JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

# GUIDANCE NOTE

# Data Transfers

Data Protection (Jersey) Law 2018
Article 66 and 67 of the Data Protection (Jersey) Law 2018

MAY 2018 • V1 • WWW.JERSEYOIC.ORG

# CONTENTS

# INTRODUCTION

1. The Data Protection (Jersey) Law (**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.

# OVERVIEW

- A controller or processor must not transfer data for processing to a third country or international organisation unless the level of protection for the rights and freedoms of data subjects is adequate. The level of protection is adequate if the European Commission has decided by means of an implementing act under Article 45 of the GDPR, there are safeguards in place that meet Art.67 of the DPJL or the transfer falls within the exceptions set out in Schedule 3 of the DPJL. Article 67 sets out those safeguards, which include binding corporate rules that comply with Schedule 4.

- These restrictions are in place to ensure that the level of protection of individuals afforded by the DPJL is not undermined when transferring their data outside the Bailiwick.

# DATA TRANSFERS

## The DPJL

4. Art.66 states that the transfer of personal data for processing is not permitted to a third country or international organisation unless that country or organisation ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data.

(1) "A controller or a processor must not transfer personal data for processing or in circumstances where the controller or processor knew or should have known that it will be processed after the transfer to a third country or an international organization, unless that country or organization ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

(2) The level of protection referred to in paragraph (1) is adequate if –

(a) the Commission has so decided, by means of an implementing act under Article 45 of the GDPR;

(b) there are appropriate safeguards in place that meet the requirements of Article 66; or

(c) the transfer falls within the exceptions set out in Schedule 3."

5. Art.67 sets out the relevant criteria where an organisation wishes to transfer data subject to appropriate safeguards:

"(1) In the absence of an adequacy decision under Article 45 of the GDPR, a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards in accordance with this Article, and on condition that enforceable data subject rights and effective legal remedies for data subjects comparable to those under this Law are available in that country or organization.

(2) The appropriate safeguards referred to in paragraph (1) may be provided for, without requiring any specific authorization from the Authority, by –

(a) a legally binding and enforceable instrument between public authorities;

(b) binding corporate rules approved by the Authority as complying with Schedule 4 or approved by another competent supervisory authority under Article 46 of the GDPR, or equivalent statutory provisions;

(c) standard data protection clauses adopted by the Authority or by a competent supervisory authority and approved by the Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR;

(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' rights; or

(e) the controller, processor or recipient in the third country having been certified in accordance with a certification mechanism either provided for in Regulations under Article 80 or approved by another competent supervisory authority under Article 42 of the GDPR.

(3) Subject to specific authorization from the Authority and where there is a mechanism for data subjects to enforce their data subject rights and obtain effective legal remedies against the controller, processor or recipient of that personal data in the jurisdiction concerned, the appropriate safeguards referred to in paragraph (1) may also be provided for by –

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or

(b) where both the transferor and the controller, processor or recipient of the personal data in the third country or international organization concerned are public authorities, provisions in administrative arrangements between those public authorities that include enforceable and effective data subject rights.

(4) In determining whether to authorize a transfer under this Article, the Authority must have regard to factors that include, but are not limited to, any opinions or decisions of the European Data Protection Board under Article 64, 65 or 66 of the GDPR that appear to the Authority to be relevant."

# Transfers on the basis of an adequacy decision

***Which countries are "adequate"***

6. The GDPR distinguishes between countries outside the European Economic Area (**EEA**) that are considered to ensure an adequate level of protection for personal data and "non-adequate" countries. The DPJL also permits transfers to adequate countries on the basis that the provide an essentially equivalent level of protection to data subjects to that afforded to them in Jersey.

7. The list of adequate countries is maintained on the European Commission's website. At the date of preparation of this Note, the following countries have been granted adequacy status:
   - Andorra
   - Argentina
   - Canada (commercial organisations)
   - Faroe Islands
   - Guernsey
   - Israel
   - Isle of Man
   - Jersey
   - New Zealand
   - Switzerland
   - Uruguay
   - The USA (limited to the Privacy Shield framework)

8. Schedule 3 of the DPJL allows for transmissions of data outwith an adequacy decision. Those exceptions are as follows[1]:
   - The transfer is specifically required by an order or judgment of a court or tribunal either having force of law in Jersey or based on an international agreement;

[1] Not all such exemptions apply to public authorities. Public Authorities should check the DPJL.

- The data subject has explicitly consented to the transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision or appropriate safeguards;
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract between the controller and a person other than the data subject;
- The transfer is by or on behalf of the Jersey Financial Services Commission and is necessary for reasons of substantial public interest;
- The transfer is necessary for or in connection with legal proceedings (including prospective), for the purposes of obtaining legal advice or otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- The transfer is necessary to protect a data subject's vital interests in circumstances where the data subject is physically or legally incapable of giving consent, consent has been withheld unreasonably or the controller or processor cannot reasonably be expect to obtain the explicit consent of the data subjects;
- The transfer is made from a register which is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register);
- The transfer is:
    - » not repetitive
    - » concerns only limited number of data subjects;
    - » necessary for the purposes of compelling legitimate interests pursued by the controller (not overridden by the interests, rights or freedoms of the data subject);
    - » If the transfer is made on this basis, the Authority must be informed as soon as is practicable and the data subject must also be told of the transfer and the compelling legitimate interests pursued.

