PERSONAL DATA PROTECTION GUIDELINES NO.: 3/2025

CROSS BORDER PERSONAL DATA TRANSFER

Version 1.0

Date of Issuance: 29 April 2025

TABLE OF CONTENTS

PART A INTRODUCTION

1. Background

1.1. Section 129 of the Personal Data Protection Act 2010 [Act 709] (**"Act 709"**) regulates the transfer of personal data out of Malaysia. In order to carry out cross border personal data transfer, data controller is required to comply with the provisions under Section 129 of the Act 709.

1.2. This Guideline sets out as a guidance to clarify the requirements for compliance with each condition specified under Section 129 of the Act 709 and to assist data controller in deciding which condition may be referred to for any cross border personal data transfer.

1.3. Please note that the examples provided in this Guideline are not intended to be exhaustive and are only included for context and for purposes of illustration.

1.4. This guideline supplements and is to be read together with Act 709 and any other relevant legislative instrument(s) issued under the Act 709, as may be amended from time to time. It should not be considered to override any other data protection-related laws and regulations in effect at any given time.

2. Legal Provisions

2.1. This Guideline is issued by the Commissioner pursuant to subsection 48(g) of the Act 709.

3. Interpretation

3.1. Unless otherwise defined in this Guideline, the terms and expressions used herein shall have the same meanings assigned to them under the Act 709 and any other relevant legislative instruments under the Act 709.

3.2. In these Guidelines, unless the context otherwise requires:

"Personal data protection notice"	means a notice in writing that the data controller is required to provide to the data subject in compliance with Section 7 of Act 709;
"Receiver"	means data controller and/ or data processor who receives personal data of subject data outside of Malaysia;
"Transfer Impact Assessment"	means is a risk assessment conducted to evaluate the legal and regulatory framework where personal data is being transferred to ensure that receiving country/ jurisdiction

	provides a law substantially similar to Act 709 or adequate level of protection in relation to the processing of personal data;
"Recognised Certificate"	means certificate issued by an accredited body or authority that verifies that a data controller or data processor is in compliance with data protection standards or laws, both locally or internationally.

PART B CONDITIONS FOR THE TRANSFER OF PERSONAL DATA TO PLACES OUTSIDE MALAYSIA

4. Conditions for cross border personal data transfer

4.1. Subsection 129(2) of the Act 709 provides that a data controller may transfer any personal data of a data subject to any place outside Malaysia if:

(a) there is in that place in force any law which is substantially similar to the Act 709; or

(b) that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the Act 709.

4.2. Notwithstanding subsection 129(2) of the Act 709, data controller may transfer any personal data to a place outside Malaysia if:

4.2.1. data subject has given consent to the transfer;

4.2.2. the transfer is necessary for the performance of a contract between data subject and data controller;

4.2.3. the transfer is necessary for the conclusion or performance of a contract between data controller and third party which —

(a) is entered into at the request of data subject; or

(b) is in the interests of data subject;

4.2.4. the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;

4.2.5. the data controller has reasonable grounds for believing that in all circumstances of the case —

(a) the transfer is for the avoidance or mitigation of adverse action against the data subject;

(b) it is not practicable to obtain the consent in writing of the data subject to that transfer; and

(c) if it was practicable to obtain such consent, the data subject would have given his consent;

4.2.6. the data controller has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the Act 709; or

4.2.7. the transfer is necessary in order to protect the vital interests of the data subject.

4.3. In the event that data controller carries out or intends to carry out the transfer of personal data out of Malaysia, the data controller shall through its personal data protection notice or such other written notice inform data subject about the transfer.

4.4. The Commissioner may conduct an investigation on data controller to ascertain whether any act, practice or request contravenes Section 129 of Act 709.

5. A law substantially similar to the Act 709

5.1. Data controller may refer to paragraph 129(2)(a) of the Act 709 if it makes a finding that the place it intends to transfer personal data to has in place a law substantially similar to the Act 709.

5.2. A law is substantially similar to the Act 709 if the content of the law such as protection, rights and requirements related to processing including collection, disclosure, retention and cross border personal data transfer are similar to that provided under the Act 709.

