PUBLIC CONSULTATION PAPER NO. 05/2024:

CROSS BORDER PERSONAL DATA TRANSFER GUIDELINES

Start Date : 1 October 2024

End Date : 18 October 2024

PART 1: INTRODUCTION AND BACKGROUND

(1) Introduction

2.1 Cross-border data transfers occur when a data controller[1] (previously known as data users) transfers personal data of a data subject in Malaysia to a different country. This transfer may be made to another data controller, a data processor who will process data on behalf of the data controller (e.g. where the data controller transfers personal data to servers or cloud storage located outside of Malaysia).

2.2 All cross-border data transfers are regulated by Section 129 of the Personal Data Protection Act 2010 ("**PDPA**"). Under Section 129, data controllers are only allowed to carry out cross-border data transfers if:

(a) it transfers personal data to a country deemed to have adequate protections and is placed on the "whitelist"; or

(b) any of the conditions provided under Section 129(3) applies to the transfer (e.g. the consent of the data subject has been obtained; a transfer is necessary for the performance of a contract).

2.3 The Personal Data Protection (Amendment) Bill 2024 ("**Amendment Bill**"), which introduces amendments to the PDPA, was passed without amendments by the House of Representatives on 16 July 2024, and by the Senate on 31 July 2024. The Amendment Bill is currently pending assent by the Yang di-Pertuan Agong.

2.4 Clause 12 of the Amendment Bill introduced several amendments to Section 129 of the PDPA, namely:

(a) removal of the whitelist by deleting Section 129(1);

(b) amendment of Section 129(2) to place the responsibility of determining whether another country has adequate laws or protections to safeguard personal data on the data controller (instead of the Minister); and

(c) deletion of Section 129(3)(h) (i.e. transfer is permitted where necessary for public interest).

2.5 For ease of reference, the **Commissioner** have provided the newly amended Section 129(2) and (3) of the PDPA:

> ***Transfer of personal data to places outside Malaysia***
>
> ***Section 129***
>
> (2) *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 this Act; or*

[1] Clause 2 of the Amendment Bill substitutes the term "data user(s)" with "data controller(s)" throughout the Amendment Bill.

(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 this Act.

(3) *Notwithstanding subsection (2), a data controller may transfer any personal data to a place outside Malaysia if-*

(a) the data subject has given his consent to the transfer;

(b) the transfer is necessary for the performance of a contract between the data subject and the data controller;

(c) the transfer is necessary for the conclusion or performance of a contract between the data controller and a third party which—

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

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

(d) 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;

(e) the data controller has reasonable grounds for believing that in all circumstances of the case—

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

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

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

(f) the data controller has taken all reasonable precautions an 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 this Act; or

(g) the transfer is necessary in order to protect the vital interests of the data subject.

2.6 Following the amendments to Section 129 of the PDPA, data controllers who wish to carry out cross-border data transfers will have to ensure that at least one of the conditions under Section 129(2) or (3) are met.

Examples:

The data controller informed and obtained the consent of the data subject to transfer the data subject's personal data to a data processor located in Singapore. This is a valid transfer of personal data outside of Malaysia as the condition under Section 129(3)(a) is met.

The data controller is involved in a dispute with a foreign company and was ordered by the High Court of Kuala Lumpur to provide certain documents containing personal data of its

data subjects to the foreign company. This is a valid transfer of personal data outside of Malaysia as the condition under Section 129(3)(d) is met.

2.7 To provide further guidance on the use of the conditions provided under Section 129(2) and (3), a proposed Guideline on Cross-Border Personal Data Transfer Guidelines ("**Cross-Border Personal Data Transfer Guideline**") is being developed by the Personal Data Protection Commissioner ("**Commissioner**").

2.8 Pursuant to the above, this Public Consultation Paper ("**PCP**") seeks to gather public views and feedback regarding aspects that will be or should be addressed in the proposed Cross-Border Personal Data Transfer Guideline.