# Transfers subject to appropriate safeguards

9. An organisation may transfer personal data where the organisation receiving the personal data has provided appropriate safeguards (Art.62 of the DPJL). Individuals' rights must be enforceable and effective legal remedies for individuals must be available (comparable to those in the DPJL) following the transfer.

10. Appropriate safeguards may be provided for by:
    a. A legally binding and enforceable agreement between public authorities or bodies
    b. BCRs (agreements governing transfers made between organisations within a corporate group);
    c. Standard model data protection clauses in the form of template transfer clauses adopted by the Authority and approved by the European Commission;
    d. Compliance with an approved code of conduct approved by the Authority;
    e. Certification under an approved certification mechanism;

11. Subject to specific authorisation from the Authority, further appropriate safeguards may also be provided for by:
    a. contractual clauses agreed between the controller or processor and the controller, processor or the recipient of the personal data in the third country; or
    b. provisions inserted into administrative arrangements between public authorities.

# BCRs

12. BCRS are a mechanism whereby an organisation can set out its global policy on the international transfer of data within that group.

13. Schedule 4 of the DPJL sets out the process by which organisations must structure their BCRs and supply then to the Authority for approval. The Authority must approve BCRs if those rules:
    a. Are legally binding and apply to and are enforced by every member of the group (including employees)
    b. Expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
    c. Fulfil the requirements of paragraph 2 of Schedule 4.

14. The BCRs must include:
    a. the structure and contact details of the group and of each of its members;
    b. the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
    c. a statement of their legally binding nature, both internally and externally;
    d. the application of the data protection principles, in particular those mentioned in Article 8(1)(b), (c) and (e), matters covered by Articles 15 and 21 and provisions relating to data quality, the legal basis for processing, processing of special categories of personal data and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
    e. the rights of data subjects in regard to processing and the means to exercise those rights, including the right
        i. not to be subject to decisions based solely on automated processing, in accordance with Article 38,
        ii. to lodge a complaint with the Authority under Article 19 of the Authority Law and to bring proceedings under Article 68 of this Law, and
        iii. to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
    f. the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group, the controller or the processor being exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the breach;
    g. how the information on the binding corporate rules, in particular on the provisions referred to in sub-paragraphs (d), (e) and (f) is provided to the data subjects in addition to the matters required by Article 12;
    h. the functions of any data protection officer appointed under Article 24 or any other person or entity in charge of monitoring compliance with the binding corporate rules within the group, as well as monitoring training and complaint-handling;
    i. the complaint procedures;
    j. the mechanisms within the group for ensuring the verification of compliance with the binding corporate rules, which mechanisms must include the following actions –
        i. data protection audits,
        ii. methods for ensuring corrective actions to protect the rights of the data subject,
        iii. communicating the results of such actions to the person or entity referred to in sub-paragraph (h) and to the board of the controlling undertaking of the group, and
        iv. making those results available upon request to the Authority;

k. the mechanisms for reporting and recording changes to the rules and reporting those changes to the Authority;

l. the mechanism for co-operating with the Authority to ensure compliance by any member of the group, in particular by making available to the Authority the results of the actions referred to in sub-paragraph (j)(i) and (ii);

m. the mechanisms for reporting to the Authority any legal requirements to which a member of the group is subject in a third country that are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

n. the appropriate data protection training to personnel having permanent or regular access to personal data.

15. We encourage organisations to make contact with us if they wish to discuss their needs in advance of making an application.

## Standard model clauses

16. Standard model clauses are contracts approved by the European Commission that can be adopted by the Authority (or approved by another competent supervisory authority) for the transfer of personal data in accordance with Article 93(2) of the GDPR.

17. Model clauses need to be signed by the organisation sending the data (the data exporter) and the organisation receiving the data (the data importer). In signing the clause, the data importer agrees that they can comply with the stipulated provisions in the agreement.

18. It should be noted that the Irish Information Commissioner has recently issued an application to the Court of Justice of the European Union in the case of the Data Protection Commissioner v. Facebook Ireland Ltd (1) and Maximillian Schrems (2) for a ruling on the validity of standard contractual clauses. The ruling sought by the Irish Commissioner relates to whether or not the clauses sufficiently protect personal data transferred outside Europe (in this case, into the US). Organisations should therefore ensure that they pay careful attention to any changes that may occur in this area and whether the use of model clauses is appropriate in the circumstances.

## Code of conduct/certification mechanism

19. There is no approved Code of Conduct or certification mechanism that has yet been put in place by the Authority. Should the position change in the future, this Note will be updated

# MORE INFORMATION

20. Additional guidance is available on our guidance pages with more information on other aspects of the DPJL and AL.

21. This guidance has been developed drawing on the Commissioner's experience. It will be reviewed and considered from time-to-time in line with new decisions by the Commissioner and/or the Jersey courts.

22. It is a guide to our general recommended approach, although each individual case will likely be different and will be decided on the particular circumstances of the case.

23. If you need any further information about this, or any other aspect of the DPJL or AL, please contact us or see our website www.oicjersey.org.

**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