5.3. Data controller may conduct Transfer Impact Assessment ("**TIA**") to review the relevant personal data protection law of the receiving country/ jurisdiction is equivalent to the Act 709 in order to fulfil the requirement under paragraph 129(2)(a) of the Act 709. The TIA shall be carried out in accordance with the following steps:

5.3.1. identify the countries to which the personal data is to be transferred to;

5.3.2. assess the personal data protection laws available in each of the receiving countries based on the factors listed in Paragraph 5.4;

5.3.3. determine whether there is in force a law substantially similar to the Act 709; and

5.3.4. ensure that the decision to transfer personal data comply with the Act 709.

5.4. Data controller shall at a minimum consider the following factors:

5.4.1. whether the law provides data subjects with similar rights such as the right of access and the right to correct personal data;

5.4.2. whether there are similar Personal Data Protection Principles in place such as the Security Principle;

5.4.3. whether there are similar requirement and protection with regards to the processing of personal data including collection, disclosure, retention and cross border data transfer;

5.4.4. whether there is similar or equivalent requirement regarding Data Protection Officer;

5.4.5. whether there is similar data breach notification requirement;

5.4.6. whether there is similar requirement imposed on data processor to protect personal data; and

5.4.7. whether there exists a regulatory authority in that country that is similar to the Department of Personal Data Protection and has similar powers to enable it to effectively enforce the relevant personal data protection law.

5.5. The TIA may be carried out by referring to the following source of information:

5.5.1. the laws, regulations, guidelines and circulars that relate to personal data protection;

5.5.2. case law or decision taken by independent judicial or administrative authorities regarding personal data protection matters;

5.5.3. reports from intergovernmental organisations, independent oversight bodies, business and trade associations and professional bodies;

5.5.4. news reports of data breaches;

5.5.5. reports provided by the receiver relating to the personal data protection practices and history of the said data controller/ data processor;

5.5.6. research articles relating to personal data protection laws and practices of receiving country/ jurisdiction; and

5.5.7. such other sources of information that are credible and not outdated relating to personal data protection.

5.6. The findings of the TIA shall be valid for no longer than three (3) years. Beyond that period, data controller shall conduct follow-up TIA following the steps outlined in paragraph 5.3.

5.7. In the event that there occurs a change or amendment to the relevant personal data protection laws during the validity period of the TIA, data controller shall conduct a review of the changes or amendments made to determine whether, as a result of the change or amendment, the relevant personal data protection law is still substantially similar to the Act 709.

6. A place with an adequate level of protection

6.1. Data controller may refer to paragraph 129 (2)(b) of the Act 709 if it makes a finding that the place it transfers personal data to is able to ensure that all the personal data transferred will be provided with an adequate level of protection that is at least equivalent to the level of protection provided by the Act 709.

6.2. Data controller may conduct TIA to determine the level of protection of personal data offered by the receiving country/ jurisdiction is equivalent to the Act 709 in order to fulfil the requirement under paragraph 129(2)(b) of the Act 709. The TIA shall be carried out in accordance with the following steps:

6.2.1. identify the countries which personal data is to be transferred to;

6.2.2. assess the mechanism to protect personal data of the receiving country/ jurisdiction based on the factors listed in paragraph 6.3;

6.2.3. based on the findings of the TIA determine:

(a) whether there are protection measures in place to ensure that the personal data is provided with an adequate level of protection equivalent to the Act 709; and

(b) whether there are further measures that must be taken by the receiver to ensure that personal data is adequately protected; and

6.2.4. ensure that the decision to transfer personal data comply with the Act 709.

6.3. Data controller shall consider the following factors:

6.3.1. whether the receiver has security measures and policies that are in line with the Security Principle and the Personal Data Protection Standard;

6.3.2. whether the receiver has in place any security related certifications which have assessed the systems in place and deemed to be secure;

6.3.3. whether the receiver is bound by legally enforceable obligations (either through contract, agreement or by law) and whether such obligations can be enforced by the data controller or data subject whose personal data is to be transferred to such recipient;

6.3.4. whether the relevant personal data protection law governing the receiver be easily enforced;

6.3.5. the receiver's past history of compliance with the relevant personal data protection law and whether it has experienced any data breach incidents;

6.3.6. whether the receiver (data controller) imposes or is legally required to impose requirements on data processor to protect personal data; and

6.3.7. whether there is a regulatory authority similar to the Department of Personal Data Protection that performs the functions and exercises powers under the law regarding personal data protection.

