Model Provisions on Data Protection

The Commonwealth

Office of Civil and Criminal Justice Reform

Model Provisions on Data Protection

The Commonwealth

Published by the Commonwealth Secretariat.

Background

Commonwealth Law Ministers adopted three model Bills on privacy and freedom of information at their meetings in 2002 and 2005. The Freedom of Information Bill, the Privacy Bill, and the Protection of Personal Information Bill were developed to assist member countries in the processing and protection of information by providing a framework to draw upon when drafting legislation on the control, collection, access, use and dissemination of data. Since then, significant developments have occurred globally in data protection law, transforming the rules regulating the handling of personal data.

At their meeting in October 2018, Senior Officials agreed that review of the Privacy Bill and the Protection of Personal Information Bill ('the Model Bills') was timely in light of recent technological advances and new international instruments. Senior Officials requested the Secretariat to convene an expert working group to review and make recommendations in respect of possible amendments to the Model Bills.

In response to this request, the Commonwealth Expert Working Group on Data Protection, comprised of representatives of member countries and led by the Commonwealth Office of Civil and Criminal Justice Reform, met over two days in June 2019, at Marlborough House, London, to review the Model Bills. This was against the background of the Commonwealth Connectivity Agenda and Cyber Declaration, adopted in April 2018 by Commonwealth Heads of Governments, which acknowledge the importance of compatible regulatory regimes to promote good regulatory practice and facilitate transnational trade.

At their meeting in June 2019, the Expert Working Group considered a detailed paper reviewing the Model Bills. The review aimed to examine whether the Model Bills were fit for purpose in light of the pace of technological and regulatory developments, and had good alignment with other international instruments. The Expert Working Group considered several international developments, including the impact of electronic devices, which have led to an exponential increase in personal data generation, and the need to promote confidence in digital trade, while ensuring a high level of protection of fundamental rights.

The Expert Working Group agreed that there was a need to revise the Model Bills in light of developments in international data protection standards, as well as the ubiquitous collection and processing of personal data through electronic systems. The Group noted the importance of alignment with relevant international standards – including the OECD Guidelines, Convention 108+, the European General Data Protection Regulation, the African Union Convention on Cybercrime and Cybersecurity, the APEC Framework and the ASEAN Framework – in order to promote economic growth and development through interoperable legal frameworks. In so far as such international and regional instruments adopt different approaches, the Group observed that the Commonwealth, with its wide geographic membership, provided the opportunity to bridge regional differences, so far as is possible.

The Expert Working Group expressed an overall preference for a new single Commonwealth model that would cover data protection rights and obligations across all sectors. It was recognised, however, that different national contexts, including different federal and state arrangements, as well as different considerations in respect of the processing of personal data by the public and private sector, meant

that there may be some differences in the application of certain provisions. To address this, the Group supported a flexible approach based on model provisions that would make use of legislative options, square brackets and explanatory notes as appropriate. The Group recognised that in such countries where it is appropriate, the new model provisions could be incorporated in separate Acts.

The Expert Working Group recommended a hybrid approach to the question of whether the new model provisions should be predominantly principles-based or rules-based. The Group agreed that the new model provisions should reflect general principles that are augmented by detailed rules where appropriate.

At their meeting in November 2019 in Colombo, Sri Lanka, Law Ministers welcomed the establishment of the Expert Working Group on Data Protection and noted the outcomes of its meeting held in June 2019. Law Ministers agreed with the Expert Working Group's recommendation of new Commonwealth model provisions that would cover data protection rights and obligations across all sectors. Law Ministers requested the Secretariat to produce the Model Provisions for their review and approval at the next Law Ministers Meeting.

In October 2019 a first draft of the proposed Model Provisions and commentary was produced in accordance with the directions of the outcome statement of the June 2019 meeting of the Expert Working Group. From October 2019 to October 2020, five further versions of the proposed Model Provisions on Data Protection, with commentary, were distributed to the Expert Working Group for comment. A final version was agreed by all members of the Expert Working Group in October 2020.

The final version of the proposed Model Provisions associated commentary was presented to Senior Officials at their meeting in February 2021. Commonwealth Law Ministers approved the final Model Provisions at their meeting from 22 to 25 November 2022, in Balaclava, Mauritius.

Model Provisions on Data Protection

Introduction

Commonwealth Law Ministers have long recognised the links between e-commerce and data protection, and the need for common legal standards for data protection frameworks. At their meetings in 2002 and 2005, Commonwealth Law Ministers adopted a Model Law on e-Commerce, as well as three inter-related Model Bills: the Model Bill on Freedom of Information, the Model Privacy Bill and the Model Bill on the Protection of Personal Information.

Since the adoption of the Model Bills, more than half of all Commonwealth member countries have either prepared or passed new legislation, or amended existing legislation, specifically related to data protection. However, national laws of member countries vary considerably in terms of structure, the level of protection they provide and their enforcement. While some member countries have dedicated data protection laws, others have legislation under development and some have none at all.

The Commonwealth Connectivity Agenda, adopted in April 2018, and the Commonwealth Cyber Declaration highlight the importance of compatible regulatory regimes to promote good regulatory practice and facilitate transnational trade. Data protection is a core component of the digital regulatory framework. Modernising and aligning the data protection frameworks of Commonwealth countries is therefore an economic as well as a societal and rights-based priority.

At the same time, a number of international standards have emerged or been further developed, including the revised OECD Privacy Guidelines, the Council of Europe' revised Convention 108, the EU's General Data Protection Regulation, the African Union Convention on Cybercrime and Cybersecurity, the revised APEC Privacy Framework, and the ASEAN Framework on Personal Data Protection.

It is important that the data protection laws of Commonwealth Countries align with relevant international standards in order to promote economic growth and development through interoperable legal frameworks. In so far as such international and regional instruments adopt different approaches, the Commonwealth, with its wide geographic membership, provides the opportunity to bridge regional differences, so far as is possible.

These Model Provisions on Data Protection take into account the exponential increase in personal data generation and use that arises from the adoption of new technologies and business models, and the need to build and maintain confidence and integrity in digital trade. They also take into account the importance of a high level of protection of fundamental rights, and seek to protect personal data undergoing processing by controllers in all sectors.

Model Provisions on Data Protection

AN ACT to make provision for the protection of individuals with regard to the processing of their personal data.

BE IT ENACTED by the Parliament *[name of legislature]* of ..... *[name of country]* as follows:

Short title

1. This Act may be cited as the Data Protection Act, 2020.

Part I – Preliminary

2(1) The objective of this law is to guarantee respect for fundamental rights and values when personal data are processed and to facilitate the free flow of personal data within and beyond the territory of Member Countries while taking into account the prerogatives of Member Countries and the rights of local communities.

(2) The objectives set out in Clause 2(1) must be reconciled with other objectives in the public interest and other rights and freedoms, including freedom of expression.

Part II – Interpretation

3. In this Act:

["Binding corporate rules (BCRs)" means obligations entered into by a controller or processor for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a corporate group, or group of enterprises engaged in a joint economic activity;]

"Commissioner" means the individual or individuals appointed to act in an executive role in the supervisory authority;

"data controller" means a natural or legal person, public authority or other entity that exercises decision-making power with regard to data processing;

"data processor" means the entity instructed to process personal data on behalf of the data controller;

"data subject**"** means any natural [or legal] person or group of persons, excluding the data controller, whose personal data are processed;

"filing system" means a set of information relating to individuals that is structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to an individual is easily accessible;

"personal data" means any information relating to an identified or identifiable individual ("data subject");

"personal data processing" means any operation or set of operations carried out on personal data, whether or not by automated means, including the collection, use, retention and disclosure of personal data. Processing does not include the passive transmission of personal data;

"personal data security breach" means any breach of security, irrespective of its cause, that compromises the confidentiality, integrity or availability of personal data or that leads to the unauthorised disclosure of, or access to, personal data;

"sensitive personal data" means [genetic], [biometric] [and health data], personal data to the extent that they reveal [racial], [ethnic] [and regional origin], [parental filiation], [political opinions], [religious or philosophical beliefs], [trade union membership],[membership of clubs and associations] [sex life], [gender identity] and [sexual orientation], and [personal data relating to offences, criminal proceedings and convictions];

"supervisory authority" means the independent public body established in accordance with Clause 24.

Part III – Scope of Act

Material Scope

4(1) This law regulates the automated or partially automated processing of personal data, and the processing of data by non-automated means in a filing system.

(2) This law applies to the processing of personal data of deceased persons for a period of [X] years following their death. The data subject may appoint an agent to provide consent and exercise rights on their behalf during this period.

(3) This law does not apply to the processing of personal data solely for:

a. personal or domestic purposes;

b. [national security purposes;]

c. [law enforcement purposes;]

d. [journalistic, artistic or literary purposes;] or

e. [academic and archiving purposes].

Territorial Scope

5. This law applies to data processing activities:

(1) where the data controller has a relevant establishment within the jurisdiction of the Member Country; or

(2) where a data controller established outside the jurisdiction of the Member Country offers goods or services that entail personal data processing to residents of that jurisdiction or tracks their behaviour within the jurisdiction.

Part IV – Data Protection Principles

Lawfulness

6(1) Personal data shall be processed lawfully.

(2) Personal data is processed lawfully only if and to the extent that it is processed:

a. in accordance with all applicable laws; and

b. on the basis of one of the legal grounds set out in Clause 6(3).

(3) Personal data shall only be processed on the basis of at least one of the following legal grounds:

a. the data subject has [freely] given his or her [specific], [informed] [and unambiguous] consent;

b. [the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps with the data subject's consent prior to entering into a contract;]

c. [the processing is necessary for compliance with a legal obligation to which the controller is subject;]

d. [the processing is necessary for the purposes of the legitimate interest pursued by the data controller or by a third party [,except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject];]

e. [the processing is necessary to protect the vital interests [or fundamental rights and freedoms] of the data subject or of another natural person;]

f. [the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;]

g. [the processing is necessary for any other purpose laid down by law.]

(4) [Where the processing concerns sensitive personal data, the controller shall also meet at least one of the following conditions:]

a. [the data subject has given his or her explicit consent;]

b. [the processing is necessary for the vital interest of the data subject or another person in situations where the data subject is unable to give his or her consent;]

c. [the processing relates to personal data which are manifestly made public by the data subject;]

d. [the processing is required by law for the purpose of an important objective of general public interest.]

(5) Any processing of personal data under Clause 6(3)(c), (f) and (g) and Clause 6(4)(d) must be based on national law in accordance with Clause 22(1).

Fairness

7(1) Personal data shall be processed fairly.

(2) Personal data is processed fairly, if it meets the data subject's legitimate and reasonable expectations and is not obtained fraudulently, through the deception of the data subject or under false pretences.

(3) Personal data is not processed fairly, if it causes unjustified detriment to:

a. the fundamental rights and interests of the data subject;

b. the rights and interests of a group or category of individuals who share significant or protected characteristics; or

c. important objectives of general or public interest.

Transparency

8(1) Personal data shall be processed in a transparent manner.

(2) The controller shall, [at the time the personal data are collected][before the personal data are processed], provide the data subject with at least the following information:

a. the identity and contact details of the controller and of his/her representative;

b. the purpose of the processing as well as the legal basis on which the processing is based;

c. where the processing is based on Clause 6(3)(d), the legitimate interests pursued by the controller;

d. the types or categories of personal data intended to undergo processing;

e. the period of time for which the data will be retained;

f. the data subject's right to subject access under Clause 19;

g. [the identity of any recipient or category of recipients to whom the personal data might be disclosed;]

h. the data subject's right to object to the processing under Clause 21;

i. [the data subject's right to rectification and erasure under Clause 20;]

j. [where the controller intends to transfer the data to a recipient in a third country, territory or international organisation, a description of the relevant safeguards taken by the controller in accordance with Clause 23(2), where applicable;]

k. [the extent to which the controller processes the personal data for the purpose of automated decision-making, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.]

(3) The controller shall provide the information in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

(4) The information shall be provided in writing or other means, including electronic means where appropriate, or orally, where requested by the data subject, and the identity of the data subject is confirmed.

(5) The controller shall provide the information to the data subject free of charge at the time the data is obtained.

(6) Where the data is obtained from a source other than the data subject, Clause 8(2) shall not apply where:

a. the data subject already has the information;

b. it is impossible for the controller to provide the information to the relevant data subjects directly, or where the provision of the information would involve a disproportionate effort;

c. an obligation of professional or statutory secrecy under national law, [which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Clause 22(1)(b)] prohibits the disclosure of the information.

(7) Clause 8(8) shall apply where a controller discloses personal data to another controller, and the following conditions are met:

a. the personal data is disclosed for further processing by the recipient controller for a purpose that is different from the purpose for which they were originally collected; and

b. Clause 8(6) applies with regard to the further processing carried out by the recipient controller.

(8) Where a controller discloses personal data to another controller under the conditions set out in Clause 8(7), he shall make publicly available, in a form that is accessible to any data subject or category of data subjects whose personal data are disclosed in this way, general information about the nature of any further processing undertaken by the recipient controller.

Purpose Limitation

9(1) Personal data shall be processed or collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

(2) Personal data may be processed for a purpose that is incompatible with that for which they have been collected:

a. with the [explicit] consent of the data subject;

b. on the basis of a national law [which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Clause 22(2)];

c. where the data are processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to appropriate safeguards set out in national law for the rights and freedoms of data subjects.

Data Minimisation

10. Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.

Storage Limitation

11(1) Personal data shall be preserved in a form that permits the identification of the data subject for no longer than is necessary for the purpose for which the data are processed.

(2) Personal data may be stored for longer periods where they are processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate safeguards for the rights and freedoms of data subjects.

Accuracy

12(1) Personal data shall be accurate and complete to the extent necessary for the purposes for which they are processed. The controller must take all reasonable steps to erase personal data that are incomplete or inaccurate with regard to the purpose for which they are processed.

(2) Personal data shall be kept up-to-date:

a. a)where this is necessary for the processing carried out by the controller and to the extent that is reasonable;

b. b)at the specific request of the data subject.

Data Security

13(1) Data controllers, and, where relevant, data processors, shall adopt appropriate technical and organisational safeguards to protect personal data against data security risks, including unlawful or unauthorised processing of, and access to, as well as accidental loss, modification or destruction of, the data.

(2) Such safeguards shall take into account and be proportionate to:

a. the likelihood and severity of risks that are presented by such processing;

b. the likelihood and severity of the harm the processing may cause to the rights and freedoms of natural persons as well as important objectives of general and public interest;

c. the sensitivity of the data processed and the context in which they are processed;

d. the state of the art and the cost of implementation.

(3) The controller shall conclude a legally binding contract with the data processor. This contract shall:

a. ensure that the processor acts only on and in accordance with the instructions of the data controller; and

b. apply the obligations set out in Clause 13(1) and (2) above to the processor.

