your specific transfer.

For example, if your organisation is a financial services business, you will need to understand what surveillance or reporting regime applies to the financial data once it arrives in the US. Examine what conditions apply and any other applicable rules or disclosure obligations. In any case, it would be advisable to apply the principle of data
minimisation or anonymisation to such transfers wherever possible. In other words, only transfer the data you absolutely need to in order to fulfil the purpose of the transfer.

Similarly, any Jersey-based business using SCCs as a transfer mechanism to another Third Country will need to ensure that the receiving jurisdiction can provide the same standard of protection as required by the Law. The receiving data importer will be expected to identify any areas or factors that may prevent them from complying with those standards. If that happens, the expectation will be that the Jersey-based company must suspend the transfer until such issues are resolved and the appropriate standards of protection can be afforded in the receiving jurisdiction.

What should Jersey businesses do now?

For Jersey companies who transfer personal data to the US, or use the services of US-based processors, you will need to ensure the appropriate safeguards are in place BEFORE making any further transfers.

There are some steps you can take. These are our top 5 tips:

1. **Find another transfer mechanism.** SCCs are still a valid transfer mechanism and may provide a suitable alternative for you if you can satisfy yourself that data subjects can be guaranteed an essentially equivalent level of protection in the receiving jurisdiction. For inter-group transfers, you could also consider Binding Corporate Rules, remembering that these must be approved in advance of any transfers by the Authority. You should also consider the exceptions at Schedule 3 of the Law and which may permit the transfer of data in specific circumstances.

2. **Map out your data flows.** Critically examine all your flows and identify what safeguards you have in place for transfers to non-EU jurisdictions. Also assess the level of protection offered to personal data in the jurisdiction to which you are transferring the data; look at access to the Court system, understand the ability to seek legal recourse if things go wrong and look at the availability and powers of any regulator/ombudsman. You may also want to consider whether the authorities in that jurisdiction can access the information and on what basis.

3. **Re-assess your Processing contracts.** If you use a service provider/Processor in the US, make sure the processing contract reflects the appropriate mechanism and safeguards for transferring personal data. You may also want to consider changing your provider to one that can offer an adequate level of protection for data subjects.

4. **Keep an eye on the news.** The European Data Protection Board (EDPB) will very likely publish updates on the legality of data transfers where SCCs have been used. Keep in mind the CJEU position on SCCs may change.

5. **Provide additional safeguards.** Try not to rely on one single mechanism for your data transfers. Instead, try using SCCs plus another mechanism to ensure you are offering the best protection you can to the personal data you are transferring.
Are you a Jersey company that transfers personal data to the UK (including Northern Ireland)?

See below a non-exhaustive list of examples of ways you might be transferring data to a UK-based company:

- Are you outsourcing your HR, IT or Payroll function to a UK based organisation?
- Are you using a UK based marketing company to send marketing communications to your customer database?
- Is your occupational health provider based in the UK?
- Is your pension scheme based in the UK?
- Are you using translation/transcribing services of a UK based company where you might be sending personal data of employees, customers or suppliers?
- Are you using a UK based company to analyse data on visitors to your website?
- Are you storing data in the UK on a server or in the cloud?

Treatment of UK as adequate for purposes of data transfers post Brexit.

- Jersey prides itself on having very high standards of data protection and has the advantage of European recognition through its positive adequacy assessment. Jersey-based data controllers and processors are not permitted to transfer personal data outside the EU/EEA unless those standards are maintained.
- When the UK left the EU on 31st January 2020, it become a third country without an adequacy decision. The Withdrawal Agreement allowed EEA states and adequate jurisdictions to free-flow data with the UK during the transition period, which expired on 1st January 2021. The EU-UK Trade and Cooperation Agreement published at the end of December 2020 provides for an additional extension period of 4 months during which the UK will continue be treated as if it was still an EU member state for data protection purposes, rather than a third country. This additional extension period will be extended for a further two months unless the EU or UK object.
- Following the UK’s departure from the EU and pending any final agreement that might be reached between the UK and EU in respect of data protection matters, Jersey had previously amended its Law to allow for a sunset provision whereby the UK would be treated in the same way as if it were still an EU member state until the end of the transition period. On 18 November 2020 the States Assembly passed an extension to this extension to 31 December 2021.
- Accordingly, Jersey organisations may continue to transfer data to the UK without any further safeguards (such as SCCs, BCRs) being necessary until the end of 2021.
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 Law 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 Law 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  
**Web:** www.jerseyoic.org