

Eighth Data Protection Principle - International transfers

At a glance

- The DPA 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 DPA is not undermined.

In brief

- [Introduction to international transfers](#)
- [What is the international transfers principle?](#)
- [What is an adequate level of protection?](#)
- [Are there any derogations from the prohibition on transfers of personal data outside of the EU or other jurisdictions ensuring adequate protection?](#)
- [What terms will the Ombudsman approve as ensuring adequate safeguards?](#)
- [What authorisations will the Ombudsman make?](#)
- [What steps should I take when I want to use a service provider not based in the Cayman Islands?](#)
- [My service provider's Data Processing Agreement \(DP Agreement\) references EU law. Can I still use it?](#)
- [My service provider won't let me amend the EU Standard Contractual Clauses \(SCCs\) to reference the Cayman DPA. Can I still use them?](#)

Introduction to international transfers

The Cayman Islands has an outside 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 DPA 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 DPA 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 DPA.

This section seeks to answer common questions data controllers may have about their obligations under the DPA 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 acts 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.

Note that this listing is not exhaustive. The data controller must conduct a self-assessment of 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.

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

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

A transfer may be made where it is:

- made with the individual's consent;
- necessary for the performance of a contract between the individual and the organisation, 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);
- authorised by the Ombudsman as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects; 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 organisations elect to use standard contractual clauses, the Ombudsman will expect the organisations 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 DPA.

However, we are aware that it may be difficult for some local data controllers to get larger organisations 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 DPA.

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 DPA. 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 favourably by the Ombudsman and will be taken into account in assessing an organisation's compliance with the eighth principle (international transfers).

When will the Ombudsman authorise a transfer?

The Ombudsman may authorise a transfer to which the eighth principle does not apply, if it is nonetheless made in "such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects".

Where an organisation has been unable to establish, including through a self-assessment using the criteria for adequacy above, that the intended transfer complies with the eighth principle, it can ask the Ombudsman to authorise the transfer in these limited circumstances.

The Ombudsman will expect the data controller to demonstrate appropriate due diligence by, (i) identifying why it is that any departure from the arrangements that are generally considered as adequate in a foreign country is necessary in the particular circumstances of the proposed transfer; and (ii) in respect of each departure identified, explaining and justifying how it is then said that the rights and freedoms of the data subjects can still be adequately protected in these circumstances.

Among other things, the data controller should take into account the following aspects:

- 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 rights and freedoms of the data subject are understood to be the rights identified in the DPA, and could also encompass the rights and freedoms in the Bill of Rights, Freedoms and Responsibilities.

The data controller will be held accountable for its assessment.

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, conduct your own adequacy assessment pursuant to Schedule 1, Part 2 (4) DPA.
- II. If adequacy has not been established, do any of the exemptions in Schedule 4 DPA 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 authorised the transfer as being made in "such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects".
- 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 condition, 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 (DP Agreement).
 - 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 (DP Agreement) 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 DP Agreements. The requirements for a DP Agreement are quite simple under the DPA,

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 organisational measures to protect the personal data.

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

My service provider won't let me amend the EU Standard Contractual Clauses (SCCs) to reference the Cayman DPA. 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 DPA.

Relevant provisions

[Data Protection Act \(2021 Revision\):](#)

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](#)