(4) The data controller shall notify data security breaches to the relevant supervisory authority in a timely manner where the breach is reasonably likely to affect adversely the rights and freedoms of individuals.

(5) Where the data security breach is reasonably likely to entail a serious interference with the rights and freedoms of the data subject, the data controller shall notify the breach to the affected data subjects without undue delay.

(6) The supervisory authority shall publish at regular intervals [,but no less than annually,] transparent information about personal data security breaches reported to it.

Accountability

14(1) The data controller shall take all appropriate technical and organisational measures to guarantee their compliance with this Act.

(2) The data controller shall put in place a data practice policy [privacy management programme] where:

a. processing entails a risk to the rights and interests of data subjects[;

b. provided for by national law].

(3) The data practice policy [privacy management programme] shall:

a. give effect to the provisions of this Act;

b. be tailored to the structure, scale, volume and sensitivity of the data controller's obligations;

c. provide for appropriate safeguards based on a privacy risk assessment;

d. be integrated into its governance structure and establish internal oversight mechanisms;

e. contain a clear and understandable record of the data processing operations available to relevant stakeholders;

f. include plans for responding to inquiries and incidents;

g. be subject to continuous monitoring and assessment and updated in light of changes.

(4) The data controller shall provide evidence of their compliance with the provisions of this Act.

[Data Protection Impact Assessment

15(1) Where a data processing operation, or set of operations, is likely to result in a high risk to the rights and freedoms of data subjects, a data protection impact assessment shall be conducted to assess the nature, severity and likelihood of such impact.

(2) [No impact assessment is required if the data processing is compelled by law and an impact assessment was conducted prior to the adoption of the law.

(3) Where the impact assessment indicates that a data processing operation is likely to have an impact on the rights and freedoms of data subjects, the data controller shall ensure that appropriate safeguards are put in place.

(4) Where the data processing is likely to entail a high risk to the rights and freedoms of natural persons, the data controller shall consult the supervisory authority before commencing the processing.

(5) Following the conduct of an impact assessment, data controllers shall continue to monitor periodically any changes to risk and the implementation of the impact assessment.]

[Data Protection Officer

16(1) The data controller [and the data processor] shall appoint or designate a data protection officer. The data protection officer shall be appointed on the basis of their professional expertise and ability to fulfil the functions of the role.

(2) [The data protection officer shall:

a. monitor the data protection compliance of the data controller;

b. advise the data controller on data protection matters and to provide training and support to promote data protection awareness and knowledge;

c. act as a primary point of contact for data subjects and the supervisory authority.]

(3) The data protection officer shall act with sufficient independence when carrying out its tasks and shall be provided with adequate resources to this end. A data controller may designate a member of staff to act as the data protection officer provided the independence of that member of staff is guaranteed.

(4) A group of undertakings or public bodies may appoint a single data protection officer.]

Data protection by design and default

17. The data controller shall design and implement their data processing operations in a way that prevents or minimises the risk of interference with the rights and freedoms of natural persons and ensures compliance with this Act.

[Prior authorisation

18(1) The prior authorisation of the supervisory authority is required to conduct data processing operations that entail a high degree of risk for natural persons. Where this authorisation is not granted, the data processing operation shall not be conducted.

(2) The supervisory authority may identify types of processing or particular factors that are deemed to entail a high degree of risk.]

Part V – Rights of Data Subjects

Right to subject access

19(1) The data subject shall have the right to obtain from the controller, on request [and at reasonable intervals], confirmation as to whether or not the controller processes personal data relating to him or her, and, where that is the case, have that personal data communicated to them [with the following information:

a. the purposes of the processing;

b. the categories of personal data concerned;

c. the recipients or categories of recipient to whom the personal data are disclosed, in particular recipients in third countries or international organisations;

d. the period for which the controller intends to retain the personal data and the criteria used to determine that period;

e. the existence of the data subject's rights under Clauses 20 and 21;

f. the right to file a complaint with the supervisory authority in accordance with Clause 32;

g. where the personal data were not obtained directly from the data subject, all available information on their origin;

h. information about the extent to which the controller processes the personal data for the purpose of automated decision-making, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

i. where the personal data is transferred to recipients in third countries or international organisations, information about the appropriate safeguards adopted pursuant to Clause 23(2) in relation to the transfer].

(2) The controller shall provide a copy of the personal data to the data subject:

a. [without excessive delay] [within [x] [days]; and

b. [free of charge][at a charge that is [not excessive][based on reasonable administrative costs]];

c. in a form that is generally understandable. [Where the request is made by electronic means, the information shall be provided in a commonly used electronic form unless otherwise requested by the data subject.]

(3) The controller shall provide the information referred to in Clause 19(1), except where:

a. the provision of the information would involve a disproportionate effort;

b. an obligation of professional or statutory secrecy under national law, [which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Clause 22(1)(b)]] prohibits the disclosure of the information; or

c. the disclosure of the information would violate the rights and freedoms of an individual other than the data subject[;

d. the request is abusive or vexatious].

(4) If a request under Clause 19(1) is denied, the controller shall provide the data subject with the reasons for, and a means to challenge, such denial.

(5) The controller shall communicate the personal data and the information referred to in Clause 19(1) in an alternative format to a data subject with a sensory disability who requests that it be transmitted in the alternative format if:

a. a version of the personal data and the information already exists in that format; or

b. its conversion into that format is reasonable and necessary in order for the data subject to be able to exercise his or rights under this Part V.

Right to rectification and erasure

20(1) The data subject shall have the right to contest the accuracy of his or her personal data and to have them amended or completed if inaccurate.

(2) The data subject shall have the right to have their personal data erased when such processing is contrary to the provisions of this Act.

(3) [Where personal data has been amended, completed or erased pursuant to Clauses 20(1) or (2), and this amendment, completion or erasure of personal data is likely to have an impact on the data subject, the data controller shall take reasonable steps to inform third parties to whom the personal data has been disclosed. Replications of, and links to, the personal data should then be amended or deleted if required by law.]

(4) The exercise of the right to rectify and erase personal data shall be:

a. free of charge;

b. addressed by the data controller without undue delay; and

c. made subject only to reasonable requirements by the data controller.

(5) If a data controller refuses a request to have personal data amended, completed or erased, it shall communicate the reasons for this refusal to the data subject.

(6) The data controller shall rectify or erase the information referred to in Clause 20(1), except where:

a. the rectification or erasure is likely to seriously impair or render impossible the maintenance of archival records;

b. the rectification or erasure is prohibited by law;

c. the rectification or erasure would violate the rights and freedoms of an individual other than the data subject;

d. [the burden on the data controller is manifestly disproportionate to the impact on the rights and interests of the data subject].

[Right to object

21(1) The data subject shall have the right to object to the processing of personal data on legitimate grounds relating to their situation. This includes, but is not limited to, situations where:

a. [the personal data processing involves wholly or partly automated decision-making;]

b. [the data processing is based on any of the legal grounds set out in Clause 6(3)(d) or (f);]

c. [personal data have been disclosed to third parties.]

(2) Where the data subject objects to the processing pursuant to Clause 21(1), the data controller shall cease the processing, unless it demonstrates that the continued processing of personal data is justified on compelling legitimate grounds, which override the rights and freedoms of the data subject.

(3) [The data subject has the right to object to processing of personal data for direct marketing purposes. Such processing shall cease with immediate effect once the data controller is notified of this objection.]]

Part VI – Exceptions

22(1) To the extent that national law restricts the scope of the controller's obligations under Part IV or the data subject's rights under Part V, such restrictions shall:

a. respect the essence of the fundamental rights and freedoms of the data subject; and

b. constitute a [necessary][reasonable] and proportionate measure prescribed by law in a democratic society to safeguard [national security], [defence], [public security], [the prevention, investigation, detection or prosecution of criminal offences], or [other important objectives of general public interest].

(2) Any legislative measure restricting the scope of the controller's obligations under Part IV or the data subject's rights under Part V shall contain specific provisions, at least, as to:

a. the purposes of the relevant processing or categories of processing;

b. the categories of personal data affected;

c. the scope of the restrictions introduced;

d. the safeguards to prevent abuse or unlawful access or transfer;

e. the controller or categories of controllers to whom the restriction applies; and

f. the permitted storage periods and any applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing.

(3) Data subjects shall be informed about any restriction, unless that is prejudicial to the purpose of the restriction.

Part VII – Cross-border data transfers

23(1) Personal data shall only be transferred to a third country or to an international organisation, if one of the following conditions applies:

a. [the supervisory authority] [the government authority charged with issuing such decisions] has issued a decision confirming that the third country or international organisation ensures an [adequate][equivalent][appropriate] level of protection through its national laws and applicable international treaties or agreements; or

b. the controller or processor has provided appropriate safeguards in accordance with Clause 23(2).

(2) The appropriate safeguards referred to in Clause 23(1) include:

a. [a legally binding and enforceable instrument between public authorities or bodies;]

b. [binding corporate rules;]

c. [standard data protection clauses adopted and published by the supervisory authority;]

d. [an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to comply with that code of conduct, including as regards data subjects' rights;]

e. [contractual clauses between the controller or processor and the recipient of the personal data in the third country or international organisation [subject to authorisation by the supervisory authority].

(3) Where the transfer or set of transfers of personal data to a third country or an international organisation does not comply with the conditions set out in Clause 23(1), it shall take place only on one of the following conditions:

a. [the data subject has given his or her explicit consent to the proposed transfer, after having been informed of the possible risks of such transfers;]

b. [the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;]

c. [the transfer is necessary for important reasons of public interest;]

d. [the transfer is necessary for the establishment, exercise or defence of legal claims;]

e. [the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.]

Part VIII – Independent supervisory authority

Establishment

24(1) An independent supervisory authority shall be established for the purposes of this Act.

(2) Members of the supervisory authority shall be appointed pursuant to a fair and transparent process.

(3) [Where the establishment of a supervisory authority is not feasible because of resource constraints, the function of the supervisory authority may be exercised by another office provided the independence of that office can be guaranteed].

Independence

25(1) The supervisory authority shall act with complete independence and shall be free from all external influence.

(2) The Commissioner shall be appointed for a period of [x] years.

(3) The supervisory authority shall be provided with sufficient resources. This includes the human, technical and financial resources and the physical infrastructure required to discharge the functions and referred to in Clauses 26 to 30.

(4) The Commissioner and any other member of the supervisory authority shall not take any actions, obtain any benefits or engage in any occupation that is incompatible with the role. while in office [and for a period of [x] years after the appointment has ended]. They shall only be dismissed during their term of office in cases of serious misconduct or if they are unable to discharge the functions of their role.

(5) The Commissioner shall be appointed for a minimum term of office of [four years], which may be renewed where provided for by law.

Powers – General

26(1) The supervisory authority shall promote and ensure respect for the obligations set out in Part IV and the rights set out in Part V of this Act by discharging the powers referred to in Clauses 27 to 30

(2) [In discharging these powers, the supervisory authority may apply a risk-based approach to their application by prioritizing the exercise of powers based on the likelihood and severity of the harm that would follow from inaction.]

Advisory Powers

27. The supervisory authority shall exercise the following advisory powers:

(1) provide advice to relevant stakeholders, including public entities, corporate bodies, charities, and individuals, about the rights and obligations set out in this Act;

(2) undertake research and provide guidance on personal data processing activities and their implications and monitor technological developments;

(3) facilitate or deliver educational programmes designed to promote data protection awareness and responsibility;

(4) make public statements in relation to relevant legal, technological and societal developments;

(5) examine relevant proposed legislation and provide input where appropriate;

(6) report to Parliament on matters affecting the processing of personal data, including the desirability of adopting international instruments.

Investigative Powers

28. The supervisory authority shall exercise the following investigative powers:

(1) audit processing by data controllers and data processors;

(2) gather such information as is necessary to discharge their corrective and advisory powers;

(3) inform the data controller or data processor of its intention to conduct an investigation before commencing the investigation;

(4) enter any premises, having obtained relevant judicial authorisation, where required;

(5) conduct inspections on the premises within the authority's powers and examine or obtain copies or extracts of relevant documentation and records;

(6) receive and investigate complaints from a complainant or any person authorised to act on their behalf and make findings in relation to these complaints;

(7) conduct a general inquiry into any law, practice, procedure or technical development that engages data protection;

(8) invite and receive representations on any matter affecting the processing of personal data;

(9) consult and cooperate with other agencies and bodies, as appropriate;

(10) [summon the appearance of persons before the supervisory authority and compel them to produce documents or to give evidence on oath;]

(11) [administer oaths].

Corrective Powers

29(1) The supervisory authority may exercise the following corrective powers:

a. order a data controller to communicate a data breach to the affected data subject(s);

b. suspend data flows to a third-country recipient or an international organisation;

c. deliver an official warning to a data controller or data processor that processing operations may not be compliant with this Act;

d. notify a data controller or data processor if processing is in violation of the Act;

e. impose a temporary or definitive restriction or ban on data processing;

f. order the data processor or data controller to make necessary changes to ensure compliance with the Act, including compliance with the rights of individuals;

g. bring infringements to the attention of judicial authorities and to commence legal proceedings where appropriate[;

h. impose an administrative fine or other sanction in addition to or instead of these corrective measures].

(2) [The Commissioner or supervisory authority has the power to perform any function incidental or conducive to the performance of the above powers.]

(3) The supervisory authority shall discharge their powers in a manner that upholds confidentiality and respects professional secrecy.

International cooperation and mutual assistance

30(1) The supervisory authority shall, where possible in the discharge of its powers, co-operate with and provide mutual support to other national and international authorities. Where more than one supervisory authority is responsible for the exercise of the powers under this Part VIII, those authorities shall jointly identify one competent authority for co-operation purposes and make the identity of this competent authority accessible to any authorities with whom it is cooperating.

(2) The supervisory authority may engage in information exchange and capacity-building with other national and international competent authorities to promote effective data protection. Such activity may include:

a. sharing information on relevant laws and supervisory practices;

b. joint research and capacity building activity, in particular co-operation in developing internationally comparable metrics for policy-making;

c. joint promotion and awareness raising campaigns for data protection;

d. sharing of experience and best practice in enforcement;

e. promotion of the development of international arrangements to promote interoperability of privacy and data protection frameworks.

(3) The supervisory authority may engage in cross-border investigation and enforcement activities with other national and international authorities. Those activities may include:

a. [the establishment of a network to co-ordinate investigations or to conduct joint actions; and]

b. the establishment of a mechanism to ensure the amicable settlement of disputes regarding cross-border processing activity.