PART 2: PROPOSED REQUIREMENTS FOR CROSS-BORDER PERSONAL DATA TRANSFERS UNDER THE PDPA

2.1 As an overview, Part 2 of this PCP on proposed requirements that will be addressed in the Cross-Border Personal Data Transfer Guideline is categorised as follows:

(a) The new condition under Section 129(2)(a)

(b) The new condition under Section 129(2)(b)

(c) Consent

(d) Necessity of the cross-border transfer of personal data

(e) Binding Corporate Rules (BCRs)

(f) Standard Contractual Clauses (SCCs)

(g) Certification

(h) Record Keeping

[A] The New Condition under Section 129(2)(a)

2.2 Background: Under the newly amended Section 129(2)(a), data controllers may carry out cross border data transfers if that country has laws that are substantially similar to the PDPA. This would primarily arise in the form of a local personal data protection law which should provide similar rights and protections to data subjects.

> ***Section 129***
>
> (2) *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 this Act;*

2.3 Certain jurisdictions such as New Zealand, Indonesia and Thailand allow cross-border data transfers to any jurisdictions that have in force any law substantially similar to their respective personal data protection laws.

2.4 Additionally, data controllers relying on any condition provided by Article 46 of the European Union General Data Protection Regulation to conduct cross-border data transfers are required to carry out a Transfer Impact Assessment ("**TIA**").

2.5 A TIA is an assessment to identify and assess the risks associated with a transfer of personal data to another country. This will assist the data controller in deciding as to whether the law in force is adequate in providing protection to personal data processed and retained in that country.

2.6 Proposal: It is proposed that any data controller who wishes to rely on this condition be required to carry out an investigation in the form of a TIA. This TIA will be carried out to determine whether the country that they intend to transfer personal data to has in place a law substantially similar to the PDPA. The TIA will contain the following steps:

(a) identifying all countries that the personal data is to be transferred to;

(b) assessing the personal data protection law available in each of the receiving countries based on the factors listed below; and

(c) conducting periodic TIAs to ensure that the level of protection is still similar.

2.7 When conducting a TIA, the data controller may consider the following factors (which are not intended to be exhaustive):

(a) whether the law provides data subject with similar rights (such as the right to access and the right to correct);

(b) whether there are similar personal data protection principles in place (such as the security principle);

(c) whether there are similar requirements and protections with regards to the processing, transfer, retention, disclosure and cross-border data transfer of personal data;

(d) whether there are similar requirements regarding data protection officers;

(e) whether there are similar data breach notification requirements; and

(f) whether the law has in place similar penalties and enforcement mechanisms (such as providing the data protection commission with powers of inspection and investigation) to deal with breaches of the local data protection law and data breaches.

2.8 Once a TIA has been conducted and concluded, the data controller will have to assess the results of the TIA to determine whether there is in force a law substantially similar to the PDPA.

Question 1

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you agree that under the newly amended section 129(2)(a), a data controller should be required to carry out an investigation or assessment in the form of a TIA as proposed in paragraph 2.6 above? If not, how do you propose the assessment or investigation be conducted?

(b) Do you agree with the factors which should be taken into account when conducting the TIA as stated in paragraph 2.7 above?

(c) Other than those stated in paragraph 2.7, are there any additional factor or specific measures you believe should be included in order to carry out TIA?

[B] The New Condition under Section 129(2)(b)

2.9 Background: Under the newly amended Section 129(2)(b), a data controller may carry out cross-border data transfers to any place that is able to guarantee that the personal data processed has an adequate level of protection. This level of protection should be similar to or better than that provided under the PDPA.

> ***Transfer of personal data to places outside Malaysia***
>
> ***129(2)***
>
> (2) *A data controller may transfer any personal data of a data subject to any place outside Malaysia if-*
>
> *(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 this Act.*

2.10 Singapore allows for cross-border data transfers to recipients who have in place legally enforceable obligations which provide a standard of protection comparable to the protection provided under the Singapore Personal Data Protection Act 2012.

