MINISTRY OF DIGITAL

PERSONAL DATA PROTECTION
GUIDELINE

DATA PROTECTION BY DESIGN (DPbD)

Version 1.0
Date of Issuance: 30 April 2026

DEPARTMENT OF PERSONAL DATA PROTECTION

Address:

DEPARTMENT OF PERSONAL DATA PROTECTION
Level 8, Galeria PjH, Jalan P4W, Persiaran Perdana
Precinct 4, Federal Government Administration Centre
62100 Putrajaya, Malaysia

TABLE OF CONTENTS

PART A: INTRODUCTION

1. Background

1.1 This Data Protection by Design Guideline ("**Guideline**") sets out guidance on applying the Data Protection by Design ("DPbD") approach to the data controller and data processor to ensure compliance with the Personal Data Protection Principles under the Personal Data Protection Act 2010 ("**Act 709**").

1.2 Section 5 of the Act 709 provides that the processing of personal data by a data controller shall comply with the Personal Data Protection Principles, which are:

1.2.1 General Principle;
1.2.2 Notice and Choice Principle;
1.2.3 Disclosure Principle;
1.2.4 Security Principle;
1.2.5 Retention Principle;
1.2.6 Data Integrity Principle; and
1.2.7 Access Principle

(collectively, "**PDP Principles**").

Where the processing of personal data is carried out by a data processor on behalf of the data controller, the data processor shall comply with the Security Principle.

1.3 The adoption of a DPbD approach is essential for the data controller and data processor to shift from a reactive to a proactive mindset towards personal data protection. It helps to ensure effective compliance with Act 709, strengthens protection of the data subject's rights and ensures that Malaysia's personal data protection framework is relevant, effective and aligned with the global data protection regulatory landscape.

1.4 This Guideline sets out guiding elements, applications, illustrations and best practices as a reference for the data controller and the data processor on how to apply the DPbD approach. It is not intended to be mandatory or prescriptive. The data controller and data processor are encouraged to apply a risk-based approach and tailor the DPbD efforts based on the nature, size, scope, purposes and context of the data processing activities.

1.5 This Guideline is linked to the Personal Data Protection Standard, Data Breach Notification Guideline, Cross-Border Personal Data Transfer Guideline and the Codes of Practice issued by or registered with the Personal Data Protection Commissioner ("**Commissioner**"). For example, actions to be taken in the event of a personal data breach are closely related to the guidance set out under the Data Breach Notification Guideline.

1.6 This Guideline supplements and is to be read together with the Act 709 and any other relevant legislative instrument(s) issued under the Act 709, as may be amended from time to time. This Guideline shall not be considered to override any other personal data protection-related laws and regulations in force.

2. Legal provisions

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

3. Interpretation

3.1 For the purposes of this Guideline, DPbD is defined as follows:

> "Data protection by design" means an approach that incorporates appropriate technical and organisational measures, which are designed to implement the PDP Principles, into the entire lifecycle of a data processing activity, from design, development and deployment to decommissioning.

3.2 DPbD requires the incorporation of personal data protection measures into the design and development of projects, systems, programmes, processes and technologies from the outset. Privacy considerations shall be taken into account at all stages of a data processing operation, by default, from the beginning to the end. The data controller and the data processor shall adopt a proactive stance to personal data protection that focuses on anticipating and preventing privacy breaches, rather than merely reacting after data protection issues have occurred.

Example of DPbD in practice:

An organisation's marketing team maintains a database of customers' email addresses processed for different purposes, such as sending marketing newsletters, processing product orders and managing loyalty programmes.

To comply with the Retention Principle under Act 709, the team creates a database query to identify the collection dates of the email addresses and applies a standard timeframe to determine when the addresses may no longer be needed. Email addresses reaching the set expiry are flagged for manual review to decide on deletion.

This approach creates gaps in data protection. Over time, the team struggles to track the date and purpose of each collection, resulting in email addresses being retained for longer than necessary.

By applying a DPbD approach, the marketing team designs the database so that each email address is automatically assigned an appropriate retention period upon entry. Once the retention period ends, the email address is automatically deleted, or at a minimum, automatically blocked from further use until it is reviewed.

PART B: DPbD ELEMENTS

4. Elements of DPbD

4.1 This Guideline outlines four (4) DPbD elements, which are as follows:

Element 1: Proactiveness;
Element 2: End-to-end protection;
Element 3: Transparency; and
Element 4: User-centricity.