Part IX – Sanctions and remedies

Sanctions

31(1) Appropriate judicial and non-judicial sanctions may be imposed on any controller [and processor] that is in breach of any of its obligations under this Act. Such sanctions may include administrative and criminal sanctions.

(2) Any sanctions imposed under Part IX shall be effective, dissuasive and proportionate to the breach of the relevant obligation under this Act.

(3) The investigation of an alleged infringement shall be subject to appropriate procedural safeguards for the parties investigated.

(4) The supervisory authority shall only impose sanctions subject to appropriate procedural safeguards, including an effective judicial remedy, due process and foreseeability.

The right to complain to a supervisory authority

32(1) Data subjects or their representative(s) may lodge a complaint before a supervisory authority, if they consider that a data processing operation violates the provisions of this Act.

(2) A supervisory authority shall assess any complaint under Clause 32(1) and indicate to the complainant [without undue delay] whether it intends to investigate the complaint.

(3) Where there is a risk that a data processing operation is in contravention of this Act and where this raises an issue of general or public importance, a third-party may lodge a complaint before a supervisory authority without instruction from the data subject.

(4) The rights under this Clause 32 are without prejudice to alternative administrative or judicial remedies which the data subject or their representative(s) may invoke.

Right to a judicial remedy including a right to appeal the decision of the supervisory authority

33(1) A data subject, controller or processor [other affected party] shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

(2) A data subject shall have the right to an effective judicial remedy where he or she considers that the actions of the supervisory authority in relation to the complaint have been insufficient or ineffective.

(3) Where a data subject alleges that a controller or, [where relevant a processor], has acted in breach of this Act, the data subject shall have the right to an effective judicial remedy.

(4) The right to an effective judicial remedy is without prejudice to any available non-judicial or administrative remedies available.

Right to seek compensation

34(1) Data subjects who have suffered material or non-material damage as a result of unlawful data processing shall have the right to receive compensation from the data controller (or where relevant, the data processor) for the damage suffered.

(2) The data controller or data processor shall not be liable for any damages under Clause 34(1), if it can prove that it was not responsible for the damage suffered.

(3) [The data subject may appoint a third-party to exercise the right under Clause 34(1).]

Model Provisions on Data Protection: Commentary and International Comparison

Introduction

The Commonwealth Connectivity Agenda adopted in April 2018 and the Commonwealth Cyber Declaration acknowledge the importance of compatible regulatory regimes to promote good regulatory practice and facilitate transnational trade. Data protection is a core component of the digital regulatory framework. Modernising and aligning the data protection frameworks of Commonwealth countries is therefore an economic as well as a societal and rights-based priority.

At the same time, a number of international standards have emerged or been further developed, including the revised OECD Privacy Guidelines, the Council of Europe' revised Convention 108, the EU's General Data Protection Regulation, the African Union Convention on Cybercrime and Cybersecurity (AUC), the revised APEC Privacy Framework, and the ASEAN Framework on Personal Data Protection.

It is important that data protection laws of Commonwealth Countries align with relevant international standards in order to promote economic growth and development through interoperable legal frameworks. In so far as such international and regional instruments adopt different approaches, the Commonwealth, with its wide geographic membership, provides the opportunity to bridge regional differences, so far as possible.

For that reason, Commonwealth Law Ministers adopted the Model Provisions on Data Protection at their meeting in Balaclava, Mauritius, in November 2022. This document is designed to provide additional guidance for Commonwealth Countries when adopting national laws based on the Model Provisions as well as a description of applicable international data protection standards in regions across the world.

Model Provisions on Data Protection: Commentary and International Comparison

Short title

1.[1] This is the introduction to and title of the national Act adopted on the basis of the Model Provisions.

Part I – Preliminary

2. Data protection and privacy and associated rights form the bedrock of data protection laws globally. Guaranteeing respect for these rights is an end in itself. Effective data protection preserves individual autonomy and agency but the regulatory framework also protects against data -driven abuses of power, such as manipulation and exploitation.

   The rights protection guaranteed also, in turn, provides reassurance that data flows will not reduce the level of human rights protection offered to individuals to an unacceptable level and facilitates the free flow of personal data.

   All of the international instruments include provisions that set out their aims and objectives. The approach taken by these instruments can broadly be divided into three groups: those that take a more market-oriented approach (OECD Guidelines, APEC Framework), those that prioritise the fundamental rights and freedoms of individuals, in particular their right to privacy (Convention 108+), and those, whose focus is on balancing economic interests of with those fundamental rights and freedoms (GDPR, AUC and ASEAN Framework).

Part II – Interpretation

3. [*Binding corporate rules*: BCRs establish a common data protection policy and related safeguards designed to enable companies that are members of a corporate group or engaged in a joint economic activity to transfer personal data between themselves in situations where some of those companies may be established in a third country.

   Only the GDPR currently include a reference to BCRs, although Convention 108+ refers to legally binding and enforceable instruments, which may include BCRs.]

1 The numbering of the sections mirrors the individual clauses of the Model Provisions.

Commissioner: Member Countries may designate a Commissioner or Commissioners in order to act as the head of, or executive for, the supervisory authority. Particular conditions may attach to the appointment and qualifications of these individuals (for instance, pursuant to Clause 26(4)) that may not apply to other staff members of the supervisory authority.

The concept of 'Commissioner' does not appear in the International Instruments. However, the GDPR and Convention 108+ clearly implicitly envisage a distinction between executive members of the supervisory authority and other staff members. For instance, Convention 108+ refers to "staff and members".

Data controller: a data controller is the person or entity that makes key decisions regarding the processing of personal data, for instance, determining the objectives of the processing and engaging a suitable data processor.

Data controllers can be both public and private sector operators. Individuals can be data controllers however they may benefit from exemptions from this law and exceptions to it in recognition of their right to freedom of expression and their limited ability to comply with its provisions.

All international instruments, with the exception of the ASEAN Framework, refer to a 'data controller' or personal information controller'.

Data processor: the primary responsibility for compliance with this law rests with the data controller. Data controllers must instruct capable data processors to process personal data in accordance with the objectives they have specified and in a manner compatible with the law (see Clause 14(3)).

While data controllers determine the purposes of processing, in practice, data processors may have more technical knowledge than controllers and may influence the means in which personal data are processed. Data controllers and data processors therefore have some shared responsibilities, for instance to ensure the security of personal data processing (see Clause 14(2)). In light of their distinct roles in the data processing process, there may be responsibilities that apply to data processors that do not apply to data controllers and vice-versa. For instance, data processors should keep a record of the personal data processing operations they are asked to undertake on behalf of the data controller.

Only the GDPR and Convention 108+ refer directly to the concept of data processor.

Data subject: the data subject is a beneficiary of the data protection framework. A clear dividing line between data subjects and data controllers is maintained to ensure that data subjects are not unduly burdened by onerous duties and to guarantee the effective protection of the rights of all data subjects.

[The regulation of personal data processing protects legal persons. Legal persons may be harmed by information and power asymmetries in personal data processing and poor data governance and security practices. The extension of protection to legal persons simplifies the regulatory environment for data controllers and data processors and minimises the risk of arbitrary differentiation between different forms of corporate entities.]

The GDPR, Convention 108+, the AUC and the OECD Guidelines used the term of art 'data subject' whereas the ASEAN and APEC Frameworks refer to individuals. Most legal frameworks refer to data subjects as 'individuals' with the exception of the GDPR, which leaves open the possibility that a data subject can be a juristic/legal person.

Filing system: Manual data processing falls within the scope of this law only to the extent that it is possible to link this processing to an individual without significant difficulty. The risks for data protection primarily lie in relation to such data processing.

The GDPR, the AUC and Convention 108+ all define a 'file' or 'filing system'.

Personal data: an individual is identifiable if they can be identified, directly or indirectly, by information related to them. This could include, among other things, their name or any other descriptor related to their physical, physiological, genetic, mental, economic, cultural or social identity, an identification number, data about their location, an IP address or other online identifier.

Most recent international instruments refer to the term "personal data". This now includes the GDPR, Convention 108+, the AUC, the revised OECD Guidelines and the ASEAN Framework. Only the APEC Framework continues to use the term "personal information".

Personal data processing: the processing of personal data is a broad and open-ended concept. It is difficult to identify activities undertaken in relation to personal data that do not constitute processing. Nevertheless, where an entity merely transmits personal data on behalf of another and does not initiate the transmission; select the recipient or exercise any substantive influence over the personal data transmitted, this will not constitute processing.

The AUC, the APEC Framework and the OECD Guidelines specify a range of activities that fall within their scope. The GDPR and Convention 108+ contain a unitary definition of personal data processing.

Personal data security breach: a data security breach can occur as a result of unlawful activity, accident or poor system design. The root cause of data security breaches – such as outdated security safeguards; inadequate governance and oversight of data processing; or sub-standard employee training – may be attributable to the data controller or data processor.

Confidentiality breaches involve the unauthorised or accidental disclosure of, or access to, personal data.

Integrity breaches involve the unauthorised or accidental alteration of personal data.

Availability breaches involve the unauthorised or accidental loss of access to, or destruction of, personal data.

As a general rule, a data security incident that breaches data security principles, only constitutes a breach under these Model Provisions where *personal* data are compromised.

The OECD Guidelines, the APEC Framework, Convention 108+ and the GDPR all contain data breach notification requirements. However, only the GDPR defines a personal data security breach.

Sensitive personal data: special rules apply to the processing of sensitive personal data, which could constitute a greater risk for the rights and freedoms of data subjects.

A definition of the term "sensitive personal data" is included in the AUC. The GDPR and Convention 108+ refer to "special categories of personal data".

Supervisory authority: The supervisory authority is an independent authority endowed with [advisory, investigative and corrective powers as set out in Clauses 27 to 29]/[advisory and investigative powers as set out in Clauses 27 and 28] in relation to processing activities within the scope of this law. The supervisory authority shall also receive complaints from data subjects.

The OECD Guidelines, the APEC Framework and the GDPR include definitions of the "supervisory" or "privacy enforcement authority".

Part III – Scope of Act

Material Scope

4(1) Automated personal data processing is used by data controllers to gain insights into the data subject and to derive inferences about them. Such insights and inferences may be of societal and commercial value. However, they may also threaten established rights, such as human dignity, privacy and freedom of association, and values, such as human agency and social cohesion. This law applies to such processing in order to negate or mitigate these effects.

While non-automated processing will not facilitate insights and inferences regarding data subjects on the same scale as automated data, such processing can engage the rights of individuals when it enables easy access to their personal data. Furthermore, excluding non-automated processing entirely from the scope of application of this law would lead to potential lacunae in the protection offered and inconsistency in their application (for example, if the rules are circumvented by using non-automatic processing for purposes which are detrimental to public or private interests). Non-automated processing of data in a relevant filing system therefore falls within the scope of the law.

The GDPR, the AUC and Convention 108+ all explicitly apply to automated and non-automated processing where the personal data are part of a file. The Memorandum to the OECD Guidelines also endorses this approach.

(2) As digital technology plays an increasing role in daily life, individuals attach more significance to their digital identity and assets. While the individual will no longer be able to benefit from their rights once deceased, post-mortem processing of personal data may impact upon their memory, dignity and freedom of testation. For instance, the processing of personal data of the deceased in order to profile them may have an impact on proximate third parties. For this reason, this law applies to the personal data of the deceased following their death, with the period of protection to be specified by the Member Country in its national law. The deceased will be able to appoint an agent to act on their behalf under this law during that period.

The international instruments surveyed do not contain a legal provision on post-mortem privacy. The GDPR leaves this possibility open to Member States and several have availed of it (Denmark; France; Hungary; Italy; Slovakia; Spain).

(3) This law does not apply to processing by a data controller for personal or domestic purposes. While the digital publications of individuals have the capacity to impact negatively on data subjects, this negative impact must be considered alongside their freedom of expression which includes the freedom to converse. In striking a balance between these rights, the impact of the processing on the data subject should be taken into consideration. Relevant factors might include: the nature of the personal data processed, in particular whether it was sensitive personal data, and the frequency and intensity of the processing.

This law also includes the option for Member Countries to exempt processing for other public policy purposes from its material scope. In practice. An intentional decision was taken not to include provisions relating specifically to processing for those purposes (for example, national security) in this law. However, Member Countries may decide to adopt specific rules that govern processing for those purposes or may exempt that processing entirely from the scope of data protection law, subject to compliance with individual rights and freedoms.

The GDPR, Convention 108+ exclude household processing from their scope, the AUC contains a similar provision and the APEC Framework excludes individuals processing for such purposes from the scope of 'data controller'.

There is differentiation in terms of exclusions beyond this: APEC has 'limited application to publicly available information' and ASEAN and the OECD Guidelines give a large degree of discretion to States.

In both the GDPR and Convention 108+ processing for special purposes (eg. Journalistic purposes) do not fall outside of the scope of the rules but is rather subject to exemptions and rights-balancing within the scope of the rules.

Territorial Scope

(5) This provision seeks to ensure the effective, complete and practical protection of data subjects, to promote fair regulatory competition by discouraging offshoring activity and to respect comity between Member Countries. The provision provides a minimum standard of protection. However, Member Countries are free to expand the territorial scope in accordance with their national rules on extraterritorial application of national laws.

A relevant establishment is one where decisions regarding the purposes and means of data processing are taken [or inextricably linked activities take place]. This provision applies irrespective of the place of residence or nationality of affected data subjects.

Establishment entails the effective exercise of activities through stable arrangements in the jurisdiction. In assessing whether activity is stable and effective it is relevant to consider the nature of the economic activity considered. The legal form of such arrangements is a factor for consideration but not decisive.

If a data controller targets residents of the Member Country by offering them goods or services (such as online content) or monitors their behaviour, then the legal framework applies irrespective of its place of establishment. This provision ensures that the framework applies when the processing affects resident data subjects.

The data controller must direct goods or services, including those provided at no monetary cost, to the data subject in a targeted way for this provision to apply. This requires an objective contextual assessment of whether the data controller has manifested an intention to establish relations with those data subjects. Relevant factors might include whether the currency, language and contact details are tailored to the territory or whether marketing or advertising campaigns were directed towards the jurisdiction. The mere accessibility of the goods and services from the jurisdiction is not, on its own, sufficient to evidence targeting.

The legal framework also applies when the data controller tracks a data subject within the territory. Such tracking could take place through mechanisms such as WiFi tracking, web cookies, device or browser fingerprinting, or other tracking technologies.

There is no consensus in the International instruments on territorial scope of application. The OECD Guidelines and APEC Framework do not address territorial scope directly. The AUC applies to processing undertaken in the State's territory; Convention 108+ applies to data subjects within the jurisdiction. The GDPR applies to data controllers and data processors established in the EU and to those monitoring residents or offering them goods or services.

Part IV – Data Protection Principles

The data protection principles set out in Part IV are designed to align with current international standards. However, Member Countries may choose to include additional principles if their national context requires it.