6.4. The TIA may be carried out by referring to the sources of information listed under paragraph 5.5.

6.5. The findings of the TIA shall be valid for no longer than three (3) years. Beyond that period, data controller shall conduct follow-up TIA following the steps outlined in paragraph 6.2.

6.6. In the event that there occurs a significant change or amendment to the systems or policies that relate to the security and protection of personal data during the validity period of the TIA, the data controller shall review the changes or amendments made to determine whether, as a result of the change or amendment, personal data is still provided with adequate protection equivalent to the Act 709.

7. Data subject's consent to the personal data transfer

7.1. Data controller may refer to paragraph 129(3)(a) of the Act 709 for cross border personal data transfer if the data subject has given consent to the transfer.

7.2. Data controller must first provide the data subject with personal data protection notice containing the following details regarding the cross border personal data transfer:

(a) the class of third parties to whom the data is transferred to; and

(b) the purpose of the transfer.

7.3. After the data subject has been provided with the personal data protection notice, data controller must obtain consent of data subject for the personal data transfer. The consent must be recorded and maintained in accordance with the requirements of the Personal Data Protection Regulations.

8. Transfer necessary for the performance of a contract between data subject and data controller

8.1. Data controller who has contract with data subject may refer to paragraph 129(3)(b) of the Act 709 for cross border personal data transfers if:

8.1.1. based on the factors listed under paragraph 8.3 and 8.4, the transfer is necessary for data controller to carry out obligations in the contract; and

8.1.2. the obligations must be for the core purpose of the contract.

8.2. There must be a direct and objective link between the performance of contract and the cross border personal data transfers.

Necessity of the cross border transfer of personal data

8.3. The word 'necessary' contained in paragraph 129(3)(b), (c) and (g) of the Act 709 does not mean that the cross border personal data transfer has to be absolutely

essential. However, the cross border personal data transfer must satisfy the following factors:

8.3.1. the cross border personal data transfer is not just practice or is carried out on a regular basis. The reasons for the transfer must be for the fulfilment of a specified purpose rather than for the general purposes or practices of the company;

> Example:
>
> A travel agency that intends to transfer personal data of its customer overseas may not rely on the argument that it is industry practice to transfer personal data out of Malaysia or that the purpose is for the travel agency's records or maintenance of its customer database.
>
> On the other hand, the travel agency would be said to be transferring personal data out of Malaysia for a specified purpose if the transfer is for the purposes of booking accommodation or event tickets for its customers.

8.3.2. the cross border personal data transfer is made to achieve a specific purpose only and not for general purpose; and

> Explanation:
>
> A transfer is considered to be made to achieve a specific purpose if the data controller is able to prove that the transfer was carried out to fulfil certain purposes. These specific purposes must not purely be for the benefit of the data controller and should be specific to the data subject or small group of data subjects as opposed to all data subjects of the data controller.

8.3.3. data controller cannot reasonably achieve the specified purpose through any alternative means which can be feasibly carried out.

> Explanation:
>
> Data controller will be considered to have "feasible alternative means" if the alternative means are:
>
> (a) able to be carried out at a lower or similar cost; and
>
> (b) able to achieve similar results or outcomes.
>
> For example, data controller who wishes to store personal data in a data centre outside Malaysia will be considered to have feasible alternative means if there are local data centres which offer data storage services at a lower or similar cost.

8.4. When making an assessment as to whether the cross border personal data transfer satisfies the above factors, data controller shall take into account the following:

8.4.1. the reason why the transfer is required;

8.4.2. the purposes for the transfer; and

8.4.3. whether there are any feasible alternatives available.

For the core purposes of the contract

8.5. The transfer of personal data must be directly related to and for the purposes of performing the obligations of the data controller as specified under the contract.

9. Transfer necessary for conclusion or performance of contract between data controller and third party

9.1. Data controller may refer to paragraph 129(3)(c) of the Act 709 for cross border personal data transfers if:

9.1.1. the transfer is necessary for the conclusion or performance of a contract between the data controller and a third party;

9.1.2. the contract:

(a) is entered into at the request of the data subject; or

(b) is in the interests of the data subject;

9.1.3. based on the factors listed out under Paragraphs 8.3 and 8.4, the transfer is necessary for the conclusion or performance of the contract.