2.11 Proposal: It is proposed that any data controller who wishes to carry out cross-border data transfers based on this condition be required to carry out an investigation in the form of a TIA. This TIA will be used to determine as to whether the country or place that they intend to transfer personal data to has in place an adequate level of protection similar to that given under the PDPA. The TIA will contain the following steps:

(a) identifying all countries that the personal data is to be transferred to;

(b) assessing the mechanisms to safeguard personal data that are in place in each of the receiving countries based on the factors listed below; and

(c) conducting periodic TIAs to ensure that the level of protection is still similar.

2.12 When conducting a TIA, the data controller may consider the following factors (which are not intended to be exhaustive):

(a) whether the recipient has security measures and policies that are in line with the security principle and the minimum security standards prescribed under the PDPA (e.g. security standards under the Personal Data Protection Standards 2015);

(b) whether the recipient has in place any security-related certifications which have assessed the systems it has in place and deemed its systems to be secure;

(c) whether the recipient 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 subjects whose personal data is to be transferred to such recipient.

Question 2

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you agree that under the newly amended section 129(2)(b), a data controller should be required to carry out an investigation or assessment in the form of a TIA as proposed in paragraph 2.11 above? If not, how do you propose the assessment or investigation be conducted?

(b) Do you agree with the factors that should be taken into account in order to determine whether the recipient has in place a similar level of protection as referred to in paragraph 2.12 above?

(c) Other than those stated in paragraph 2.12, are there any additional factor you believe should be included in order to determine whether the recipient has in place a similar level of protection?

[C] Consent

2.13 Background: Under Section 129(3)(a) of the PDPA, a data controller may carry out cross-border data transfers if the data subject has provided their consent for the cross-border data transfer.

Transfer of personal data to places outside Malaysia

Section 129

(3) *Notwithstanding subsection (2), a data controller may transfer any personal data to a place outside Malaysia if-*

(a) the data subject has given his consent to the transfer;

2.14 Other jurisdictions such as the EU, UK, Japan, South Korea, Singapore, New Zealand, Australia, Indonesia and Thailand allow for cross-border data transfers where the consent of the data subject has been obtained.

2.15 Jurisdictions such as Singapore and Australia allow for this consent to be taken in the form of explicit or implied consent. On the other hand, jurisdictions such as the EU and UK require consent obtained to be explicit.

2.16 Explicit consent requires an action to be taken by the data subject to indicate that they consent to the cross-border data transfer. On the other hand, implied consent is consent taken from an observation of the data subject's behaviour, such as their continued use of service or lack of objection.

2.17 Proposal: It is proposed that data controllers who wish to obtain a data subject's consent to transfer their data outside Malaysia and rely on Section 129(3)(a) be required to carry out the following process:

(a) inform data subjects about the cross-border data transfer by including such details in their written notice (personal data protection notice / privacy notice) and given to the data subject as soon as practicable. The information provided to data subjects must include the class of third parties that may have access to the data subject's personal data outside of Malaysia, as well as the purpose of the data transfer; and

(b) A data controllers ~~will then~~ ~~be~~ is required to obtain the consent of the data subject for cross-border data transfers. This consent must be capable of being recorded or maintained in accordance with the requirements of the Personal Data Protection Regulations 2013.

Question 3

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you agree with the above process laid out in paragraph 2.17 above to obtain consent from the data subject?

(b) Do you think that there are any additional measures that should be taken by data controllers when relying on the consent of data subjects?

(c) Do you think that the consent referred to under Section 129(3)(a) of the PDPA should be limited to explicit consent? If not, please specify and justify.

[D] Necessity of the Cross-Border Transfer of Personal Data

2.18 Background: Several conditions found under Section 129(3) may only be relied on by data controllers if the cross-border data transfer is necessary to achieve the stated purposes. These conditions are:

(a) **Section 129(3)(b)**: the transfer is necessary for the performance of a contract between the data subject and the data controller;

(b) **Section 129(3)(c)**: the transfer is necessary for the conclusion or performance of a contract between the data controller and a third party which—

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

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

(c) **Section 129(3)(g)**: the transfer is necessary in order to protect the vital interests of the data subject.