4.2 **Proactiveness** is an approach that emphasises anticipating and preventing privacy risks before they occur, as well as actively developing processes to prevent personal data breaches, rather than merely taking reactive measures when such risks arise. This approach involves:

4.2.1 establishing governance arrangements and allocating adequate resources to support personal data risk management within the organisation; and

4.2.2 designing the personal data processing systems that minimise the collection, use and retention of personal data to the minimum extent necessary, and protecting personal data by default.

4.3 **End-to-end protection** refers to ensuring data protection throughout the entire lifecycle of the personal data involved. Every phase, namely collection, processing, storage and disposal shall comply with the PDP Principles.

4.4 **Transparency** refers to demonstrating accountability in personal data processing activities. The data controller and data processor shall be open and honest about how the personal data is handled and be prepared to demonstrate compliance with the stated practices.

4.5 **User-centricity** refers to recognising that personal data ultimately belongs to the data subject and giving the data subject control over his personal data. Projects, products, services, systems and processes shall be consciously designed around the interests and needs of the data subject, who has the greatest vested interest in the management of his own personal data.

PART C: DPbD FOR GENERAL PRINCIPLE

5. General Principle

Section 6 of Act 709 outlines the General Principle:

"

(1) A data controller shall not-

(a) in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his consent to the processing of the personal data; or

(b) in the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with the provisions of section 40.

(2) Notwithstanding paragraph (1)(a), a data controller may process personal data about a data subject if the processing is necessary-

(a) for the performance of a contract to which the data subject is a party;

(b) for the taking of steps at the request of the data subject with a view to entering into a contract;

(c) for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;

(d) in order to protect the vital interests of the data subject;

(e) for the administration of justice; or

(f) for the exercise of any functions conferred on any person by or under any law.

(3) Personal data shall not be processed unless-

(a) the personal data is processed for a lawful purpose directly related to an activity of the data controller;

(b) the processing of the personal data is necessary for or directly related to that purpose; and

(c) the personal data is adequate but not excessive in relation to that purpose."

5.1 The General Principle under the Act 709 requires that the data controller:

(a) has a valid legal basis (e.g. consent, performance of a contract, etc.) for the processing of personal data;

(b) only process personal data for a lawful purpose directly related to the data controller's activity and where necessary for or directly related to the purpose; and

(c) only process personal data that is adequate but not excessive in relation to the purpose.

5.2 A DPbD approach in compliance with the General Principle requires the data controller to embed privacy considerations into the design of the data processing operation to ensure, from the outset that the data processing operation is valid, purpose-specific and guided by necessity, with measures that ensure end-to-end adherence to the relevant legal bases and purposes of processing by default.

5.3 A DPbD approach in compliance with the General Principle further requires the data controller to embed privacy considerations into the personal data of the data subject aged under eighteen (18) years, including ensuring that valid consent is obtained on behalf of the data subject. Such consent shall be obtained from the parent, guardian or person who has parental responsibility for that data subject.

5.4 The following concepts and applications are intended to guide the implementation of DPbD in complying with the General Principle. They are not prescriptive or exhaustive and shall be adapted by the data controller based on the specific risk profile[1] and the personal data processing operations.

(a) **Pre-determination:** The purpose and the legal basis of processing shall be established before the processing takes place. These shall guide the design of the processing and set the processing boundaries.

(b) **Specificity:** The purposes of processing shall be specified and explicit.

(c) **Data minimisation:** Before processing personal data, the data controller shall assess whether collecting and using the personal data are truly necessary for the intended purpose. Where the purpose can be achieved with less data, less detailed or aggregated personal data[2] or without using personal data at all, the processing shall be designed accordingly.

During processing, the data controller shall regularly review whether the personal data remains necessary. Where identification of individuals is no longer required (for example, for statistical analysis), the personal data shall be permanently deleted or anonymised as soon as practicable.

(d) **Differentiation:** The legal basis and purpose used for each processing activity shall be differentiated.

(e) **Relevance:** The correct legal basis shall be applied to the processing and clearly connected to the specific purpose of processing. The personal data processed shall be relevant to the processing in question, and the data controller shall be able to demonstrate this relevance.

(f) **Necessity:** The purpose of processing determines what personal data is required. Each type of personal data shall be collected and used only where it is necessary to achieve that purpose and where the purpose cannot reasonably be achieved by other means.