Lawfulness

6(1) This principle recognises that the processing of personal data is prima facie prohibited unless it complies with the lawfulness principle.

The requirement that personal data must be processed lawfully is well established in nearly all international data protection instruments although the interpretation of "lawfulness" varies.

(2) The obligation to process personal data in accordance with all applicable laws acknowledges that data controllers (and processors, where appropriate) must not only process personal data in accordance with data protection laws; in doing so they must also comply with other applicable laws, including statutory and common law, constitutional laws, the fundamental rights and freedoms of individuals and any other legal principles that would be interpreted and taken into account by competent courts. This means that the processing of personal data cannot be authorised by the existence of a legal ground alone, if it is otherwise unlawful, for example, because it results in a violation of specific legislation or common law principle, the breach of an enforceable contract or an infringement of fundamental rights.

The concept of "lawfulness" as a requirement to comply with the wider legal order of a country arises from the way the GDPR is applied in the EU member states. However, it is likely that in most countries, data processing activities that violate other applicable laws (for example, copyright law, criminal laws, etc.) would also be considered unlawful under data protection laws.

While rights-based instruments generally require all types of processing to comply with at least one of an enumerative list of legal grounds, more market-oriented instruments often focus on a more general obligation to collect personal data "by lawful means", often without further specifying what constitutes such means.

(3) Personal data processing can be justified either on the data subject's consent or if the processing is necessary for a particular objective. The necessity requirement does not imply that the processing must be the only way to achieve that objective. However, it prohibits the collection, use, storage and disclosure of personal data where this is only incidental to the objective.

This means that controllers must consider if the processing of personal data is truly necessary to achieve their objective when adopting new technologies or business models. Processing will generally not be necessary, if the controller's objective can equally be achieved by other, less intrusive means.

The data subject's consent as a means to authorise the processing of their personal data is included in all international data protection instruments.

The GDPR, the APEC Privacy Framework and the AUC include one or more necessity grounds, while Convention 108+, the OECD Privacy Guidelines, the APEC Privacy Framework and the ASEAN Framework also include a more general provision that authorises processing "by the authority of" or if "laid down in" law.

a. *Consent:* [Consent is freely given if it represents a voluntary decision by the data subject. This means that it must not be obtained by direct or indirect coercion of any kind. For example, consent cannot provide a valid legal ground for processing that is mandated by law. Similarly, consent should not be regarded as freely given, if the data subject has no genuine or free choice, for example, where there is an imbalance of power or a situation of subordination between the data subject and the controller and where, consequently, the data subject's refusal to give their consent would be likely to result in them suffering some kind of detriment.]

[To be specific, consent must be connected with the processing operation it seeks to authorise, including the type of data processed, the type of processing, and the purpose of the processing. Where processing involves multiple types of data or processing activities, or has multiple purposes, consent must be given for all of them.]

[For consent to be informed, the data subject must have been provided with all essential information concerning the fundamental aspects of the processing in the light of the context of the specific case. The data subjects must be in a position where they understand what they are agreeing to in order to enable them to make an informed decision. This means that the controller must at least provide information about the controller's identity and the purposes of the processing for which consent is sought, and the type of data the controller will collect and use. In addition, the controller should highlight the fact that the data subject may withdraw his or her consent, provide information about the use (if any) of the data for automated decision-making, and, where relevant, information about the possible risks of any data transfers to recipients in third countries that may not provide equivalent protection of the data. This information should be provided in clear and plain language.]

[Consent is unambiguous if it is given either by making a statement or indicated by a clear affirmative action of the data subject. A statement can be made orally or in writing. An affirmative action includes any deliberate action with which the data subject signifies their approval of the data processing. In an online context, this can include, for example, ticking a box or actively setting or amending technical settings that determine the way in which the data subject's personal data will be processed. Silence, pre-ticked boxes, unamended default settings or merely continuing the ordinary use of a website or service does not constitute consent.]

Only the GDPR and Convention 108+ have taken steps to define consent as "freely given, specific, informed and unambiguous".

While the GDPR and Convention 108+, the OECD Privacy Guidelines (with regard to "use" only) and the ASEAN Framework view consent as one of two or more legal grounds of equal status, the AUC privileges consent as a condition while at the same time providing for broad exceptions to that condition.

The APEC Privacy Framework and the OECD Privacy Guidelines (with regard to data collection only) require consent only "where appropriate".

b. *Necessary for the performance of a contract:* This condition specifically applies in situations where personal data is collected in the context of the performance of a contract between the controller and the data subject. While there may be some overlap with the consent condition, the data subject's consent to the contract itself is sufficient to authorise any processing necessary for the performance of that contract.

   This condition is included in the GDPR and the AUC. The APEC Privacy Framework includes a similar provision that authorises processing "when necessary to provide a service or product requested by the individual.

c. *Necessary for compliance with a legal obligation:* Legal obligations that justify the processing of personal data may include data collection, storage or disclosure requirements to comply with a statutory or common law obligation, for example in the context of employment law, criminal law, public administration, tax or health and safety. The legal obligation must constitute a [necessary and proportionate][reasonable and proportionate] measure in a democratic society (see Clause 6(5)). Controllers should be able to identify and demonstrate the specific obligation they rely on for their processing activities.

   This condition is included in the GDPR and the AUC.

d. *Legitimate interest:* A legitimate interest includes any real and current interest of a controller or a third party that is sufficiently clearly articulated. To be legitimate, it must be in accordance with both data protection law and other laws. Legitimate interest may include, for example, commercial interests (revenue generation, marketing, customer engagement and retention, enforcement of contracts, prevention of fraud), interests in upholding and enforcing laws and regulations, the controller's individual rights and freedoms, security interests, etc.

   [The legitimate interest of the controller or third party must be balanced against the interests or fundamental rights and freedoms of the data subject. The controller must carry out a balancing test to establish whether

the data subject's interests override those of the controller or the third party. This should take into account the benefits for the controller or a common or public interest in the processing, any risks associated with the processing and the effect it would have on the data subject, if that risk materialised, the nature of the data being processed and the way in which they are processed, the relationship between the controller and the data subject in terms of resources and negotiating power, and the reasonable expectations of the data subject.]

This condition is included in the GDPR.

e. *Vital interests:* Processing of personal data is necessary to protect the vital interest of the data subject or another natural person, if it is necessary to protect their life.

The "vital interest" condition is included in the GDPR and the AUC although the latter only takes into account the interest of the data subject. Unlike the GDPR, it also authorises processing that is necessary for the protection of the fundamental rights and freedoms of the data subject or of another natural person.

f. *Performance of a task carried out in the public interest or in the exercise of official authority:* This public interest condition is most relevant for the processing activities of public authorities or for private organisations acting as, or on behalf of, public bodies. Those activities must normally be mandated by statutory or common law. Those laws must constitute a [necessary and proportionate][reasonable and proportionate] measure in a democratic society (see Clause 6(5)). Member countries might consider introducing specific provisions that determine, among other things, the specific purpose of the processing, the types of data and data subjects that are covered by the processing and other related questions.

This condition is included in the GDPR and the AUC.

g. *Other purpose laid down by law:* Member countries may introduce specific laws that authorise the processing of personal data for certain purposes. For example, the sharing of health data for research or archiving purposes, or the collection, retention or sharing of certain types of personal data for the prevention, detection or prosecution of crime. Those laws must constitute a [necessary and proportionate][reasonable and proportionate] measure in a democratic society (see Clause 6(5)).

This condition or a condition of similar effect is included in Convention 108+, the OECD Privacy Guidelines, the APEC Privacy Framework and the ASEAN Framework.

(4) [As the processing of sensitive personal data carries a greater risk for the rights of the data subject, such processing is only lawful, if certain additional conditions are met.]

All of the rights-based instruments (GDPR, Convention 108+ and AUC) include provisions that give special protection to sensitive personal data, while market-oriented instruments make no distinction in the level of protection. However, the Original Explanatory Memorandum to the OECD Privacy Guidelines states that member economies are able to take into account different degrees of sensitivity with regard to different types of data depending on their own legal cultures.

a. [*Explicit consent:* Consent is explicit, if the data subject makes an express statement consenting to the processing that goes beyond an act from which consent could be inferred. Explicit consent could include a written or oral statement, sending an email or uploading a signed document, or using an electronic signature or other technical means like two-factor authentication.

   Both the GDPR and the AUC permit the processing of such sensitive personal data on the basis of the data subject's explicit or written consent.]

b. [*Vital interest:* The vital interest condition will often be relevant with regard to the processing of health data, which is defined as "sensitive personal data". Controllers cannot rely on the vital interest condition with regard to sensitive personal data, if the processing is carried out against the express wishes of the data subject, for example, if the data subject has refused to give his or her consent. The condition will only apply if the data subject is unable to give consent because of physical or legal impediments.

   This condition is included in the GDPR and the AUC.]

c. [*Personal data manifestly made public*: Sensitive personal data are manifestly made public by the data subject him-or herself, if they are deliberately placed in the public domain, where they can be accessed by a[n] [significant] [indefinite] number of individuals. It is up to Member Countries to decide, which standard to apply. Even if this condition applies, the processing of sensitive personal data must still be based on one of the conditions in Clause 6(3) to be lawful.

   This condition is included in the GDPR and the AUC.]

d. [*Required by law:* Important objectives of general public interest may include, among other things, national security, defence, public security, the prevention, investigation, detection or prosecution of criminal offences, public health, an important economic or financial interest of the member country, the need to safeguard specific rights of the controller or of the data subject in the field of employment and social security and social protection law, archiving in the public interest, scientific or historical research, statistical purposes, the establishment, exercise or defence of legal claims, the protection of judicial independence and judicial proceedings, and the protection of the data subject or the rights and freedoms of others. Any law on which processing is based must constitute a necessary and proportionate measure in a democratic society (see Clause 6(5)).

   One or more conditions that permit(s) the processing of sensitive personal data for specific objectives of public interest is included in the GDPR, Convention 108+ and the AUC.

   While the GDPR and the AUC each include an enumerative list of specific conditions, Convention 108+ emphasises that such processing must be subject to "appropriate safeguards enshrined in law" designed to "guard against the risks that the processing may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination".

   None of the international instruments specifies the particular safeguards that must be adopted.]

(5) Processing of personal data that is necessary to comply with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or that is required by law should be mandated by a national law, including statutory and common law, which is subject to the constitutional safeguards that apply in the Member Country. In accordance with Clause 22(1), those laws must constitute a [necessary and proportionate][reasonable and proportionate] measure in a democratic society.

The GDPR provides that the processing that is necessary for compliance with a legal obligation to which the controller is subject and processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller must be based on EU or member state law. This law must meet an objective of public interest and be proportionate to the legitimate aim pursued.

Fairness

7(1) This principle recognises that even if personal data is processed lawfully on the basis of one of the legal grounds enumerated in Clause 6(3), the processing may still be considered unfair, if it goes beyond what the data subject has reasonably expected, if the personal data was obtained through fraud, deception or on false pretences (see Clause 7(2)), or if it has unjustified adverse effects on the data subject, a group of data subjects or important objectives of general or public interest (see Clause 7(3)).

The concept of "fairness" is well established, if largely undefined, in international data protection instruments. All of the comparable international instruments include a fairness requirement save for the ASEAN Framework.

(2) The data subject's reasonable expectations may be exceeded, if a controller has collected the personal data for a very general purpose (for example, "providing an online service") but then processes it in a way the data subject could not envisage at the time of collection (for example, to develop or support new features of the online service of which the data subject was not aware).

Personal data may be obtained fraudulently or on false pretences if the data subject is deceived, for example, about the identity of the data controller, the type of data that is collected or processed, the purposes for which the data is processed, whether the data is disclosed to third parties and the identity of those third parties, or whether the data is transferred to countries, territories or international organisations that may not provide a[n] [adequate][appropriate] [equivalent][comparable] level of protection.

There is some agreement that to be processed fairly, personal data must not have been obtained fraudulently (AUC) or on false pretences (APEC Privacy Framework).

(3) The processing may cause unjustified detriment to the data subject or others, when the benefit he or she derives from the processing is significantly outweighed by any material or immaterial harm, including long-term harm, he or she may suffer as a result. This could be the case, for example, where individual data subjects share personal data with a controller in exchange for the provision of a service, or to obtain a discount or because of another incentive, but where the controller then uses the data to profile and categorise data subjects in a way that may result in a subsequent price increase, service deterioration or denial of service for some of them.

Finally, the processing may cause unjustified detriment to important objectives of general or public interest, if the controller processes the data of a significant group of individual data subjects in a way that adversely affects important objectives of a democratic society (for example, where profiles of individual data subjects that were created for the purpose of commercial advertising are subsequently used for political microtargeting with malicious intent, e.g. to rig an election or to destabilise the political system of a particular country).

There is currently no consensus on what constitutes unfair processing because it causes unjustified detriment to data subjects, third parties or important objectives of general or public interest. Some guidance is available in this regard from competent EU data controllers (see, for example, the Guide to the General Data Protection Regulation" published by the UK's Information Commissioner's Office).

Transparency

8(1) This principle recognizes that data subjects have a right to be informed about the way in which and the purposes for which their personal data is processed, how long the data will be retained and who they will be shared with.

The transparency principle is linked to the fairness principle in that the information provided to the data subject about the processing determines the data subject's reasonable expectations.

In situations where the processing is based on the data subject's consent, transparency is linked to the requirement that consent must be informed and specific.

Transparency also facilitates demonstrable accountability and the exercise of the data subject's rights to subject access, rectification, erasure and to object to the processing.

Transparency requirements are included in all international data protection instruments. Convention 108+, the GDPR and the AUC include specific transparency principles, supported by detailed information requirements.

The APEC Privacy Framework requires data controllers to provide "clear and easily accessible statements about their practices and policies with respect to personal information" and includes an enumerative list of information requirements that controllers must comply with.

The OECD Privacy Guidelines provide that personal data must be processed "with the knowledge of the data subject" but without prescribing the type of information controllers must provide.

Similarly, the ASEAN Framework mandates controllers to inform data subjects of "the purpose(s) of the collection, use or disclosure of his/her personal data" but without laying down specific information requirements.

(2) The information requirements imposed on the controller as part of the transparency principle are intended to ensure that the data subject is in a position to evaluate whether the controller complies with the data protection principles and to alert him or her to the existence of applicable data subject rights. This is particularly important with regard to the data subject's right to object to the processing of his or her personal data.

To facilitate the evaluation of the controller's compliance with the data protection principles, the data subject must be informed [before the processing begins][at the time of collection of the data], at least, about the legal grounds on which the processing is based ("lawfulness"), the categories of data concerned ("data minimisation"), the purposes of the processing ("purpose limitation"), and the retention period ("storage limitation").