2.19 As the word "necessary" is subjective, it may create a lot of confusion as to when a transfer is necessary and satisfies the above conditions. Therefore, the Cross-Border Personal Data Transfer Guideline intends to provide guidance on how to determine as to whether a transfer is necessary.

2.20 Both the EU and the UK contain similar conditions which require proof that the transfer is necessary. In line with that, both the EU and the UK have introduced a necessity test to determine as to whether a particular cross-border data transfer is necessary.

2.21 Proposal: It is proposed that any data controller who intends to rely on one of the above conditions may consider the following factors to determine whether the transfer is "necessary" for the stated purposes:

(a) the cross-border data transfer is not just useful and standard practice. Any cross-border data transfer must be for more specific reasons rather than it being generally useful to the data controller and/or data subject and must not be a common or standard practice carried out by the data controller;

(b) the cross-border data transfer is made to achieve a specific purpose only and not for a wider general purpose; and

(c) the data controller cannot reasonably achieve the specified purpose through an alternative means.

2.22 When considering the above factors, data controllers should take into account the following:

2.22.1 the reasons why the transfer is required / the purposes for the transfer; and

2.22.2 any alternatives available.

Question 4

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you agree with the above factors to determine whether a transfer is "necessary" for the stated purposes set out in paragraph 2.21 above?

(b) Do you think that there are any additional factors that should be considered by a data controller when assessing whether the transfer is necessary for the stated purposes referred in paragraph 2.22 above?

[E] Binding Corporate Rules (BCRs)

2.23 Background: Section 129(3)(f) of the PDPA provides that a data controller may transfer personal data outside Malaysia 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 PDPA.

Section 129

(3) *Notwithstanding subsection (2), a data controller may transfer any personal data to a place outside Malaysia if-*

(f) 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 this Act;

2.24 BCRs are a set of data protection rules or policies that apply to intra-group cross-border data transfers and are typically applicable to multinational companies or between related companies.

2.25 Please note that BCRs are not contracts formed between two related companies. BCRs are typically policies (similar to any internal policies or codes of conduct) which are created to govern conduct within the company and within the wider group of companies.

2.26 A BCR directly governs and sets out an employee's conduct in handling personal data and when transferring data to another country. Failure to comply with the guidance set out in the BCR often results in disciplinary proceedings and an internal investigation to ensure that there is no loss of data. Therefore, cross-border data transfers guided by a BCR will typically be safe and effective as long as employees comply with it.

2.27 The EU, UK, Singapore, New Zealand, Australia, Indonesia and Thailand recognise BCRs as valid cross-border mechanisms. While jurisdictions such as the EU and UK require BCRs to be approved by the applicable regulator, Singapore does not require approval from the regulator as long as the contents of the BCRs comply with the minimum requirements.

2.28 Proposal: It is proposed that the use of BCRs be recognised as proof that the data controller has taken all reasonable precautions and satisfies Section 129(3)(f) of the PDPA.

2.29 It is also proposed that no regulator approval be required for the adoption of BCRs by data controllers. Nevertheless, all BCRs must contain the following information:

(a) the specified recipients covered by the BCRs;

(b) the requirement for recipients to ensure a standard of protection equivalent to that under the PDPA;

(c) the designated countries/territories where personal data may be transferred to;

(d) procedures for handling data subject requests/complaints; and

(e) security measures that recipients must implement to protect transferred data.

2.30 Any BCR that does not meet the above requirements as to information will not be recognised as valid BCRs and will not be seen to satisfy the requirements under Section 129(3)(f).

Question 5

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Should the adoption of BCRs be seen as proof that a data controller has complied with Section 129(3)(f) of the PDPA?

(b) Should the BCRs require prior approval by the Commissioner?