(g) **Limitation:** The data controller shall limit the collection of personal data to what is necessary for its intended purpose and shall not process personal data beyond such intended purpose. To reduce the risk of misuse or repurposing,

[1] "Specific risk profile" refers to the level and nature of risks to a data subject arising from a data controller's particular processing operation. As an example, a data controller in the healthcare services industry may have a specific risk profile such as the processing of medical records or biometric data, as compared to other industries, whereby a data controller's application of DPbD will be focused on safeguarding against reputational harm or identity theft.

[2] "Aggregated personal data" refers to information that has been combined and summarised so that it can no longer be linked to a specific individual. For example, a data controller may minimise personal data in a human resources report by reporting aggregated indicators such as average salary, leave utilisation, and staff turnover rates rather than using individual records.

the data controller shall implement appropriate technical measures (including hashing[3] and encryption[4]) and organisational measures (such as policies and contractual controls).

(h) **Review:** Regular reviews shall be conducted to verify whether the processing is necessary for the purposes for which the personal data was collected.

(i) **Cessation:** If the legal basis or purpose for processing no longer applies, the processing must cease immediately.

(j) **Adjustment:** If there is a valid change of legal basis for the processing, the actual processing shall be adjusted in accordance with the new legal basis.

(k) **Allocation of responsibility:** If multiple parties are involved in the processing, the parties shall clearly and transparently define their respective responsibilities toward the data subject and design the processing measures according to this division of roles.

(l) **Privacy-enhancing technologies (PETs):** The data controller is recommended to apply up-to-date and appropriate technologies for data minimisation.

(m) **Consent:** Where consent is the legal basis for processing, the data controller shall ensure that consent is properly obtained. The processing operation shall facilitate the withdrawal of consent process in accordance with section 38 of Act 709.

Example 1:

A café intends to launch an online platform with an ordering system, customer loyalty programme and feedback form. Before launching the platform, the café determines the purposes for processing personal data, which are to:

(i) process orders;
(ii) process payments;
(iii) notify customers when their order is ready for pickup;
(iv) verify that the correct customer is picking up the order;
(v) allow for membership benefits, including birthday rewards;
(vi) collect feedback from customers; and
(vii) send customers marketing emails about new products and promotions.

The café then identifies the minimum personal data required for the purposes of processing. For example, to limit the personal data required to verify that the correct customer is picking up an order, the café designs the platform to automatically generate a unique code for each order, so that customers can use the unique code to identify themselves when picking up their order.

[3] "Hashing" describes a one-way process to transform input data into a value of fixed length or size. For example, through the use of an algorithm on a website, logging into the website account through a password will trigger the system to compare the input data with a stored hash value in the password database. the two values match, access to the account will be granted.

[4] "Encryption" describes a process of converting human-readable text into incomprehensible text. The process is usually two-way, encryption of data is performed using a key by the sender, and upon receipt, the receiver decrypts using a separate key to recover the original human-readable data.

To account for the likely scenario where customers lose the unique code to their order, the platform collects other minimum personal data, e.g. first name and phone number, as fallback identifiers. For the café's customer loyalty programme, the café only collects the customers' birth month (and not their birth date or birth year), as it intends to offer birthday rewards that are redeemable any time during the customer's birth month.

The café then identifies the legal bases which can be relied upon for each purpose of processing.

Legal basis	*Purpose*
Performance of a contract to which the data subject is a party	(i) Process orders (ii) Process payments (iii) Notify customers when their order is ready for pickup (iv) Verify that the correct customer is picking up the order (v) Allow members to enjoy membership benefits, including birthday rewards
Consent	(i) Collect feedback from customers to improve service (ii) Send customers marketing emails about new products and promotions

The café makes sure that a separate consent is obtained when it collects personal data from customers to collect feedback about its service and to send marketing emails to customers. Customers are given the option to opt-in by ticking a checkbox to receive marketing emails when they make an order. This checkbox is by default unchecked.

Customers providing feedback via the website's online feedback form are notified to be cautious about including their personal data in the feedback form and to opt-in by ticking a checkbox to consent to the processing of the personal data that they provide in the feedback form. The checkbox is by default unchecked.

The café also ensures that by default, only the strictly necessary cookies used by the online platform are active. The additional cookies are activated only when the customer consents to their use.