9.2. The request by the data subject referred to in paragraph 9.1.2(a) must be:

9.2.1. provided in written form; or

9.2.2. where the request was made through means other than in writing, the said request maintained and kept in a proper form that can be shown as proof that the data subject made such request.

9.3. Data controller that intends to refer to paragraph 9.1.2(b) (interests of data subject) may only do so if the interest of data subject is shown to be:

9.3.1. clear and substantial: there must be an obvious benefit which can be clearly identified and stated by the data controller;

9.3.2. direct: the benefit to the data subject arises as a direct result of the conclusion or performance of the contract; and

9.3.3. targeted towards the data subject: the primary aim or purpose of the contract shall provide direct benefits to the data subject.

Examples:

- Data subject buys a travel package for his family. The travel agency then enters into agreements with operators (such as hotel and flight operators) and subsequently transfers their personal data out of Malaysia to those

operators for the purposes of making bookings related to the trip. This is considered a clear, direct and targeted benefit as the contract entered into:

(a) has a clear benefit. Data subject and his family will be able to go on holiday with their hotels and flights booked in advance;

(b) is direct. The performance of the contract between the travel agency and the operator provides direct benefits to the data subject and his family; and

(c) is targeted towards the data subject: the primary aim of the contract between the travel agency and operator is to ensure that the data subject and his family are able to go on holiday. It is also targeted towards the data subject and his family.

9.4. Additionally, data controller shall consider the factors listed under paragraphs 8.3 and 8.4 in relation to the conclusion or performance of the contract between the data controller and third party to ensure that the transfer is necessary.

10. Transfer for the purpose of legal proceedings

10.1. Data controller may refer to paragraph 129(3)(d) of the Act 709 for cross border personal data transfer if the transfer is for the purpose of:

10.1.1. legal proceedings;

10.1.2. obtaining legal advice; or

10.1.3. establishing, exercising or defending legal rights.

10.2. The legal proceeding includes the following:

10.2.1. a claim that would be brought and defended in a court (including civil and criminal law);

10.2.2. a claim that would be brought and defended in a tribunal (e.g. a consumer claims tribunal);

10.2.3. administrative or regulatory procedure (e.g. to defend an investigation (or potential investigation) in competition or financial services law, or to seek approval for a merger); or

10.2.4. an out-of-court procedure (e.g. without prejudice meeting, mediation or arbitration).

10.3. Data controller shall not refer to the condition under paragraph 129(3)(d) of the Act 709 if there is only a possibility that a legal proceeding or other formal proceedings may be brought in the future. Nevertheless, data controller may refer to this condition if the data controller:

10.3.1. is engaged in pre-action correspondence;

10.3.2. is taking advice about the legal risk in bringing or defending a claim; or

10.3.3. has received a request for information from an overseas regulatory authority with a view to it potentially taking formal action.

11. Reasonable grounds of the data controller

11.1. Data controller may refer to paragraph 129(3)(e) of the Act 709 for cross border personal data transfers if it has reasonable grounds for believing that:

11.1.1. the transfer is for the avoidance or mitigation of adverse action against the data subject;

11.1.2. it is not practicable to obtain the consent in writing of the data subject for that transfer; and

11.1.3. if it was practicable to obtain such consent, the data subject would have given his consent.

11.2. Paragraph 129(3)(e) of the Act 709 only applies if it is not possible for the data subject to give their consent such is:

11.2.1. data subject is unconscious;

11.2.2. data subject is not contactable, and given the circumstances, reasonable and proportionate steps have been taken to try and contact them; or

11.2.3. data subject is unable to provide consent due to insufficient time for the provision of all the information needed for a consent.

12. Requirement to take all reasonable precautions and exercise all due diligence for cross border transfers of personal data

12.1. Data controller may refer to paragraph 129(3)(f) of the Act 709 for any cross border personal data transfer if the data controller has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the Act 709. In this regard, all reasonable precautions and exercised due diligence may be deciphered by the following mechanisms:

12.1.1. Binding Corporate Rules ("**BCR**");

12.1.2. Contractual Clauses ("**CC**"); or

12.1.3. Certification under an approved certification scheme ("**Certification**").

Binding Corporate Rules

12.2. BCR is personal data protection policies that are implemented by multinational corporate group, group of undertakings or a group of enterprise engaged in a joint economic activity such as franchise, joint venture or professional partnership.