Information about data subject rights is designed to increase the data subject's awareness of those rights with a view to facilitating their exercise, where appropriate. Information about the controller's identity, location and contact information will facilitate the exercise of those rights against the correct addressee.

Information about the recipients or categories of recipients to whom the data are disclosed allows the data subject to assess and to use available legal remedies to prevent such disclosure, where appropriate. This is the case, particularly, where the data are transferred to third countries, territories or international organisations that may not provide equivalent or adequate protection and where the risk that those data are accessed by third parties in ways that might violate the data subject's fundamental rights and freedoms may therefore be higher.

Nearly all of the international data protection instruments include detailed information requirements although the extent of those requirements varies. All instruments, either explicitly or impliedly, require controllers to inform data subjects about their identity. There is also broad international agreement that data subjects must receive information about the fact that, and the purposes for which, the data are processed, the categories of data processed, and the (types of) persons to which the data may be disclosed, the period for which the data may be stored and any transfer of data to third countries.

Most instruments (AUC, APEC Framework, Convention 108+, and the GDPR) also mandate the provisions of information about the existence of data subjects' rights and how to exercise them.

(3) Controllers must tailor the information to the intended audience. In particular, where controllers process personal data of children or other individuals whose cognitive or physical abilities may be diminished, the information must reflect the abilities of the intended recipient.

Most international instruments (GDPR, OECD Guidelines, APEC and ASEAN Frameworks) provide that the information must be "easily accessible" or "readily available".

(4) The information should be provided in a durable format that the data subject can easily access or retain unless the data subject specifically requests the information to be provided orally.

In practice, it is often advisable to provide the information by the same means by which the personal data are collected. This means that if personal data is collected, for example, via a smart phone, the information should be provided in a form that is easily accessible on that device.

In this context it may be useful to consider the "layering" of information, that is, the provision of information through a combination of short notices, icons and longer more detailed privacy policies.

Only the GDPR includes a formal requirement that controllers must provide the information in writing. However, this is suggested as advisable in some circumstances in the commentary on the APEC Framework.

(5) The information should generally be provided at the time the personal data are first processed. In most cases this is likely to be the time at which the controller obtains the information, either from the data subject or from a third party.

The information must be provided free of charge, including pecuniary and non-pecuniary consideration.

The GDPR, the APEC Framework and the AUC specifically provide that the information should/must be made available before or at the time of collection.

The GDPR is the only international instrument that requires controllers to provide transparency information free of charge although several instruments state that controllers must not charge a fee for responses to a specific subject access request. The Original Explanatory memorandum to the OECD Guidelines states that individuals must be able to obtain the information "without unreasonable cost".

(6) In cases where the data are not obtained from the data subject directly but from another source, it is often difficult, or would involve disproportionate effort, to provide the data subject with the relevant information.

Where the controller seeks to process the data for the original purpose notified to the data subject, it is not always necessary to provide the information, as the data subject may already have it.

In certain cases, the data are obtained and disclosed under conditions of confidentiality or secrecy. In this case, the purpose of the disclosure may be adversely affected, if the data subject is provided with the information. This may, for example, be the case, where a law enforcement agency obtains the data in the context of a criminal investigation. However, any measure that authorises the processing of personal data under conditions of secrecy or confidentiality must itself be a necessary and proportionate measure in a democratic society to safeguard a limited range of public interest objectives set out in Clause 22(1)(b) below.

Some international instruments distinguish in their information requirements between cases where the data are obtained directly from the data subject and those where the data are obtained from another source. Only the GDPR sets out a separate list of requirements for either of these scenarios while other instruments (or their explanatory memorandums, reports or commentary) merely make allowances for the greater difficulties that controllers may find themselves in, if they obtain personal data from third parties. For example, convention 108+ provides that in those cases controllers must not comply with the information requirements, "where the processing is expressly prescribed by law or this proves impossible or involves disproportionate efforts". Equally the APEC Framework states that it may not be necessary to provide the notice to the data subject, if the information is "publicly available".

(7) In cases where the data are not obtained from the data subject directly but from another source, and where the controller seeks to process the data for a purpose that is different from that for which they were originally collected,

the controller's obligation to provide the information may be replaced with a corresponding obligation on the disclosing party to provide general information about the controller's processing activities.

There are no equivalent provisions in international instruments that would require the disclosing controller to provide information about the processing activities of the recipient controllers to the data subjects.

However, this approach is often taken in practice, for example, in the context of a transfer of personal data in the context of a merger and acquisition transaction where the seller will be contractually obliged to notify data subjects of the transfer and subsequent processing activities on behalf of the buyer.

(8) None of the international instruments include comparable provisions. However, the OECD Guidelines highlight "the need for a "general policy of openness about developments, practices and policies with respect to personal data".

Purpose Limitation

9(1) The purpose limitation principle connects the processing of personal data to the purpose for which those data were originally collected. As a general rule, further processing of the data for other incompatible purposes is prohibited.

The controller must specify the purpose for which the data are collected no later than at the time of data collection. The requirement to specify the purpose is closely linked to the transparency requirement set out in Clause 8(2)(b)].

Any purpose must also be legitimate. As with the lawfulness principle (Clause 6(1)), this goes beyond the requirement for a legal ground under Clause 6(3) and extends to other areas of law. This means that the legitimacy of a given purpose can change over time, if scientific or technological developments lead to changes in the regulatory framework or societal or cultural attitudes.

A general purpose limitation principle is included in all international data protection instruments, although the scope of this principle varies. While a majority of instruments (OECD Guidelines, GDPR, Convention 108+ and AUC) specifically provide that purposes must be "specified", others (APEC and ASEAN Frameworks) only include a transparency requirement.

The GDPR, Convention 108+ and the AUC contain a requirement that the purposes for which data are collected must be legitimate, while some other instruments include other quality requirements.

In particular, the ASEAN Framework only permits the collection, use and disclosure of data "for purposes that a reasonable person would consider appropriate", while the APEC Framework requires controllers to look at "the nature of the personal data, the context of collection, the individual's expectations and the intended use of the information".

The OECD Guidelines do not include any quality requirements with regard to the purposes for which personal data may be collected.

(2) Data originally collected for a specific and legitimate purpose may be further processed for another incompatible purpose in limited circumstances. This includes processing with the data subject's explicit consent or where the processing is mandated on the basis of a national law.

However, any such law must itself constitute a necessary and proportionate measure to safeguard one of the public interest objectives set out in Clause 22(2).

Data may also be further processed for archiving, scientific or historical research, or statistical purposes, provided that national law provides for appropriate safeguards for the rights and freedoms of data subjects.

Such safeguards could include technical and organisational measures that ensure respect for the data protection principles (including transparency, data minimisation, storage limitation and data security) and the rights of the data subject. Safeguards may include, *inter alia*, anonymisation and pseudonymisation.

While all international instruments include restrictions on further incompatible processing of personal data, the scope of those restrictions varies.

The OECD Guidelines and the APEC Framework permit a deviation from the original purpose with the consent of the data subject or by the authority of law.

The APEC Framework also permits further processing for incompatible or unrelated purposes "when necessary to provide a service or product requested by the individual".

The GDPR and Convention 108+ include exceptions to the compatible use requirement where the data are further processed for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes. However, such further processing must be subject to appropriate safeguards.

The AUC contains no exceptions to the compatible use requirement.

Data Minimisation

(10) The data minimisation principle ensures that controllers only collect and process the minimum amount of personal data necessary to achieve the purpose for which those data were collected. The collection or further processing of data that do not meet this requirement is unlawful.

What is adequate, relevant and not excessive will depend on the circumstances of collection, the type of data collected and the purpose for which the controller plans to process the data.

Data are likely to be excessive and/or irrelevant when they are not required to achieve the purpose for which they are collected or if that purpose could equally be achieved by other means, even if this results in a more onerous financial or organisational burden on the controller.

Data may be inadequate when they are insufficient to allow the controller to achieve the specified purpose. In those cases, controllers may need to collect more or different data than they had originally anticipated to ensure that any decisions they make on the basis of those data is based on a sufficiently complete picture of the individual data subject.

Controllers must assess what constitutes the right amount of personal data with regard to all categories of data collected and all purposes for which they plan to process those data. They should also periodically review their assessment to ensure that they still comply with this principle.

While data minimisation requirements are included in the majority of international instruments, the scope of those requirements varies. The GDPR, Convention 108+ and the AUC contain the most restrictive minimisation principles, stipulating that personal data collected or undergoing processing must be adequate, relevant and (in the case of Convention 108+ and the AUC) not excessive. The GDPR goes even further and requires that data must be "limited to what is necessary" in relation to the purposes for which they are processed.

Both the OECD Guidelines and the APEC Framework contain somewhat less restrictive data minimisation requirements, providing merely that personal data must be "relevant" to the purposes for which they are collected or to be used.

The ASEAN Framework does not include a data minimisation principle.

Storage Limitation

11(1) The storage limitation principle ensures that controllers will only be able to keep personal data in identifiable form for as long as those data are actually needed to achieve the purpose for which they were collected or further processed. The continued storage of identifiable personal data beyond that point is unlawful and controllers are then required to either anonymise or to delete the data.

Retention periods can be determined by legal, business and/or practical requirements. For example, an employer may be required to keep certain employee data even after the employee has left their employment to comply with tax law requirements or to deal with future pensions arrangements or to defend against future legal claims.

In accordance with the data minimisation requirement the amount of data stored must be limited to what is needed for the relevant purpose.

Controllers must consider how long they need to store personal data and must justify any continued storage with respect to one or more specific purposes. They should also periodically review their assessment to ensure that they still comply with this principle.

Where the data subject exercises their right to subject access (see Clause 19 below), the controller may retain the relevant data until he or she has complied with that request. However, controllers should not retain personal data beyond what is reasonable under the storage limitation period in expectation of future subject access requests.

There is a marked difference in relation to storage limitation between the market-based instruments (OECD Guidelines, APEC and ASEAN Frameworks) and the rights-based instruments (GDPR, Convention 108+ and the AUC). While the former include no storage limitation requirements, the latter do.

(2) Where personal data are processed solely for archiving, scientific or historical research, or statistical purposes, longer retention periods may be appropriate. In this case, controllers must implement appropriate safeguards for the rights and freedoms of data subjects to ensure that the data are protected from unlawful access and accidental loss or destruction and that they are not used for other purposes during this period. One of those safeguards may be the pseudonymisation of the data during the extended storage period.

Accuracy

12(1) This principle recognises the importance of accurate and complete personal data for the controller's processing activities. Decisions made on the basis of incomplete and inaccurate data are likely to affect the interests of both the controller and the data subject. The controller must delete inaccurate and incomplete data that do not serve the purpose for which they were collected or further processed.

However, the accuracy requirement is limited to those specific purposes. Inaccurate data that does not affect those purposes does therefore not constitute a violation of this principle. It may, however, violate the data minimisation or storage retention principles.

Nearly all international instruments contain an adequacy requirement. However, the scope of this requirement varies.

While the GDPR, Convention 108+ and the AUC provide that any personal data processed must be accurate, the OECD Guidelines, the APEC Framework and the ASEAN Framework mandate that it must be accurate and complete.

While the GDPR and the AUC include an obligation to erase or rectify inaccurate data, no such obligation is included in the other instruments.

(2) After collection, the controller is only required to maintain the data's accuracy where this is either necessary for the processing, to the extent that this is reasonable, or where the data subject specifically requests the controller to keep the data up-to-date.

This may be the case, for example, in the case of credit reference agencies, where incomplete or inaccurate data may affect the data subject's credit rating.

All of the international instruments, save for the ASEAN Framework, include an ongoing obligation to keep the data up-to-date. However, this obligation only applies where, or to the extent, necessary.

Data Security

13(1) This principle ensures that personal data are processed in a way that ensures the security of the data.

The security risks resulting from any data processing are context-dependent and need to be assessed on an ongoing, case-by-case basis [, for example, as part of a Data Protection Impact Assessment under Clause 15]. Such risks include the risk of unauthorised and unlawful processing, loss or destruction of data, and other forms of misuse.

Appropriate safeguards may include, but are not limited to, the pseudonymisation and encryption of personal data, the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner where required, or a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure security.

All international instruments contain a specific principle on data security, using the language of 'appropriate' precautions (eg. AUC) or safeguards (APEC).

(2) Controllers, and where relevant, processors should put in place appropriate technical and organisational measures to mitigate such risks and should periodically review and assess their effectiveness.

In determining what measures are appropriate, controllers and, where relevant, processors must take account of all relevant factors. These include the current state of the art of data security measures, the nature, sensitivity and volume of the personal data processed, the purposes of the processing, and, the severity and likelihood of adverse consequences for individuals as a result of a security breach.

Risk is a dynamic concept and the controller and, where relevant, processor should review and assess the measures adopted regularly, in keeping with the data controller's accountability duty.

Many of the international instruments specify that the measures put in place should take account of risk, and identify types of risk.

(3) The contractual arrangements between the data controller and data processor relating to data protection and data security must be specified in a legally binding contract.

Such a contract should indicate the subject-matter and purposes of the processing, including the type of personal data processed and categories of data subjects and the duration of the processing.

This provision is intended to ensure that the controller appoints a data processor that is capable of implementing appropriate technical and organisational measures to ensure the controller's compliance with the data protection principles (including the data security principles) and the protection of data subjects.

The contract between the controller and the processor should, where feasible, be in writing to evidence the relationship between them with regard to the data processing, and to protect against the risk that the processor may exceed its competences.

The GDPR provides that processing by a processor must be governed by a binding contract between the controller and the processor that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

(4) The notification of data security breaches to regulatory authorities enables those authorities to exercise their powers under Part VII of these Model Provisions.

Personal data security breaches can have a reputational impact on organisations and lead to a loss of trust in them. The notification requirement is therefore intended to encourage data controllers to comply with the data security principle, to put in place appropriate data security measures, and to pay necessary attention to breaches that are reasonably likely to entail a risk to individuals.

Nevertheless, the over-reporting of personal data security breaches should be avoided as this could hinder the effectiveness of notification and place an unnecessary burden on the supervisory authority and other stakeholders.

Most significantly, personal data security breaches can affect the rights and freedoms of individuals. Data controllers must therefore notify breaches to the supervisory authority where it is reasonable to believe that such an impact is likely. In making this assessment, the controller should consider both the likelihood and the severity of the impact.

A personal data security breach is reasonably likely to affect adversely the rights and freedoms of individuals if the risk of the impact occurring is moderate or high.

The adverse effect a breach may have on a data subject's rights and freedoms should be interpreted broadly. Specifically, it can go beyond economic loss and include physical, emotional and other non-material damage. Examples of adverse effects include a loss of confidentiality of personal data, or where processing involves sensitive personal data or a large amount of personal data or affects a large number of data subjects.