(c) Are the minimum details listed at paragraph 2.29 above sufficient or should there be additional requirements as to detail?

(d) If your answer above is no, please let the Commissioner know what details should be included in these minimum requirements.

[F] Standard Contractual Clauses (SCCs)

2.31 Background: Under Section 129(3)(f) of the PDPA, a data controller may transfer personal data outside Malaysia 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 PDPA.

Section 129

(3) *Notwithstanding subsection (2), a data controller may transfer any personal data to a place outside Malaysia if-*

(f) 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 this Act;

2.32 SCCs are standardised contractual clauses that must be inserted into a contract between two parties for the purposes of regulating the transfer of personal data between parties to the contract.

2.33 The primary purpose of SCCs is to legally bind all parties involved in the cross-border data transfer to commit to the adoption of appropriate safeguards to ensure the security of personal data.

2.34 SCCs are typically prescribed by the relevant data protection commission or department or international body. The prescribed clauses must be present in the SCC signed by all parties.

2.35 As SCCs form legally binding obligations and are often stringent in its data protection requirements, the use of SCCs should be deemed to be a sign that the data controller has taken all reasonable precautions and exercised due diligence to ensure that personal data is not processed in contravention with the PDPA.

2.36 The EU, UK, Singapore, New Zealand, Indonesia and Thailand recognise SCCs as valid cross-border mechanisms. While the EU and UK provide SCCs as template contracts that can be immediately adopted by any party, Thailand provides 2 separate models of SCCs that can be selected and it is similar to the model proposed below.

2.37 Proposal: It is proposed that any data controller who enters into an SCC with the receiving data controller or processor be recognised to have taken all reasonable precautions and will be able to rely on Section 129(3)(f) of the PDPA for the cross-border transfer of personal data to that receiving data controller or processor.

2.38 Additionally, it is proposed that 2 separate models of SCCs be provided to data controllers, namely:

(a) the Malaysian Model: the Commissioner will set out minimum clauses that must be inserted in any contractual agreements relied on by parties to conduct cross-border data transfers. Requirements may include:

(i) clauses that state that all processing must comply with the PDPA; and

(ii) minimum security measures that must be implemented to protect personal data;

(b) the Overseas Model: the Commissioner will set out regional/international model contractual clauses that may be adopted and adapted to address matters prescribed under the PDPA. The current regional/international model contractual clauses that are proposed are:

(i) the ASEAN Model Contractual Clauses for Cross-Border Data Flows;

(ii) the EU GDPR's Standard Contractual Clauses for the Transfer of Personal Data to Third Countries; and

(iii) such other SCCs as may be determined by the Commissioner from time to time.

2.39 Data controllers using SCCs are not required to obtain approval from the Commissioner. However, any SCCs that do not meet the applicable requirements will not be recognised as valid SCCs and will not be seen to satisfy the requirements under Section 129(3)(f).

Question 6

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Are you aware of any SCCs that are currently recognised? If yes, please specify the relevant SCCs.

(b) Should the use of SCCs be seen as proof that a data controller has complied with Section 129(3)(f) of the PDPA?

(c) With reference to paragraph 2.38 above, do you agree with the adoption of the 2-model system used by Thailand? In particular, do you agree with the use of the Overseas Model?

(d) If your answer above is no, please explain your reasons why along with the alternative that you prefer.

(e) What is the likely impact that may be felt by data controllers following the introduction of SCCs?

[G] Certification

2.40 Background: Under Section 129(3)(f) of the PDPA, a data controller may transfer personal data outside Malaysia 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 PDPA.

Section 129

(3) *Notwithstanding subsection (2), a data controller may transfer any personal data to a place outside Malaysia if-*

(f) 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 this Act;

2.41 There currently are internationally accredited bodies which are able to conduct assessments on the policies, processes and systems of data controllers to determine as to whether they are compliant with a particular data protection law (i.e. Europrivacy seal which certifies compliance with the EU General Data Protection Regulation). These certificates must be renewed from time to time to ensure their validity.