Example 2:

A telecommunications company is developing a new mobile application that allows customers to manage their accounts and receive personalised offers and allows the company to monitor usage for internal analytics and service improvement. In the beginning stages of designing the app, the company identifies the purposes for processing personal data and determines the minimum personal data required and valid legal bases for processing the personal data.

Purpose	***DPbD measures***
Account management and billing	To allow customers to log in, view their personal details, update their billing information, view their bills and payment

	history and make payments, the app processes data such as a customer's name, mobile number, physical address, email address, and payment information. This is deemed necessary for the performance of the contract as these functions are integral to fulfilling the telecommunications service contract with a customer.
Personalised offers	Initially, the marketing team proposed collecting detailed location data and browsing history to create highly personalised offers. However, following the data minimisation measure, the team decides that this is excessive. Instead, they determine that offers can be effectively personalized using less intrusive data, such as a customer's current service plan, data usage volume, and call destinations (country code only). For the purpose of sending personalised offers, the company relies on customer consent. The app is designed so that customers must opt in for marketing and promotional offers by ticking a checkbox which is unchecked by default. Customers can easily withdraw their consent at any time through the app's settings.
Internal analytics and service improvement	The company notes that it is not necessary to analyse individual usage patterns linked to personal identifiers for purposes of internal analytics and service improvement and collects aggregated data (e.g. trends across broad customer segments) instead.

5.5 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the General Principle:

	General Principle Checklist	Y/N
1.	**Predetermination.** Establish the purposes and the legal basis for processing before any personal data processing takes place.	
2.	**Specificity.** Define the purpose(s) for processing as narrowly and specifically as possible.	
3.	**Data minimisation.** Minimise the collection and processing of personal data to what is strictly necessary for the identified purpose(s).	

General Principle Checklist		Y/N
4.	**Consent.** Where consent is the legal basis, ensure it is obtained through an opt-in mechanism, easily withdrawn and not using misleading or vague language.	
5.	**Assessment.** Conduct a Data Protection Impact Assessment (DPIA) before the processing to identify personal data risks and implement appropriate mitigation measures.	
6.	**Review.** Conduct regular reviews throughout the lifecycle of the personal data to verify whether the processing remains necessary for the purpose(s) for which the personal data was collected and whether the legal bases continue to apply.	

PART D: DPbD FOR NOTICE AND CHOICE PRINCIPLE

6. Notice and Choice Principle

Section 7 of Act 709 outlines the Notice and Choice Principle:

"

(1) A data controller shall by written notice inform a data subject-

- *(a) that personal data of the data subject is being processed by or on behalf of the data controller, and shall provide a description of the personal data to that data subject;*
- *(b) the purposes for which the personal data is being or is to be collected and further processed;*
- *(c) of any information available to the data controller as to the source of that personal data;*
- *(d) of the data subject's right to request access to and to request correction of the personal data and how to contact the data controller with any inquiries or complaints in respect of the personal data;*
- *(e) of the class of third parties to whom the data controller discloses or may disclose the personal data;*
- *(f) of the choices and means the data controller offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;*
- *(g) whether it is obligatory or voluntary for the data subject to supply the personal data; and*
- *(h) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data.*

(2) The notice under subsection (1) shall be given as soon as practicable by the data controller-

- *(a) when the data subject is first asked by the data controller to provide his personal data;*
- *(b) when the data controller first collects the personal data of the data subject; or*
- *(c) in any other case, before the data controller-*

(i) uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected; or
(ii) discloses the personal data to a third party.

(3) A notice under subsection (1) shall be in the national and English languages, and the individual shall be provided with a clear and readily accessible means to exercise his choice, where necessary, in the national and English languages."

6.1 The Notice and Choice Principle requires the data controller to be clear and open with the data subject about how the data controller collects, uses and share the data subject's personal data.

6.2 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Notice and Choice Principle. They are not prescriptive or exhaustive and shall be adapted by the data controller based on the specific risk profile and personal data processing operations.

(a) **Clarity:** Information shall be provided in clear, plain, concise and intelligible language.

(b) **Semantics:** Communication shall have a clear meaning to the data subject in question.

(c) **Accessibility:** Information shall be easily accessible to the data subject.

(d) **Contextual:** Information shall be provided at the relevant time and in the appropriate form.