The security breach notification to the supervisory authority must be timely and should avoid unnecessary delay. What constitutes undue delay must be determined on a case-by-case basis taking into account, in particular, the time at which the controller gained actual or constructive knowledge of the breach and the nature and gravity of the breach. When a controller becomes aware of a potential breach it should take prompt action to investigate whether a breach has occurred and what the impact of the breach might be.

The OECD Guidelines, the APEC Framework, Convention 108+ and the GDPR all contain explicit provisions on data breach notification. These provisions contain a proviso that the breach should be significant, and/or should affect individuals.

(5) Data security breaches likely to entail a serious interference with the rights and freedoms of data subjects include, for example, breaches that affect vulnerable categories of data subjects (such as children, or employees) or special category personal data.

Notifying the data subject directly may allow data subjects to take the necessary steps to protect themselves from further harm and to exercise their rights under these Model Provisions. However, the benefits of notification must be balanced against "notification fatigue" that might result from over-notification. Notification directly to data subjects should therefore be reserved for particularly serious breaches.

Where notification of the data subject is necessary, this should be done in a timely manner so the data subject can take effective measures to mitigate the risk to their rights.

The GDPR, the OECD Guidelines and the APEC Framework require a data controller to notify a data breach to an individual where it may lead to a high risk to their rights. This is subject to the proviso that it is reasonable and feasible in the APEC Framework.

(6) Supervisory authorities must collate data and report on such breaches in the interests of transparency.

An equivalent provision is not found in the text of international instruments.

Accountability

14(1) The scale of personal data processing has made it impossible, in practice, to subject all data processing activities to the prior authorisations of a competent supervisory authority.

The accountability principle ensures that controllers will use the discretion afforded to them by this law in a manner that is compatible with its spirit and letter. Accountability ensures that data controllers are responsible for data processing operations under their control, irrespective of the location of the data. The Model Provisions are designed to encourage data controllers to use the discretion afforded to them in a manner that is compatible with its spirit and letter.

In particular, data controllers must take all appropriate technical and organisational steps to achieve compliance and they must document or record these measures in order to provide evidence of their compliance measures, in particular to regulators.

Accountability is not an alternative to data subject rights and remedies, or to enforcement by supervisory authorities. It is an additional layer of responsibility that enhances the effectiveness of data subject rights and remedies and facilitates the oversight work of supervisory authorities.

The APEC and ASEAN Framework, the GDPR and the OECD Guidelines all contain references to data controller accountability. Convention 108+ does not explicitly refer to accountability but contains a similar obligation by obliging data controllers to take appropriate measures to ensure compliance and to demonstrate this compliance.

(2) Data practices policies [privacy management programmes] constitute a helpful mechanism to aid data controllers to evidence their accountability obligations. As such, such policies [programmes] must be implemented where provided for by national law or where the data processing entails a risk to the rights and interests of data subjects.

In assessing the necessity of such a policy [programme], and what level of detail it should contain, controllers should take account of the specific characteristics of the data processing operations under their responsibility.

Relevant factors include: the nature, scope, context and purposes of the data processing operation, whether the processing entails automated decision-making, and the level of risk the processing entails for natural persons.

In assessing risk, controllers should consider both the likelihood and the severity of the potential risk.

The APEC Privacy Framework, OECD Guidelines and the GDPR and mandate or encourage data controllers to establish a Privacy Management Programme [or Information Practice Policy].

The GDPR contains detail on the types of information that might be contained in the processing record while the APEC and OECD Framework provide more general guidance on such policies.

(3) In order to aid transparency and render accountability meaningful, the data practice policy [privacy management programme] should contain a readily understandable record of the data processing operations that could be made available to relevant stakeholders.

Such a record could include general details about the processing operations such as the name and address of the controller and the individual responsible for data protection compliance, a description of the personal data processed and an account of the purposes of data processing, a copy of relevant documents setting out the data controller's data protection policies, a description of the categories of recipient to whom personal data is made available, envisaged time limits for the erasure of personal data, and a general description of the technical and organisational security measures in place.

These requirements are (with the exception of Clause 14(3)(e)) present in the OECD Privacy Guidelines. The APEC Privacy Framework contains all but (a) and (e). The GDPR contains a similar requirement with limited exceptions.

(4) In order to be effective, data controller accountability must be demonstrable. The data controller must therefore be able to provide evidence of the measures it has put in place to ensure compliance with this Act, in particular by providing this evidence to supervisory authorities.

The GDPR, Convention 108+ and the OECD Guidelines all require demonstrable accountability (ie that compliance can be demonstrated and evidenced to the relevant supervisory authority). APEC considers that such documentation provides a sound basis to demonstrate compliance but does not mandate it.

[Data Protection Impact Assessment

15(1) A data protection impact assessment enables a data controller to conduct a detailed assessment of the likely impact of a data processing operation, or set of operations, on the rights and freedoms of natural persons.

An impact assessment might contain:

- A systematic description of the envisaged operations and the purposes of processing, including where relevant the legitimate interests pursued by the data controller;
- An assessment of the necessity and proportionality of the processing operations in light of their purpose;
- An assessment of the risks to the right and freedoms of data subjects;
- The measures envisaged to address the risks and to demonstrate compliance with these provisions.

When conducting an impact assessment the data controller may seeks the views of data subjects or their representatives on the intended processing.

The supervisory authority may enact guidelines to identify high risk data processing operations

In assessing whether an impact assessment is required, it is necessary to take into account factors such as the nature and volume of the data, the nature, scope and purpose of the processing and the size of the data controller. Where a number of processing operations entail a similar risk, a single assessment can be conducted.

Processing is deemed to be high risk processing where it involves large scale processing of special categories of data, including data relating to criminal convictions or offences or the systematic monitoring of a public accessible area. The use of automated decision-making to evaluate or reach inferences regarding an individual may also entail a high risk for the rights of data subjects.

Processing with an impact on societal values and rights, such as equal treatment and opportunity, freedom of expression or freedom of association, is also high risk processing. For instance, the systematic monitoring of public places through the deployment of facial recognition technology constitutes high risk processing.

Only the GDPR and Convention 108+ provide explicitly for impact assessments. However, both the OECD Guidelines and APEC Framework require privacy management programmes to provide for 'appropriate safeguards based on a privacy risk assessment'.

(2) An equivalent obligation is found in the GDPR.

(3) Data protection impact assessments promote the accountability obligations of the data controller and may be used to demonstrate compliance with the data protection framework.

Moreover, impact assessments also function as an early warning system for controllers, alerting them to potential data protection issues before implementing new processing operations.

Where data processing operations are likely to have an impact on the rights and freedoms of data subjects, the controller must adopt measures to negate such impact or, if not feasible, desist from the relevant processing operation.

The publication of the impact assessment, or a summary thereof, would enable the controller to demonstrate data protection compliance to the wider audience and reflect best practice in terms of accountability and transparency.

The GDPR provides that an impact assessment shall set out "the measures envisaged to address the risks to the rights and freedoms of data subject" (Article 35(7)).

(4) The supervisory authority shall be consulted regarding data processing operations that entail a high risk to individuals and groups. The supervisory authority should also be consulted where processing is undertaken for public interest purposes and entails such a risk. The supervisory authority may ensure that appropriate measures are put in place to address this risk before the data processing commences.

The GDPR provides for a similar prior consultation of the supervisory authority (Article 36).

(5) Impact assessments should be reviewed periodically and, in particular, where there is a change to the data processing operation or operations.

A similar obligation is implicit in the GDPR which provides that 'where there is a change in the risk entailed by processing, the controller shall carry out a review' (Article 35(11)).

[Data Protection Officer

16(1) The designation of an identified individual to act as a data protection officer on behalf of the data controller may assist the data controller to discharge its accountability obligations.

The data controller should ensure that the data protection officer has the necessary experience and knowledge to deal with requests and queries efficiently and the unnecessary duplication of compliance efforts will be avoided.

The GDPR recognises certain situations where a data protection officer must be appointed (for instance, when processing is carried out by a public authority or body, except courts acting in their judicial capacity). It also identifies circumstances where the designation of a data protection officer is optional.

(2) [Internally, the data protection officer must ensure that the data controller remains compliant with its data protection obligations by conducting periodic audits and impact assessments, where appropriate. The data protection officer should also promote data protection awareness and compliance through systematic involvement in relevant decision-making and initiatives such as training programmes.

Externally, the designation of a data protection officer as a single point of contact for data subjects and supervisory authorities may lower the transaction costs of compliance.

The data controller should ensure that the data protection officer has the necessary experience and knowledge to deal with requests and queries efficiently and the unnecessary duplication of compliance efforts will be avoided.

The GDPR sets out the tasks of the data protection officer.]

(3) In order to discharge these duties effectively, the data protection officer must be provided with sufficient resources to carry out his or her duties and must be free from all internal and external, direct and indirect, influence over its actions.

The GDPR provides a similar obligation (Article 38(3)).

(4) In order to minimise the resource implications of designating a data protection officer, a group of undertakings or public bodies may designate a single data protection officer. In considering whether the designation of a single officer is sufficient, the data controller should consider the size and structure of its organisation as well as the intensity of its data processing activities.

The GDPR contains a similar provision (Article 37(3)).

Data protection by design and default

17. Ensuring effective data protection is important for economic development and rights protection in a digital society. Protection of fundamental rights should not be an afterthought in data processing systems. Data protection principles and obligations must be embedded in data processing systems from the outset.

Data controllers must identify and assess the risk entailed by a new data processing operation and design the data processing in a way that guarantees respect for this Act. For instance, if a data controller is implementing a new system that processes special categories of data and retains these data in

an unencrypted format, this may violate the principle of data security. Where possible, the processing should be designed in a way that maximises data security by adopting security measures such as encryption.

Alternatively, data protection by design could be instrumental in securing respect for data minimisation. For instance, it could ensure that only personal data that is necessary for a specific purpose is processed and retained thereby processing less data over a shorter timeframe.

When designing and implementing data processing systems, data controllers must make a holistic assessment of how best to embed data protection principles. This includes an assessment of the risk entailed by the data processing operation (based on the nature, scope, context, purposes of processing and identified risks). In addition, the data controller must take into account the current state of the art and the cost of implementation of alternative options.

The APEC Framework provides that member economies should promote technical measures which help to protect privacy. Convention 108 requires data controllers to design data processing to minimise the risk of interference with rights and to implement appropriate technical and organisational measures, taking into account the impact of data processing on data protection. The GDPR contains an explicit data protection by design and by default principle in addition to similar data security obligations.

[Prior authorisation

18(1) The introduction of an accountability principle limits the need for the prior authorisation of data processing operations by supervisory authorities. This process of prior authorisation, if conducted at scale, is cumbersome and resource intensive.

Nevertheless, Member Countries may wish to include a prior authorisation requirement that applies where a data controller has conducted an impact assessment and identified that a particular processing operation entails a high risk for the rights and freedoms of data subjects, or where a supervisory authority has identified a category of data processing as posing such a risk, such operations should be notified to the supervisory authority prior to their implementation (see Clause 18(2)).

In these cases, the supervisory authority may then determine that the processing operation is unable to proceed on the basis of the risk it entails for individuals, or it may assist the data controller to identify appropriate measures which can be enacted in order to mitigate or eliminate the risk.

The AUC sets out preliminary formalities prior to data processing (declarations; authorisations and opinions). The other international instruments do not contain prior authorisation requirements.

(2) This clause grants the supervisory authority the power to make general determinations and issue guidance on processing activities that it deems to be subject to the prior authorisation requirement in Clause 18(1).

The AUC is the only international instrument to continue to provide for prior authorisation. While this was not explicitly risk-based (the provisions were drafted before the more widespread integration of risk-based approaches

in data protection laws), it is the supervisory authority that is tasked with establishing and publishing standards to simplify or introduce exemptions from prior authorisation.

Part V – Rights of Data Subjects

Right to subject access

19(1) The right to subject access is an essential right that allows data subjects to find out who processes their personal data and enables them to assess whether or not a controller complies with its obligations under data protection law. It is therefore a fundamental condition for the exercise of any other data subject right set out in Part V and is essential to enable data subjects to hold controllers accountable for their processing activities.

The right consists of [two] three separate elements, including a right to obtain confirmation from the controller as to whether or not personal data is processed, a right to have any personal data that is processed communicated to him or her[, and the right to receive additional information about the nature of the processing].

Nearly all international instruments include a right to data subject access although the scope of this right varies.

All instruments save for the ASEAN Framework grant the data subject a right to obtain confirmation of whether or not his or her data are being processed.

All instruments also include a right of the data subject to access any personal data related to them that is processed by the controller or to have a copy of those data communicated to them.

In addition, the GDPR, Convention 108+ and the AUC also impose an obligation on the controller to provide the data subject, on request, with additional information about the nature of the processing. The extent of this information varies between the three instruments with Convention 108+ imposing the least specific requirement (choosing instead to refer to the controller's general transparency obligation), the AUC requires the disclosure of information about at least the purpose of the processing, the categories of data concerned and the recipients or category of recipients to whom the data is disclosed. In contrast, the GDPR contains a detailed list of additional information that largely mirrors the information requirements with which controllers must comply in the context of the transparency principle.

(2) The right to data subject access is subject to certain procedural constraints. In particular, there are limits as to the length of the appropriate period for the controller's response to a data subject access request and the fee controllers may charge.

Controllers should consider making available a standard form to individuals to facilitate subject access requests. In particular, controllers, who obtain personal data electronically should allow data subjects to make requests in electronic form and should respond by electronic means.

The international instruments differ in their approach to procedural constraints with regard to the data subject access request.

Nearly all of the instruments provide that the controller must respond to the request within "a reasonable time" (OECD Guidelines, APEC and ASEAN Frameworks) or "without excessive delay" (Convention 108+).

The OECD Guidelines, Convention 108+ and the APEC Framework also stipulate that the information provided must be in a form that is readily intelligible or in a form that is reasonably understandable to the data subject.

The GDPR makes specific provision for requests made by electronic means, in which case the information must be provided in a commonly used electronic format.

Most instruments permit controllers to charge a fee for responding to the request, although this must generally be "not excessive" (Convention 108+, OECD Guidelines, and the APEC Framework) or "reasonable [...] based on administrative costs" (GDPR).

(3) The right to data subject access is restricted in cases where a response would involve a disproportionate effort on the part of the controller, where its disclosure would violate professional or statutory rules of confidentiality or secrecy or where the disclosure violates the rights and freedoms of other individuals.

Professional and statutory rules adopted by member countries may include rules relating to public or national security, law enforcement, trade secrets, legal privilege, legal proceedings and the enforcement of legal judgments.