12.3. Data controller may refer to BCR that applies to the data controller and receiver for any cross border personal data transfer that are intra-group in nature.

> Explanation:
>
> Data Controller may carry out cross border personal data transfers to its franchisor or subsidiary company where there exists a BCR that is implemented by both the data controller and receiver.

12.4. The requirements for BCR are:

12.4.1. the BCR contains the following details:

(a) parties governed under BCR;

(b) specified countries/ jurisdictions where personal data may be transferred to;

(c) the legally binding nature of the BCR to all parties to the BCR and to any data subject of the parties to the BCR in relation to the data transfer made under the BCR;

(d) requirement for parties to ensure a standard of protection equivalent to the Act 709;

(e) requirement to comply with the personal data protection principles;

(f) personal data retention periods;

(g) reporting of any personal data breach;

(h) mechanisms for ensuring compliance;

(i) apportionment of liability for any personal data breach;

(j) requirements or restrictions related to the transfer of personal data to any third party service provider;

(k) the rights of data subject and methods to exercise their rights;

(l) the implementation of audit to ensure compliance by each party;

(m) effective date and last reviewed date of the BCR;

(n) responsibilities of the Data Protection Officer or any other person responsible for monitoring compliance with BCR; and

(o) complaint procedures.

12.4.2. BCR is legally binding on all parties to the contract and can be legally enforced; and

12.4.3. BCR is reviewed from time to time to ensure that it is up to date.

12.5. Any review of the BCR is to take into account the latest developments in the relevant data protection laws. The data controller is also encouraged to appoint an independent auditor to review the BCR to ensure that it is compliant with the Act 709.

Contractual Clauses

12.6. CC is a set of clauses inserted into a contract which would legally bind both the data controller and receiver to ensure adequate level of protection in relation to the processing of personal data.

12.7. Data controller who wishes to adhere to CC, shall ensure that the CC at least, cover the following:

12.7.1. the security measures that are to be implemented to provide adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by Act 709; and

12.7.2. clauses that state and guarantee that the processing of personal data shall be carried out in compliance with the Act 709.

12.8. Data controller relying on the use of CC shall at all times take all reasonable precautions to ensure that the receiver complies with the terms provided by the CC. In the event that the data controller discovers a breach of terms provided by the CC, the data controller shall cease the transfer of personal data to the other parties to the contract until such party rectifies the breach.

Use of the International Model

12.9. Data controller who wishes to use the international model may adopt the following list of contractual clauses including, but not limited to:

12.9.1. the Association of Southeast Asian Nations (ASEAN) Model Contractual Clauses for Cross Border Data Flows;

12.9.2. the European Union General Data Protection Regulation (EU GDPR) Standard Contractual Clauses for the Transfer of Personal Data to Third Countries; or

12.9.3. such other CC as determined by the Commissioner from time to time.

12.10. Prior to the use of international model above, data controller is recommended to review the CC to determine whether any additional clauses are necessary to be included to ensure adequate level of protection which is at least equivalent to the level of protection afforded by Act 709.

Certification

12.11. Data controller/ data processor may obtain certification regarding personal data protection as a method of verifying that the data controller/ data processor has in place adequate policies and processes to comply with data protection standard/ laws or provide an adequate level of protection to protect personal data.

Example:

- Europrivacy is a certification scheme managed by the European Centre for Certification and Privacy and is designed to assess, document, certify and value compliance with the EU GDPR.
- The Legal Services Operational Privacy Certification Scheme is designed to assist legal service providers demonstrate compliance with United Kingdom data protection law when processing their clients' personal data.
- The Asia Pacific Economic Cooperation Cross Border Privacy Rules System ("APEC CBPR") and Privacy Recognition for Processors ("APEC PRP") Certification is issued by the Infocomm Media Development Authority (Singapore) and TrustArc to certify that the data protection policies and processes of data controller/ data processor complies with the APEC CBPR and APEC PRP Principles.