(e) **Relevance:** Information shall be relevant and applicable to the specific data subject.

(f) **Universal design:** Information shall be accessible to the data subject. This includes the use of machine-readable languages to facilitate and automate the readability and clarity of the information.

(g) **Comprehensible:** The data subject shall have a fair understanding of what he can expect with regard to the processing of his personal data.

(h) **Multi-channel:** Information shall be provided through various channels and media, not limited to textual forms, to increase the likelihood of the information reaching the data subject effectively.

(i) **Layered:** Information shall be layered in a manner that balances completeness and understanding, while accounting for the data subject's reasonable expectations.

6.3 The data controller shall refrain from the use of deceptive design patterns in interfaces as these designs may mislead or pressure the data subject into making unintended or into making otherwise potentially harmful choices, especially those that benefit the data controller instead of protecting the data subject's best interests.

6.4 Examples of deceptive design patterns that shall be avoided include:

(a) **Overloading:** The data subject is presented with too many requests, information, options or possibilities in order to prompt the data subject to share more personal data or unintentionally allow personal data processing against the data subject's expectations.

Example: A website asks the data subject to click through four (4) different pop-up boxes just to confirm the cookie settings.

(b) **Skipping:** The interface or user journey is designed so that the data subject forgets or overlooks the data protection aspects.

Example: A social media platform requires the data subject to provide a phone number and sets the phone number's visibility setting to "Everybody" by default, even when there are other more privacy-protective settings like "Nobody" and "My Contacts".

(c) **Stirring:** Behavioural or visual prompts or nudges are used to influence the data subject's decisions. This affects the choice the data subject would make by manipulating his emotions.

Example: A social media platform displays the message "You will no longer stay connected with your friends. Are you sure?" when the data subject attempts to delete his account.

(d) **Obstructing:** The interface makes it difficult or impossible for the data subject to understand how the personal data is processed or managed.

Example: Privacy controls are not made available in standard locations such as the account settings or the website header or footer but concealed under multiple confusing steps.

(e) **Fickle:** The design of the interface is inconsistent and unclear, making it hard for the data subject to navigate different personal data protection controls and information.

Example: Usually, the red colour is used for "Delete" or "Cancel" action. However, on the data permission screen, red colour is suddenly used for the "Allow All" button to attract the attention and to confuse the data subject.

(f) **Left in the dark:** Personal data protection information or controls are hidden or complicated, causing the data subject unsure of how his personal data is processed and the rights he has over his personal data.

Example: The data subject is not informed when deleting his account that some of his personal data will still be retained even after the account is deleted, as well as the period for which the personal data will be stored.

Example:

The café ensures that customers are directed to the personal data protection notice (privacy notice) when they make an order or create a membership account. The personal data protection notice (privacy notice) is written in clear and concise language to make it easy for the customers to understand how the personal data is processed. The information is provided in a layered manner, where the most

important points are highlighted and detailed information is made easily available to further explain the various items and concepts used in the personal data protection (privacy notice). The personal data protection notice (privacy notice) is made available and is visible on all web pages of the website, so that the customer is always only one click away from accessing the information.

6.5 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Notice and Choice Principle*:*

	Notice and Choice Principle Checklist	Y/N
1.	**User-centred design.** Design systems that respect the data subject's interests through robust default privacy settings, easily accessible personal data protection notices (privacy notices) and appropriate user-friendly privacy management tools.	
2.	**Consent.** Where consent is the legal basis, ensure it is obtained through an opt-in mechanism, easily withdrawn and not using misleading or vague language.	
3.	**Notice.** Provide a personal data protection notice (privacy notice) in both the National Language and English, using clear and plain language and ensure that the notice is easily accessible and, where applicable, communicated through multiple channels or media.	
4.	**User Control**: Ensure that mechanisms enabling the data subject to exercise his rights are provided in clear and plain language, easily accessible, contextually appropriate and where applicable, communicated through multiple channels or media.	

PART E: DPbD FOR DISCLOSURE PRINCIPLE

7. Disclosure Principle

Section 8 of Act 709 outlines the Disclosure Principle:

"

Subject to section 39, no personal data shall, without the consent of the data subject, be disclosed-

(a) for any purpose other than-

(i) the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or

(ii) a purpose directly related to the purpose referred to in subparagraph (i); or

(b) *to any party other than a third party of the class of third parties as specified in paragraph 7(1)(e)*."