The rights and freedoms of other individuals may be violated, for example, where the communication of the personal data to the data subject would also disclose personal information related to another data subject.

Given that a subject access request allows the data subject to access his or her own personal data or information about how that data is processed, subject access requests will rarely be considered vexatious or abusive. A request may be abusive or vexatious, if it puts undue stress on the controller in responding to it. This could be the case, for example, where a large number of repeated requests or requests for individual types of personal data are made rather than a broader, well-defined access request. There is likely to be significant overlap between the circumstances that are covered by Clause 19(3)(a) and (d).

Many international instruments contain exceptions from the subject access right.

The APEC Framework provides that no access need be provided where this would constitute an unreasonable burden or expense for the controller.

The APEC Framework also states that requests must not be disproportionate to the risks to the individual's privacy. Similarly, the GDPR provides that the data subject's right to obtain a copy of his or her personal data must not "adversely affect the rights and freedoms of others".

The APEC Framework, the ASEAN Framework and the GDPR also allow for national laws, particularly laws imposing an obligation of secrecy or confidentiality, to restrict the subject access right.

(4) Where the controller denies a request for data subject access on one of the grounds set out in Clause 19(3), it must inform the data subjects of the reasons for such a denial. In particular, the data subject should be told on which of the grounds the denial is based.

The controller must provide the data subject with a means to challenge its decision, which should ideally reflect the means by which the personal data is processed or by which the request was made.

Some international instruments specifically provide for a remedy for the data subject in case his or her request is denied. This includes, in particular, the OECD Guidelines and the APEC Framework.

(5) The obligation on the controller to provide the personal data and the additional information in an additional format, where appropriate, reflects the controller's general transparency obligation set out in Clause 83) that controllers must tailor the information to the intended audience.

While none of the international instruments include a specific requirement to make allowances for individuals with a sensory disability, in some cases this is implied by the general transparency obligation to provide information in an easily accessible form (GDPR, OECD Guidelines, APEC and ASEAN Frameworks).

Right to rectification and erasure

20(1) Data accuracy is a core principle of data protection law. The processing of inaccurate data has the potential to disadvantage the data subject and is of little utility to the data controller. Those data should therefore be amended, completed or erased.

All international instruments include a right of the data subject to request correction and/or deletion of incorrect or out-of-date information. The scope of these rights varies across instruments. In some (GDPR, AUC and Convention 108+) it is strongly linked to the accuracy principle.

(2) Where personal data are processed in a manner that contravenes this law, for instance where the data subject has withdrawn his or her consent or the processing is no longer necessary for the purposes for which the data were initially processed, the data subject has the right to have those personal data deleted.

If personal data are inaccurate because they are incomplete, the data controller may rectify this inaccuracy by adding a supplementary statement to the personal data.

All international instruments contain a right to erasure, albeit in different forms.

The OECD Guidelines provide for such a right following a 'successful' challenge by a data subject to the data relating to them.

The AUC provides for erasure where the data is inaccurate, incomplete, equivocal or out date or where its processing [collection, use, storage or disclosure] is prohibited.

The APEC Framework provides for a qualified right (if appropriate and possible). Similarly, ASEAN allows for erasure in case of error or omission.

Convention 108+ and GDPR allow for erasure where processing is contrary to their provisions.

(3) [If reasonably practicable, the right to rectification and erasure can include an obligation on the data controller to inform other third parties to whom the personal data has been disclosed of the data subject's request. This obligation applies when the data processing is likely to have an impact on the data subject,

for instance if the changed information has been or will be used to inform decision-making in respect of the data subject. These third parties are then required to assess the compatibility of their continued processing of those personal data with the law.]

Only the GDPR contains a 'right to be forgotten'. The South African Protection of Personal Information Act 2013 contains a comparable obligation.

(4) The right to rectification and erasure offers practical support to the principle of data accuracy. Data controllers should facilitate data subjects' exercise of this right by addressing such requests without undue delay, and ensuring that such requests can be made without the data subject incurring any cost.

In order to address a request to rectify or erase data effectively, the data controller may require some specific information from the data subject. For instance, the data subject will need to specify the contested information and to provide some explanation indicating why it is inaccurate or requires completion, or if deletion is sought, why its processing is incompatible with this law.

The APEC Framework sets out a number of limits to the exercise of the right, including where it would constitute an unreasonable expense or burden for the data controller.

(5) If the data controller does not deem the request for amendment, completion or erasure to be justified, then it must communicate it refusal and its reasons for that refusal to the data subject. This communication should take the same form as that in which the initial request was made.

Such a provision is not provided for in the international instruments.

(6) The right to rectification and to erasure is not absolute. This right does not apply where the maintenance of the data in its original form is indispensable for archiving purposes, or is required by law. The right also does not apply, or applies only to the extent necessary, when its exercise interferes with the rights and freedoms of others, including the right to exercise or defend legal claims and the freedom of expression and information.

The international instruments all allow for exceptions or limitations to the right to rectification and/or erasure. The APEC Framework allows for an exception where compliance would place an unreasonable burden or expense for the data controller; or would be disproportionate to the risks to the individual's privacy. The GDPR provides that the right to erasure does not apply to the extent necessary to achieve a set of specified aims (including the exercise of freedom of expression and information and the establishment, exercise and defence of legal claims).

[Right to object

21(1) [This provision recognises that, even if the data controller is lawfully processing their personal data, the individual circumstances of a data subject may justify ending a processing operation at the data subject's request.

While a data subject can withdraw their consent to personal data processing, thereby objecting to such processing, this right enables data subjects to object when the controller relies on a lawful basis other than consent. Taking account of the individual circumstances of the data subject this may be particularly

important where the processing relies on Clause 6(3)(d) or (f) (and is justified based on a public interest or the legitimate interests of the controller or a third party).

Wholly or partly automated decision-making may, among other things, fail to take account of the individual circumstances of a data subject. The right to object enables the data subject to bring this failure to the attention of the data controller and to cease data processing as a result.

When personal data are disclosed to third parties, the original context in which personal data were processed may change materially. This change may impact data subjects in distinct ways. The right to object allows particularly affected individuals to bring this to the attention of the data controller and to cease data processing as a result.

The GDPR, Convention 108+ and the AUC contain a right to object to personal data processing in certain circumstances. The GDPR right applies in three circumstances whereas both Convention 108+ and the AUC contain a broader right to object on grounds that are specific to the data subject. The AUC also provides that an individual can object to disclosures of data to third parties.

No such right is present in the OECD Guidelines, the APEC Framework and the ASEAN Framework.]

(2) The right to object is not absolute. The data controller may discharge the burden of proof to demonstrate that legitimate grounds exist to justify the continued processing of personal data of the data subject, despite their objections.

This provision entails a balancing of the rights of the data subject with the interests of the data controller.

Compelling legitimate grounds must override the interests, rights and freedoms of the data subject and might include the establishment, exercise or defence of legal claims or reasons of public safety.

Compelling legitimate grounds must be examined on a case-by-case basis.

The right contained in the GDPR, AUC and Convention 108+ is similarly subject to exceptions and caveats.

(3) [The data subject has an unconditional right to object to the processing of their personal data for direct marketing purposes. They do not need to invoke their particular situation in making this claim, nor does the controller have the possibility of invoking compelling legitimate grounds to justify its continued processing.

The data subject's right to object to direct marketing includes profiling to the extent that it is related to such marketing.

The GDPR contains a right to object to direct marketing.

Part VI – Exceptions

22(1) National laws may be used to restrict a controller's obligation to comply with the data protection principles and/or the rights of the data subject where this is [necessary and proportionate][reasonable and proportionate] for specific public interest purposes. Any restriction must be prescribed in the relevant Member Country's national law.

As a general rule, Member Countries will be able to use the standard applied as part of their own constitutional law and fundamental rights framework. However, legislative measures that include such restrictions must respect the essence of the data subject's fundamental rights and freedoms.

Member Country should be aware that the application of a standard that falls below that of "necessity" may result in other Member Countries prohibiting data exports to their territory under Clause 23(1)(a).

Several of the international instruments permit signatories or member countries to introduce exceptions to the controller's obligation and the rights of the data subject's for limited public interest purposes.

There is a clear distinction between those instruments that are principles-based and of an advisory nature (OECD Guidelines, APEC Frameworks) and those that impose binding legal rules (GDPR and Convention 108+).

While the former generally encourage member countries to limit exceptions to the minimum (OECD Guidelines and APEC Framework) and to ensure that any restrictions are a proportionate measure to meet their objectives, they do not impose any particular substantive or procedural restrictions on member countries.

In contrast, rule-based instruments largely include detailed provisions about the public interest objectives that may be used to justify exceptions, the need for those exceptions to be provided for by law and the need of any legislative measure to respect the essence of the fundamental rights of the data subject and others.

(2) Legislative measures that restrict the controller's obligations to comply with the data protection principles or data subject's rights must comply with certain procedural requirements to ensure that the restrictions are limited to specific instances.

In addition to the substantive requirements that member countries must comply with when adopting exceptions, the GDPR also includes procedural safeguards in the form of a specific list of provisions that any legislative measure must include.

(3) Data subjects affected by a restriction must be provided with appropriate information about the scope of the restriction as it applies to them. This is not necessary where providing this information would prejudice the purpose of the restriction. For example, a legislative measure might restrict the controller's obligation to provide the data subject with clear and easily accessible information about the processing in a situation where data is shared with law enforcement agencies for the purpose of the detection and prosecution of a criminal offence committed by the data subject. In this case, disclosing informing the data subject about such data sharing might impede the investigation.

Several international instruments provide that data subjects must be informed about any restrictions (GDPR) or that those restrictions must be made public (OECD Guidelines, APEC Framework).

Part VII – Cross-border data transfers

23(1) When personal data are transferred to third countries or international organisations with different data protection standards, controllers [and processors] must ensure that the rights of data subjects are adequately protected with regard to any processing that takes place after the transfer.

[Controllers [and processors] must assess, prior to the transfer, if a third country or international organisation ensures an [adequate][equivalent][appropriate] level of protection.][The decision on whether a third country or international organisation ensures an [adequate][equivalent][appropriate] level of protection is taken by [the supervisory authority] [the government authority charged with issuing such decisions] on the basis of a procedure set down in national law.]

When carrying out that assessment, [the controller and [processor]][the supervisory authority] [the government authority charged with issuing such decisions] should take into account the national laws and international obligations applicable in the relevant third country or international organisation. Among other things, this may include the third country's or international organisation's respect for human rights and fundamental freedoms, its data protection rules, professional rules and other relevant legislation and their implementation and enforcement; rules governing the onward transfer of personal data to another third country or international organisation; the extent to which, and the basis on which, public authorities may be able to access the personal data transferred for the purpose of public security, defence, national security and law enforcement; case-law; as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred.

International instruments can broadly be distinguished between those that operate a relatively flexible approach to cross-border data flows (OECD Guidelines, APEC Framework and ASEAN Framework) and those that operate a strict rule-based approach (GDPR, Convention 108+ and the AUC). The latter generally prohibit transfers of personal data to third countries unless those countries provide an "adequate" or "appropriate" level of protection" for incoming data or unless a range of other conditions are met.

Those conditions include other "appropriate safeguards" as well as other derogations from the transfer prohibition that may apply to individual transfers.

Under the GDPR, the decision on determining a country's or international organisation's "adequacy" is left to the European Commission. The AUC and Convention 108+ leave it open to signatory states to determine, who should have the power (and the duty) to make that decision.

However, the AUC also grants power to the national data protection authority to authorise individual transfers.

(2) Transfers to third countries or international organisations that do not ensure an [adequate][equivalent][appropriate] level of protection may still be lawful, if the controller or processor can provide evidence that he has put in place appropriate safeguards to ensure the protection of the transferred data after the transfer.

The safeguards that may be appropriate depend on the nature of the transfer and the identity of the [controller or processor].

Public authorities in the relevant countries are encouraged to enter into legally binding and enforceable instruments that govern specific types of (usually recurrent) transfers, which must provide a framework that ensures compliance with the data protection principles and grants enforceable rights to data subjects.

Commercial data controllers may be able to rely on standard contractual clauses adopted and published by the supervisory authority that they can incorporate into their agreements with the recipients of data transfers in third countries or on contractual clauses individually negotiated between them and the recipient of the personal data. Optionally, such contractually clauses may be subject to authorisation by the competent data protection authority.

Binding corporate rules are most suitable for data transfers between companies of the same group of companies.

The concept of appropriate safeguards as a means to authorise cross-border data transfers is most clearly embraced by the GDPR and Convention 108+.

While the GDPR includes a detailed list of safeguards that controllers and processors may rely on (including BCRs, standard contractual clauses, codes of conduct and certification mechanisms), Convention 108+ refers to more general " ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments" adopted and implemented by the parties involved in the transfer.

(3) Where the third country does not provide an [adequate][equivalent] [appropriate] level of protection and where controllers are unable to rely on appropriate safeguards, transfers may still be possible where certain derogations apply.

Transfers may be authorised by data subjects giving their explicit consent. However, this is subject to them having been provided with information about the risks involved in such a transfer, particularly to countries or international organisations that do not ensure an [adequate][equivalent][appropriate] level of protection.

Closely linked to the data subject's consent are transfers that are either necessary for the performance of a contract that the data subject him or herself has entered into, or transfer that are in the data subject's vital interest but where consent cannot be obtained.

Finally, transfers may be permitted where they are necessary for important reasons of public interest. This could include, among other things the list of interests set out in Clause (22(1)(b)].

Only the GDPR and Convention 108+ include additional derogations from the transfer prohibition. However, they differ in the scope of those derogations. While both permit transfers that are authorised by the data subject's explicit consent, or where they are necessary for the "vital"(GDPR) or "specific" (Convention 108+) interests of the data subject, or the public interest, each instrument also includes a range of derogations that are not reflected in the other instrument.

Convention 108+ allows transfers where this constitutes a "necessary and proportionate measure in a democratic society for freedom of expression", while the GDPR includes derogations "for the establishment, exercise or defence of legal claims", or where the transfer is made from a public register under certain circumstances.

Part VIII – Independent supervisory authority

Establishment

24(1) While data controllers are bound by the accountability principle when processing [personal data, independent oversight of data protection compliance is a key component of effective data protection. This function should be carried out by a public body specifically appointed for that purpose.

The GDPR, the AUC and Convention 108+ require the establishment of a supervisory authority. The OECD Guidelines encourage Members to maintain privacy enforcement authorities.

(2) Provided that the process used for the appointment is fair and transparent, Member Countries are free to choose whether members of the supervisory authority , are appointed by parliament, government, the Head of State or by an independent body entrusted with this task.