2.42 Therefore, a data controller who has been issued with a valid certificate is recognised to be compliant with the relevant personal data protection law and has sufficient safeguards in place to protect personal data.

2.43 The EU, UK, Singapore, New Zealand, Japan, South Korea and Thailand recognise certification mechanisms as valid cross-border mechanisms. While most jurisdictions recognise certificates provided by certain accredited independent certification bodies, South Korea only recognises certificates issued by the Data Protection Commission of South Korea.

2.44 In order to carry out cross-border transfers of personal data under the certification mechanism, the EU and UK also require the data controller to ensure that the receiving data controller or processor is legally bound to apply the appropriate safeguards. This is usually in the form of an agreement or contract.

2.45 Proposal: It is proposed that the following requirements must be met in order to rely on the certification mechanism as proof that the data controller has taken all reasonable precautions and satisfies Section 129(3)(f) of the PDPA:

(a) the receiving data controller or processor has been issued with a valid certificate that is recognised by the Commissioner; and

(b) the data controller enters into a legally binding agreement or contract with the receiving data controller or processor to guarantee that the receiving data controller or processor applies to appropriate safeguards to protect the personal data transferred to it.

2.46 It is also proposed that the Commissioner issue a list of certifications that are recognised for compliance with Section 129(3)(f) of the PDPA.

Examples:

Certificates issued by the Asia Pacific Economic Cooperation Cross Border Privacy Rules System

Question 7

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Are you aware of any certifications that are currently recognised by data controllers?

(b) Should the cross-border transfer of personal data to a data controller or processor which has been issued with a certification recognised by the Commissioner be recognised as proof that the data controller or processor has complied with Section 129(3)(f) of the PDPA?

(c) Do you agree with the proposal to recognise certifications from certain certification agencies or should the South Korean approach be adopted, in which only certificates issued by the Commissioner be accepted?

(d) Apart from the certification mentioned in the proposal, are there any other certifications that should be recognised by the Commissioner? If yes, please specify which certifications.

[H] Record Keeping

2.47 Background: In order to carry out cross-border data transfers, a data controller must first ensure that one of the conditions under Section 129(2) or 129(3) is met. However, it will be difficult for the Commissioner to investigate and ensure that any cross-border data transfer meets one of the conditions if no record of such transfer is kept and maintained.

2.48 Other jurisdictions such as the EU require data controllers to maintain detailed records of their cross-border data transfers including the categories of personal data transferred, countries involved and the legal basis for the transfer.

2.49 Proposal: It is proposed that any data controller who carries out cross-border data transfers be required to keep and maintain as records the following information:

(a) the details of the data controller/data processor that personal data is transferred to. This includes:

(i) the name of the data controller/processor;

(ii) company registration number; and

(iii) contact details of the data protection officer or such other person with equivalent roles, powers or responsibilities of the data controller/processor;

(b) the country that the personal data is being transferred to;

(c) the type of data that is transferred;

(d) reasons for the transfer; and

(e) such other information as the Data Controller deems necessary.

2.50 Additionally, it is proposed that any data controller who carries out cross-border data transfers be required to maintain such records that may sufficiently prove that each cross-border data transfer complies with at least one of the conditions listed under Section 129(2) and 129(3) of the PDPA.

Examples:

Condition that the transfer is based on	***Record***
Section 129(2) of the PDPA	*Records of the Transfer Impact Assessment carried out and the results of such assessment.*
Consent	*Records of the consent provided by the data subject*
A contract between a data controller and a third party in the interests of the data subject	*A copy of the contract and reasoning for it is in the interest of the data subject*
Binding Corporate Rules	*A copy of such rules*
Standard Contractual Clauses	*A copy of such contract or agreement*
Certification	*A copy of such certification and the legally binding agreement or contract.*

Question 8

In providing your responses to the questions below, please provide clear justifications to support your views:

Do you agree that data controllers should be required to keep and maintain the above records as proposed at paragraph 2.49 above?