Eighth Data Protection Principle - International transfers

At a glance

- The DPL imposes restrictions on the transfer of personal data to countries that are located outside the European Union (EU), and to third countries that do not have adequate protection.
- These restrictions are in place to ensure that the level of protection of individuals afforded by the DPL is not undermined.

In brief

Introduction to international transfers

The Cayman Islands has an outsize role in the global economy and our businesses are active participants in the global network of international data flows.

Broadly speaking, the eighth data protection principle of the Data Protection Law, 2017 (DPL) prohibits the international transfer of personal data where the destination does not offer an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This is to ensure that the level of protection guaranteed by the DPL cannot be circumvented by transferring personal data abroad.

This does not mean that personal data cannot be transferred internationally. However, any such transfers need to be assessed against the DPL.

This section seeks to answer common questions data controllers may have about their obligations under the DPL when it comes to transferring personal data and using service providers based outside the Cayman Islands.

What is the international transfers principle?

The eighth data protection principle says:

Personal data shall not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

What is an adequate level of protection?

Personal data must not be transferred to another country or territory unless an "adequate level of protection" can be ensured.

For the purposes of the eighth data protection principle, the Ombudsman considers the following countries and territories as ensuring an adequate level of protection:

- Member States of the European Economic Area (that is, the European Union plus Lichtenstein, Norway, and Iceland) where Regulation (EU) 2016/679 (the General Data Protection Regulation or "GDPR") is applicable;
- any country or territory in respect of which an adequacy decision has been adopted by the European Commission pursuant to Article 45(3) GDPR or remains in force pursuant to Article 45(9) GDPR.

Other countries and territories may still be deemed to have an adequate level of protection depending on:

- the nature of the personal data (e.g. "Are there sectorial data protection laws that apply?");
- the country or territory of origin of the information contained in the data;
- the country or territory of final destination of that information;
- the purposes for which and period during which the personal data is intended to be processed;
- the law in force in the country or territory in question;
- the international obligations of that country or territory;
- any relevant codes of conduct or other rules that are enforceable in that country or territory,

whether generally or by arrangement in particular cases; and
- any security measures taken in respect of the data in that country or territory.

The data controller must assess the above elements when deciding whether a country or territory would be compliant with the eighth data protection principle. The data controller will be held accountable for its decision. Where unsure, the data controller may wish to request an authorization from the Ombudsman pursuant to Schedule 4(9) DPL for the transfer.

Are there any derogations from the prohibition on transfers of personal data outside of the EU or other jurisdictions ensuring adequate protection?

The DPL provides exemptions from the general prohibition on transfers of personal data outside the EU (or other countries officially recognized as offering adequate protections) in certain specific circumstances.

A transfer, or set of transfers, may be made where the transfer is:

- made with the individual's consent;
- necessary for the performance of a contract between the individual and the organization, or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of substantial public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject;
- made in regard to public data on a public register, and any conditions subject to which the register is open to inspection are complied with;
- made on terms of a kind approved by the Ombudsman as ensuring adequate safeguards for the individual(s);
- authorized by the Ombudsman as ensuring adequate safeguards for the individual(s); or,
- required under international cooperation arrangements between intelligence agencies or regulatory agencies, if permitted or require under an enactment or an order issued by the Grand Court.

What terms will the Ombudsman approve as ensuring adequate safeguards?

The Ombudsman will approve the following terms as ensuring adequate safeguards:

- data transfer agreements based on standard contractual clauses published by the Ombudsman

(forthcoming); or
- data transfer agreements which replicate the rights and obligations contained in the EU 'standard contractual clauses' pursuant to Article 46 paras (2)(c), (2)(d), or (5) GDPR.

Where organizations elect to use standard contractual clauses, the Ombudsman will expect the organizations to amend them accordingly to address the fact that specific cross-references to provisions of European data protection law need to be replaced with cross-references to corresponding provisions of the DPL.

However, we are aware that it may be difficult for some local data controllers to get larger organizations to amend their standard SCCs. We will accept SCCs in the understanding that the intent of the parties is to interpret references to EU law as to the equivalent under the DPL.

The Ombudsman does not consider other types of safeguards specified in Article 46(2) GDPR to automatically qualify as “terms of a kind approved by the Commissioner” for the purposes of paragraph 8 of Schedule 4 to the DPL. However, transfers of personal data made in accordance with other types of safeguards approved in the European Union in accordance with Article 46 or Article 47 GDPR will be considered favorably by the Ombudsman and will be taken into account when the Ombudsman assesses whether to authorize a transfer in accordance with paragraph 9 of Schedule 4 to the DPL, or in assessing an organization's compliance with the eighth principle (international transfers).

What authorizations will the Ombudsman make?