7.1 The Disclosure Principle requires that the data controller:

(a) obtain the data subject's consent or otherwise have a valid legal basis for the disclosure of personal data;

(b) only disclose personal data for the purpose for which the personal data was to be disclosed at the time of collection of the personal data; and

(c) only disclose personal data to the class of third parties specified in the personal data protection (privacy notice) provided to the data subject.

7.2 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Disclosure Principle. They are meant to be flexible and may be adjusted by the data controller based on the specific risk profile and the personal data processing operations.

(a) **Predetermination:** The legal basis of disclosure shall be established prior to any disclosure. Such legal basis shall guide the design of the disclosure process and set the disclosure boundaries.

(b) **Data avoidance:** The data controller shall avoid disclosing personal data altogether whenever possible for the relevant purpose. Pseudonymised[5] or aggregated personal data shall be used when feasible.

(c) **Differentiation:** The legal basis and purpose used for each disclosure activity shall be clearly differentiated.

(d) **Relevance:** The valid legal basis shall be applied to each disclosure and shall be clearly connected to the specific purpose of disclosure. The data controller shall be able to demonstrate that the personal data disclosed is relevant to that disclosure.

(e) **Necessity:** The purpose determines what personal data is necessary for the disclosure. Each personal data type shall be necessary for the specified purposes and shall only be disclosed if it is not possible to fulfil the purpose by other means.

(f) **Review:** Regular reviews shall be conducted to verify whether the disclosure remains necessary for the purposes for which the personal data was disclosed.

(g) **Cessation:** Personal data shall no longer be disclosed if the legal basis and purpose of disclosure cease to apply. Measures and safeguards shall be in place to ensure that the third party ceases processing and permanently deletes or destroys the personal data.

[5] In a personal data context, a pseudonym serves as an identifier replacing a data subject's actual identity (e.g., changing an individual's full name to 'Customer001'). This enables the data controller to perform operations and use the data without directly revealing the data subject's identity.

(h) **Adjustment:** If there is a valid change of legal basis for the disclosure, the disclosure shall be adjusted in accordance with the new legal basis.

(i) **Security:** Technical measures, including hashing and encryption, and organisational measures, such as policies and contractual obligations shall be in place to ensure that personal data is disclosed securely.

Example 1:

The café maps its data flows to identify the types of personal data that will be disclosed to third parties. It confirms that there is a legal basis for such disclosure and that customers have been informed accordingly. During the identification process, the café reviews the services specified in the contract with the online ordering system vendor.

The types of personal data may include name, phone number, ordering patterns, and payment details. Since personal data will be disclosed to the vendor for purposes of maintaining back-ups and logs, the café ensures that its agreement with the vendor clearly outlines the roles and responsibilities of each party in handling personal data. Furthermore, the agreement explicitly allows the café to conduct audits to verify the vendor's compliance with those responsibilities.

Example 2:

A specialist clinic maps its personal data flows to ensure that disclosures of patient information, such as referrals to external laboratories or insurers, are based on clearly defined legal grounds and patient consent. Disclosure boundaries are embedded into system design, allowing only the minimum necessary personal data to be shared, and pseudonymisation is applied where full identifiers are not required. Patients are informed of the third parties to whom their personal data may be disclosed through a personal data protection notice (privacy notice) during registration.

The clinic conducts regular reviews to assess whether ongoing disclosures remain necessary and relevant to the original purpose. If a disclosure purpose expires, such as after a treatment episode ends, personal data sharing is ceased and third parties are contractually required to securely delete the personal data. All disclosures are logged, encrypted and governed by personal data-sharing agreements ensuring that patient confidentiality is preserved while maintaining transparency and accountability.

Example 3:

A manufacturing company uses Internet-of-Things (IoT) sensors and cloud-based systems to monitor production efficiency and equipment condition. When disclosing operational data to third-party analytics providers or equipment vendors, the company ensures that only pseudonymised or aggregated data is shared unless personal data is strictly necessary. Disclosure boundaries are defined in advance, and all third-party contracts include clauses requiring secure handling and deletion of personal data once the purpose is fulfilled.

The company regularly reviews its personal data-sharing arrangements to ensure disclosures remain relevant and necessary. If a vendor relationship ends or the legal basis for disclosure changes, the company halts personal data transfers and verifies that previously shared personal data is securely destroyed. All disclosures are encrypted and logged and employees are trained to understand the limits and conditions under which personal data, such as employee performance metrics or access logs, may be disclosed.