12.12. Data controller may refer to the condition under paragraph 129(3)(f) of the Act 709 to transfer personal data out of Malaysia if:

12.12.1. receiver possesses a valid Recognised Certificate;

12.12.2. data controller undertakes reasonable efforts to verify the validity of the Recognised Certificate;

Example:

Reasonable efforts to verify the validity of the Recognised Certificate include:

(a) obtaining a certified true copy of the Recognised Certificate; and

(b) where possible, verify the validity of the Recognised Certificate through an online database. For example, Europrivacy has a Registry of Certificates that allows members of the public to search for and verify the validity of the Recognised Certificate.

12.12.3. data controller enters into a contract with the receiver which:

(a) imposes an obligation on the receiver to ensure that it has in place adequate level of protection to protect personal data transferred to; and

(b) warrants that the Recognised Certificate is valid.

12.13. Data controller shall at all times take all reasonable precautions to ensure that the receiver complies with its obligations to protect personal data. In the event that the data controller discovers a breach of such obligations, the data controller shall cease the transfer of personal data to the receiver until the breach has been rectified.

13. Transfer necessary to protect the vital interests of the data subject

Vital Interests of data subject

13.1. Data controller may refer to paragraph 129(3)(g) of the Act 709 for any cross border personal data transfer if:

13.1.1. the necessity of the transfer satisfies the factors laid out under paragraph 8.3 and 8.4; and

13.1.2. the purpose of the cross border personal data transfer is to protect the vital interests of the data subject.

13.2. Notwithstanding paragraph 13, the risk to the data subject's vital interests must outweigh any personal data protection concerns.

Example:

Data controller may refer to paragraph 129(3)(g) of the Act 709, for cross border personal data transfer if a Malaysian Data Subject is in a coma in Singapore and personal data about his/ her medical history needs to be transferred to Singapore for his/ her essential medical treatment.

If the Malaysian Data Subject is conscious and capable of giving consent, and the data controller has sufficient time to obtain consent, cross border personal data transfer does not fulfil the requirement under paragraph 129(3)(g) Act 709.

PART C HANDLING CROSS BORDER PERSONAL DATA TRANSFER

14. Responsibilities of the data controller when transferring personal data

14.1. Data controller is responsible for the security of personal data when transferring out of Malaysia and shall take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

14.2. Data controller shall ensure that the method for transferring personal data out of Malaysia is secure and in line with the Security Principle under the Act 709, subsidiary legislation, standard and any other applicable guidelines relating to protection of personal data.

15. Dealing with third party/ data processor

15.1. Data controller shall ensure that any contract entered into with third party/ data processor contains clauses governing the processing of personal data, including the security of personal data.

15.2. Data controller shall ensure that data processor complies with Section 9 of the Act 709, subsidiary legislation, standard and any other applicable guidelines relating to protection of personal data.

16. Record keeping

16.1. Data controller that carries out cross border transfer of personal data must keep and maintain record of the receiver to whom personal data is transferred to. Such record shall contain the following details:

16.1.1. the details of the receiver at least the following:

(a) the name of the receiver;

(b) company registration number (if any); and

(c) contact details of the Data Protection Officer or such other person at the receiver's end;

16.1.2. the country that the personal data is being transferred to;

16.1.3. the type of personal data transferred;

16.1.4. purposes of the transfer; and

16.1.5. such other information as the data controller deems necessary.

16.2. Additionally, data controller that carries out cross border personal data transfer must keep and maintain record that may sufficiently prove that each cross border personal data transfer complies with Section 129 of the Act 709. Examples of such records include:

Conditions	**Record**
Subsection 129(2) of the Act 709	- Record of TIA; and - Findings of TIA.
Paragraph 129(3)(a) of the Act 709	- Personal data protection notice; and - Record of data subject's consent.
Necessary for the performance of a contract	- Copy of the contract; and - Proof that the processing is necessary for the performance of the contract.

Conditions	**Record**
Reasonable precautions and due diligence	- Copy of BCR; - Copy of the Recognised Certificate; or - Copy of the signed contract between data controller and receiver.

16.3. Data controller must keep and maintain records provided under paragraph 16.1 subject to Retention Principle under the Act 709, subsidiary legislation, standard and any other applicable guidelines relating to protection of personal data or other laws in force.

[End of Document]