It is expected that the Ombudsman will issue a general authorization for transfers where, taking into account the following aspects, the rights and freedoms of the data subjects affected will be adequately protected:

a. the nature of the personal data;
b. the country or territory of origin of the information contained in the data;
c. the country or territory of final destination of that information;
d. the purposes for which and period during which the personal data are intended to be processed;
e. the law in force in the country or territory in question;
f. the international obligations of that country or territory;
g. any relevant codes of conduct or other rules that are enforceable in that country or territory, whether generally or by arrangement in particular cases;
h. any security measures taken in respect of the data in that country or territory;
i. the recipient of the personal data; and
j. any relevant rules the recipient is bound by.

The data controller will need to assess the above elements when deciding whether a transfer would be compliant with the eighth data protection principle. This will include conducting appropriate due diligence on the recipient. The data controller will be held accountable for its decision. Where unsure, the data controller may wish to request a specific authorization for the transfer from the Ombudsman pursuant to Schedule 4(9) DPL.

What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?

Even where the destination of a data transfer cannot be said to offer an "adequate level of protection", transfer is not made on terms approved by the Ombudsman, and none of the derogations apply, the DPL provides that personal data may still be transferred provided that the transfer is limited in terms of scope, volume, and frequency.

However, such transfers are permitted only where the transfer:

- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (similar transfers are not made on a regular basis);
- involves limited data related to only a small number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organization (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable measures put in place by the organization (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data (e.g. using encryption and password protection, entering into non-disclosure agreement with the recipient, etc.).

Organizations should remember that pursuant to section 8(1)(d) of the DPL they are under an obligation to inform individuals about any international data transfers, upon request in the context of a data subject access request (SAR).

What steps should I take when I want to use a service provider not based in the Cayman Islands?

I. Assess whether the country or territory ensures an adequate level of protection
   a. Is it a country within the European Economic Area (EEA)? Then the transfer is allowed.
   b. Is it on the EU's list of adequate countries? Then the transfer is allowed.
   c. If not, you can conduct your own adequacy assessment regarding the country or territory pursuant to Schedule 1, Part 2 (4) DPL.

II. If adequacy has not been established, do any of the exemptions in Schedule 4 DPL apply?

These are:

a. Consent
b. Contract between the data subject and the data controller
c. Third-party contract in the interest of the data subject
d. Public interest
e. Legal proceedings, etc.
f. Vital interests
g. Public register
h. Transfer made on terms approved by the Ombudsman
i. Ombudsman has authorized the transfer
j. International cooperation between intelligence agencies or regulatory agencies

If none of the above apply and the transfer is not to an adequate country or territory, a transfer is not permitted. If one of the above applies, a transfer is permitted in principle, subject to the requirements of the next section.

III. Whether through adequacy or a Schedule 4 exemption, is the transfer to a data processor or to a data controller?
   a. If to a data processor, you need to put in place a Data Processing Agreement (DPA).
   b. If to another data controller, is there a legal basis for the transfer from you to the other data controller? If yes, the transfer is prima facie compliant.

My service provider's Data Processing Agreement (DPA) references EU law. Can I use it?

Yes. We are aware that it may be difficult for some local data controllers to get larger data processors to amend their standard DPAs. The requirements for a DPA are quite simple under the DPL, and require merely:

1. A written contract that requires the data processor:
   1. to act only on instructions from the data controller and
   2. to ensure appropriate technical and organizational measures to protect the personal data.

These requirements are also found in EU law, so that an EU compliant DPA will also be compliant under Cayman's DPL.

My service provider won't let me amend the EU Standard Contractual Clauses (SCCs)

to reference the Cayman DPL. Can I use them?

Yes. We are aware that it may be difficult for some local data controllers to get larger data processors to amend their standard SCCs. We will accept the EU's SCCs on the understanding that the intent of the parties is to interpret references to EU law as to the equivalent under the DPL.

Is Privacy Shield a valid transfer condition?

No. The EU-US Privacy Shield is a bilateral framework between the EU and the US. It provides rights only to individuals in the EU. It does not provide rights to individuals in the Cayman Islands.

However, self-certification under Privacy Shield may be taken into consideration as a positive factor when assessing the recipient of personal data under the Ombudsman's general authorization (see What authorizations will the Ombudsman make?).

Relevant provisions

Data Protection Law, 2017

Schedule 1, part 1, paragraph 8: Eighth data protection principle – International transfers

Schedule 1, part 2, paragraph 3: Content of Data Protection Agreement

Schedule 1, part 2, paragraphs 4-6: Adequate protection, EU findings

Schedule 4: Transfers to which eighth principle does not apply

Data Protection Regulations, 2018:

Regulation 10: Exception to the eighth data protection principle – international cooperation between intelligence and regulatory agencies

Further guidance

ICO:

Guidance on international transfers

European Commission:

Standard contractual clauses – controller to controller (2001)

Standard contractual clauses – controller to controller (2004)

Standard contractual clauses – controller to processor (2010)

European Data Protection Board:

Guidelines on derogations of Article 49 under Regulation 2016/679