7.3 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Disclosure Principle*:*

	Disclosure Principle Checklist	Y/N
1.	**Predetermination.** Establish the purposes and the legal basis of disclosure before the disclosure of personal data.	
2.	**Abstraction.** If the purpose of the processing (e.g., to compile statistics) does not require the final dataset to refer to an identified subject data, anonymise and/or delete the personal data as soon as identification is no longer necessary.	
3.	**Security.** Implement technical security measures to protect personal data (e.g., hashing and encryption) and organisational measures (e.g., policies and contractual obligations) to ensure all personal data is securely handled and disclosed.	
4.	**Consent.** Where consent is the legal basis, ensure it is obtained through an opt-in mechanism, easily withdrawn and not using misleading or vague language.	
5.	**Review.** Conduct regular reviews throughout the lifecycle of the personal data to verify whether the processing remains necessary for the purpose(s) for which the personal data was collected and whether the legal bases continue to apply.	
6.	**Third-Party Management**: Ensure that third parties have adequate personal data protection measures in place through contractual agreements or other means before transferring personal data to them.	

PART F: DPbD FOR SECURITY PRINCIPLE

8. Security Principle

Section 9 of Act 709 outlines the Security Principle:

“

(1) A data controller and a data processor shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification,

unauthorized or accidental access or disclosure, alteration or destruction by having regard-

(a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;

(b) to the place or location where the personal data is stored;

(c) to any security measures incorporated into any equipment in which the personal data is stored;

(d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and

(e) to the measures taken for ensuring the secure transfer of the personal data.

(2) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data processor shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction-

(a) provide sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and

(b) *take reasonable steps to ensure compliance with those measures*."

8.1 The Security Principle requires that the data controller and data processor take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access disclosure, alteration or destruction.

8.2 The data processor shall guarantee to the data controller that they have sufficiently robust technical and organisational security measures in place to process personal data and subsequently take reasonable steps to comply with that guarantee.

8.3 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Security Principle. They are not prescriptive or exhaustive, and shall be adapted by the data controller and data processor based on the specific risk profile and the personal data processing operations.

(a) **Information security management system:** Implement and maintain operative means of managing policies and procedures for information security.

(b) **Risk analysis:** Assess the risks against the security of personal data by considering the potential impact on the data subject and implementing measures to address identified risks. For risk assessment purposes, develop and maintain a comprehensive, and systematic "threat modelling" and an attack surface analysis of the software design to reduce attack vectors and opportunities to exploit weak points or vulnerabilities.

(c) **Security by design:** Consider security requirements as early as possible in the system design and development, and continuously integrate and perform relevant tests.

(d) **Maintenance:** Regularly review and test software, hardware, systems and services to uncover and address vulnerabilities of the systems supporting the processing of personal data.

(e) **Access control management:** Only authorised personnel who require access to personal data for their processing tasks shall be granted access and such access privileges shall be differentiated based on roles.

(f) **Access limitation:** Data processing shall be designed to ensure that only a minimal number of personnel have access to personal data to perform their duties.

(g) **Access limitation (content):** For each processing operation, limit access only to those attributes per personal data set that are required to perform that operation. Additionally, restrict access to personal data pertaining to only those data subjects who fall within the remit of the respective personnel.

(h) **Access segregation:** Personal data processing shall be designed to ensure that personal data is segregated, such that no authorised individual is required to have comprehensive access to all personal data without a legitimate interest.

(i) **Secure transfers:** Personal data transfers shall be protected against any unauthorised access or unintended changes.

(j) **Secure storage:** Data storage shall be secure from unauthorised access and alterations. Procedures shall be established to assess the risk of centralised or decentralised storage and what categories of personal data this applies to. Certain personal data may require additional security measures or isolation.

(k) **Pseudonymisation:** Personal data shall be pseudonymised as soon as it is no longer necessary for the data to be directly identifiable personal data as a security measure to minimise risks of potential personal data breaches, for example, using hashing or encryption. Identification keys shall be stored separately from the pseudonymised data.

(l) **Backups/logs:** Back-ups and logs shall be maintained to the extent necessary for information security. Audit trails and event monitoring shall be implemented as a routine security control. These records shall be protected from unauthorised or accidental access and alteration.