The rules governing the appointment procedure should specify, at least, the term of office of the Commissioner; relevant qualifications and experience required for appointment of the Commissioner and other members of the supervisory authority, other eligibility conditions for appointment, and the procedure for any appointment.

A similar obligation for 'transparent' appointment is found in the GDPR.

(3) No similar provision is found in international instruments however the APEC Framework does allow for 'flexible' implementation, accommodating various models including multi-agency enforcement bodies or a network of designated industry bodies.

Independence

25(1) The independence of the supervisory authority enables it to perform its tasks efficiently and without undue influence from public and private bodies, thus ensuring the appropriate use of resources and the effective and reliable protection of individuals' rights and freedoms.

The GDPR details the conditions required for the independence of a supervisory authority. The AUC also specifies that membership of the supervisory authority is incompatible with membership of Government, carrying out the functions of a business executive or owning shares in ICT businesses.

(2) The mandate of the Commissioner must be of a sufficient duration to guarantee their independence. In practice, this generally means a period of five years or more.

The GDPR provides that the supervisory authority should not be subject to financial control which affects its independence. Should have separate, public annual budgets which are part of the overall state or national budget.

(3) The supervisory authority must be provided with sufficient resources to enable it to conduct its business without dependence on public or private funding that might influence its actions.

Adequate resources include human, technical and financial resources as well as the physical infrastructure need to enable the Authority to exercise its powers under Clauses 26 to 30.

The GDPR provides that supervisory authorities must be provided with the 'human, technical and financial resources, premises and infrastructure necessary for the effective performance of their tasks and the exercise of their powers. Should not be subject to financial control which affects its independence. Should have separate, public annual budgets which are part of the overall state or national budget.

(4) During their term of office, the Commissioner shall conduct themselves in an independent manner. For instance, it might not be permissible for the Commissioner to be employed in another capacity while in office. This would be the case, for instance, if the Commissioner was a member of government or acted as a business executive or shareholder in a private company. These guarantees might be extended to a period of time following office. The former Model Bills deemed the Commissioner ineligible for appointment to the public service after their term in office.

A Commissioner or a member of the authority should only be removed from office during their term in extreme circumstances. For instance, a removal from office or dismissal would be appropriate in the case of gross misconduct or misbehaviour or alternatively if the Commissioner or other member was no longer able to discharge the functions of his or her office.

The GDPR provides that dismissal of a member of the supervisory authority should be only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of their duties.

(5) The Commissioner shall be appointed for a minimum term of office to preserve their integrity. The conditions for renewal, where applicable, shall be provided for by law.

Powers – General

26(1) Supervisory authorities must be endowed with a broad range of powers of an advisory, investigative and corrective nature in order to ensure the effectiveness of the Act.

The GDPR, the AUC and Convention 108+ identify specific functions and powers of supervisory authorities.

(2) [Where resources act as a constraint on the actions of the supervisory authority, a risk-based approach to their usage may be appropriate to prioritise resources].

The APEC Framework sets out a similar provision.

Advisory Powers

27. Supervisory authorities are responsible for ensuring the effective application of this law. The advisory role of supervisory authorities, primarily giving advice and guidance, is critical in achieving this aim.

The advisory powers of the supervisory authority require it to engage constructively with relevant stakeholders, including law and policy-makers, controllers, processors, data subjects and the general public.

By raising public awareness of data protection law, data subjects will be encouraged to exercise their rights and to contribute to a higher level of data protection.

The AUC and GDPR provide that supervisory authorities should have such advisory powers. The term 'advisory powers' is not used however tasks such as 'advising persons/bodies engaged or likely to engage in personal data processing' are indicated (AUC).

Investigative Powers

28. In order to fulfil their enforcement responsibilities, the supervisory authority is endowed with a range of investigative powers that help it to establish whether and to what extent a controller complies with its data protection obligations and that support, among other things, the exercise of the authority's corrective powers and advisory (see Clauses 27 and 29).

    These investigative powers include powers of audit, inspection, information retrieval and cooperation, among others.

    Supervisory authorities may also use those powers, in the first instance, to provide advice and support to controllers with regard to ensuring their compliance with the Act.

    None of the international instruments categorise the powers of supervisory authorities as 'advisory, investigative and corrective'. However, Convention 108+, the AUC and GDPR all provide for investigative powers. For instance, Convention 108+ provides for 'powers of investigation and intervention'.

Corrective Powers

29(1) To ensure the effective application of the data protection framework the supervisory authority must be able to exercise a range of corrective powers where it finds that a controller or processor has failed to comply with the Act. Such corrective powers may be applied to all data controllers.

    While administrative fines have proven to be an effective corrective instrument to ensure compliance with data protection law, it is nevertheless acknowledged that their imposition on public sector data controllers may have direct implications for public sector finances. Member Countries may therefore decide to limit the supervisory authority's power to impose administrative fines to data controllers in the private sector. Similar considerations may apply with regard to controllers from the third sector.

    Fines imposed pursuant to this clause shall not be administered in such a way as to undermine the independence of the supervisory authority.

    The AUC, the GDPR and Convention 108+ all provide for some form of corrective powers.

(2) The exercise of corrective powers may entail preparatory work by the supervisory authority (such as gathering information on turnover to calculate administrative fines or instructing legal representatives). All such functions necessary to discharge the powers in Clause 29(1) fall within the remit of the supervisory authority.

An equivalent provision is not explicitly stated in the international instruments.

(3) In discharging its powers, supervisory authorities will process private information as well as business secrets.

Even where members of the supervisory authority are not subject to a duty of professional secrecy, they are required not to disclose information of the kind covered by professional secrecy.

This includes confidential information relating to individuals in order to respect their fundamental rights and the business secrets of enterprises in order to protect their commercial interests.

This obligation on supervisory authorities should be performed in a proportionate manner, so as not to unduly hamper the transparency of the supervisory authority's activities.

The AUC and GDPR contain a similar provision.

International cooperation and mutual assistance

30(1) The intangible nature of personal data means that its processing raises common challenges across national boundaries and inevitably gives rise to enforcement activities in multiple jurisdictions.

Co-operation and mutual assistance between supervisory authorities serves dual aims. Co-operation minimises the risk of duplication of efforts thereby reducing costs for authorities and other stakeholders. It also renders the application of data protection law more effective by facilitating regulatory alignment.

In order to facilitate this co-operation, in legal orders where multiple supervisory authorities exercise data protection competences (such as federal systems), the supervisory authority should identify a competent domestic authority to co-ordinate cooperation and communicate this to partner authorities nationally and internationally.

Convention 108+ and the APEC Framework provide for cooperation and mutual assistance between supervisory authorities and the identification of a competent authority for these purposes.

(2) Information exchange and capacity building are commonly acknowledged to promote these aims and encouraged by international data protection instruments. Such activities are therefore strongly encouraged, where relevant. Of particular significance is the joint development of internationally comparable metrics for policy-making.

Any information shared with other national and international authorities should only include personal data where indispensable for cooperation or where the data subject's consent has been obtained.

Convention 108+, the APEC and ASEAN Frameworks and the OECD Guidelines contain specific provisions detailing information-exchange and support for policy-making between supervisory authorities.

(3) As a result of globalisation and an increased reliance on digital communications infrastructures, like the Internet, personal data processing is now rarely confined within national borders. Effective data protection enforcement may therefore require cross-border co-operation between supervisory authorities when personal data processing occurs or has effects across multiple jurisdictions.

Personal data processing activities also cut across fields of economic and social activity. This has implications for regulators in fields like competition law, election regulation and consumer protection law. Co-operation with those regulators in order to ensure coherent and consistent regulatory outcomes is also desirable.

The establishment of networks of regulators or co-ordination within existing networks (such as GPEN, the Global Privacy Enforcement Network) is desirable.

Furthermore, the identification of legal mechanisms to resolve disputes regarding competences or cross-border processing activity will facilitate such co-operation and the effective enforcement of data protection law. An example of such a mechanism is the GPEN 'Global Cross Border Enforcement Cooperation Arrangement'.

Convention 108+ and the APEC Framework refer to the possibility of coordinating investigations and enforcement activity across borders.

Part IX – Sanctions and remedies

Sanctions

31(1) Effective data protection is contingent upon ensuring that relevant stakeholders respect the law. A critical piece of this picture is the availability of appropriate remedies for individuals and the power of supervisory and judicial authorities to impose appropriate sanctions on controllers and, where relevant, processors.

The GDPR provides for strict and prescriptive sanctions. The OECD Guidelines encourages countries to provide for 'adequate sanctions' and Convention 108+ and the APEC Framework afford similar discretion in this regard.

(2) This Clause recognises that Member Countries implementing national data protection laws come from distinct legal and regulatory traditions. It therefore aims to recognise Member Countries' procedural autonomy and respect their legal culture by leaving some discretion as to the precise sanctions or remedies to be brought to bear on data controllers or data processors in the event of non-compliance.

This discretion should nevertheless be exercised in a way that ensures that sanctions are effective, dissuasive and proportionate. In assessing the proportionality of a sanction, a risk-based approach may be adopted. This should take into account the potential likelihood and severity of harm caused as a result of the non-compliance.

This formula is used in the GDPR. The APEC Framework provides that remedial measures should be 'proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information'.

The OECD Guidelines provides for 'adequate' sanctions', Convention 108+ provides for 'appropriate judicial and non-judicial sanctions and remedies'.

(3) Investigations conducted by the supervisory authority may culminate in sanctions, including significant administrative fines. Those investigations must therefore comply with the right to an effective remedy and ensure that those investigated are offered appropriate procedural safeguards, in light of the severity of the alleged infringement and the potential sanction to be imposed.

Safeguards may include, for instance, the right to a hearing before the supervisory authority or the right to make full submissions in relation to the alleged infringement.

The international instruments do not contain a similar provision.

(4) Sanctions and remedies should be imposed in a manner which respects procedural safeguards, including transparency. Legislation or an administrative document might therefore provide guidance on the factors that influence the supervisory authority's decision on which sanction to impose and how the extent of that sanction is calculated. For instance, when deciding upon a sanction, the supervisory authority might take into account the nature, gravity and duration of the infringement, whether it was intentional or negligent; and steps taken by the data controller [or processor] to mitigate the damage suffered by individuals.

The GDPR contains a similar provision.

The right to complain to a supervisory authority

32(1) Supervisory authorities are tasked with overseeing and ensuring the effective enforcement of the data protection rules. Individual data subjects must therefore have the right to complain to the supervisory authority [or an ombudsperson] and to receive a response to their complaint. Data subjects also have the right to appoint a third-party representative (for instance, a family member or a lawyer) to exercise this right on their behalf.

The supervisory authority may facilitate the submission of complaints, by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

The supervisory authority will receive complaints and exercise its functions free of charge with some limited exceptions in the case of manifestly unfounded or excessive requests.

This right is set out in Convention 108+, the GDPR and the AUC.

(2) The supervisory authority must carry out an initial assessment of any complaint it receives to determine whether it merits further investigation.

When making this assessment, the supervisory authority may take account of a range of factors, including whether the complaint could reasonably be considered to be abusive or vexatious, and whether the investigation of the complaint will contribute to the effective protection of data subjects.

Supervisory authorities may, as best practice, introduce publicly available guidelines to identify how complaints are assessed and, where relevant, prioritised.

The GDPR contains a similar provision.

(3) Data subjects may not be aware of the illegality of a data processing operation, or may not have the resources (time, financial, or educational) or desire to pursue a complaint before a supervisory authority. In those circumstances, an interested third party may complain to a supervisory authority about a potential contravention without the mandate of the data subject. This right is limited to situations where the potential illegality is of broader public interest. Member Countries may impose some restrictions on the nature of the third party pursuing such a complaint (for instance, they may stipulate that the third party operate on a non-profit basis, or have expertise in the areas of data protection or privacy law).

Such a right is contained in the GDPR.

(4) The right to lodge a complaint with a supervisory authority shall be without prejudice to other remedies that the data subject or their representative(s) may wish to pursue.

The GDPR contains a statement with similar effect.

Right to a judicial remedy including a right to appeal the decision of the supervisory authority

33(1) Supervisory authorities are administrative authorities, not tribunals. Their decisions must therefore be subject to full review by a court in order to guarantee the right to an effective remedy to the addressees of their decisions.

Data subjects and other parties affected by a legally binding decision of a supervisory authority can seek to have this decision judicially reviewed.

[Affected parties might include controllers, processors or third parties impacted by the decision (for example, if a business model is deemed illegal by a supervisory authority, third parties using this business model may wish to challenge this decision before a court].

Furthermore, where a supervisory authority fails to handle the complaint in a satisfactory manner the data subject or legal person may appeal to a Court. For instance, if the supervisory authority decides that no investigation of the complaint is required, or fails to provide the complainant with an indication of the complaint's status within a reasonable timeframe, a complaint may be lodged before a Court.

Convention 108+ requires that appropriate judicial and non-judicial remedies are in place, without further elaboration. The GDPR contains a similar provision. The AUC also allows for appeals against sanctions imposed and decisions taken by the supervisory authority.

(2) Where the data subject considers that the supervisory authority has failed to take appropriate action in relation to a complaint, this failure to act can be challenged before a judicial authority.

The GDPR provides for a similar right.

(3) National law shall provide for appropriate private causes of action to ensure that the data subject can seek a judicial remedy against a controller [or, where relevant, a processor]. Such actions might include, for instance, actions for compensation (as outlined in Clause 34), actions in contract or actions in tort or delict.

The GDPR contains a similar provision.

(4) The judicial remedies set out in Clause 33(1)-(3) do not preclude the data subject or any other affected party from seeking an administrative remedy from the supervisory authority.

The GDPR contains a provision with similar effect.

Right to seek compensation

34(1) Individuals who have suffered damage as a result of unlawful data processing have a right to obtain compensation. Damage may be of a material or a non-material kind. Material damage may include financial loss or theft suffered as a result of the illegal processing. Non-material damages are particularly important in this context and may include distress or damage to reputation.

The GDPR provides for a similar right.

(2) Responsibility for damage suffered as a result of illegality should be apportioned by a Court and compensation should be calculated on the basis of this apportionment. A data processor should only be directly responsible for damage to the data subject, where it has not complied with those provisions of the Act directed explicitly towards it, or where it has acted outside or contrary to the lawful instructions of the data controller. In all other cases, the obligation to pay damages will fall on the data controller, notwithstanding that the controller may itself have a right to compensation against the processor in accordance with the contract between them.

The GDPR contains a similar provision.

(3) In order to enhance the effectiveness of data subject rights and to promote compliance with the data protection framework, data subjects may mandate a third-party organisation to claim compensation on their behalf. Member Countries may introduce conditions to deter speculative claims for compensations, for instance by specifying that only non-profit organisations can exercise this right on behalf of data subjects.

The GDPR contains a similar provision.

The Commonwealth

D19113