(m) **Disaster recovery/business continuity:** Information system disaster recovery and business continuity requirements shall be established to ensure timely restoration and the availability of personal data.

(n) **Protection according to risk:** All categories of personal data shall be protected in accordance with the individual risk of each personal data type rather than based solely on the entire data processing risk.

(o) **Security incident response management:** Establish routines, procedures and resources to detect, contain, handle, report and review personal data breaches systematically.

(p) **Incident management:** Establish processes to handle personal data breaches to make the processing system more robust. This includes notification procedures for notifying the Commissioner and affected data subjects.

Example 1:

The café ensure that privacy is embedded in the online ordering system. Customers' personal data are stored and processed in a separate encrypted database system. Before the system launch, a cybersecurity risk assessment is performed on the IT infrastructure to ensure that it functions as expected. Reassessment is performed periodically.

Example 2:

A consulting firm embeds security into its project management and client engagement systems by implementing an information security management system aligned with international standards. Client data, such as financial report, strategic plan and HR record, is stored in encrypted repositories with differentiated access controls based on project roles. During system design, threat modelling is conducted to identify potential vulnerabilities and regular penetration testing ensures ongoing resilience.

Access to personal data is strictly limited to the consultants assigned to specific projects, with further segmentation to restrict access to only relevant personal data attributes. Secure file transfers and encrypted communications are used for client interactions and pseudonymisation is applied when preparing benchmarking or analytical reports. The firm maintains a secure backups and a business continuity plan and has a documented incident response protocol to manage and report a data breach in line with Act 709 obligations.

8.4 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Security Principle*:*

	Security Principle Checklist	Y/N
1.	**Separation.** Establish technological, policy and procedural controls to prevent data linkages (e.g. isolate personal data processed for different purposes in separate databases by default).	
2.	**Abstraction.** If the purpose of the processing (e.g., to compile statistics) does not require the final dataset to refer to an identified subject data, anonymise and/or delete the personal data as soon as identification is no longer necessary.	
3.	**Access limitation.** Implement access controls to ensure that access to personal data is granted only to authorised parties with a legitimate need.	
4.	**Security.** Implement security measures to protect personal data throughout its entire lifecycle so that all personal data is collected, processed, transferred, stored and destroyed in a secured manner.	
5.	**Top-level commitment.** Ensure that top management recognises that personal data protection can coexist with legitimate business interests, and establishes a clear commitment to define and enforce high standards of personal data protection.	

Security Principle Checklist		Y/N
6.	**Accountability.** Establish a dedicated function within the organisation (e.g. the Data Protection Officer) responsible for documenting, communicating, overseeing and implementing all personal data protection policies and procedures.	
7.	**Assessment.** Conduct a Data Protection Impact Assessment (DPIA) before the processing to identify personal data risks and implement appropriate mitigation measures.	
8.	**Review.** Conduct regular reviews throughout the lifecycle of the personal data to verify whether the processing remains necessary for the purpose(s) for which the personal data was collected and whether the legal bases continue to apply.	
9.	**Risk assessment and audit.** Conduct regular risk assessments and audits to identify any potential vulnerabilities and compliance gaps.	
10.	**Third party management.** Ensure a third party has adequate personal data protection measures in place through contractual or other means before transferring personal data to that party.	
11.	**Breach management.** Establish adequate procedures and resources to detect, contain, handle, report and learn from personal data breaches.	

PART G: DPbD FOR RETENTION PRINCIPLE

9. Retention Principle

Section 10 of Act 709 outlines the Retention Principle:

"

(1) The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.

(2) *It shall be the duty of a data controller to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed*."

9.1 The Retention Principle requires that the data controller not keep the personal data for longer than is necessary for the fulfilment of purpose for which it was processed.

9.2 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Retention Principle. They are not prescriptive or exhaustive and shall be adapted by the data controller based on the specific risk profile and the personal data processing operations.

(a) **Data minimisation:** When further processing personal data, the data controller shall periodically consider whether processed personal data is still adequate,

relevant and necessary, or if it shall be deleted. If the purpose of the processing does not require the final dataset to refer to an identified or identifiable data subject (e.g. for statistical purposes), but the initial processing does (e.g. before data aggregation), then the data controller shall permanently delete personal data as soon as identification is no longer needed.

(b) **Deletion and/ or anonymisation:** Where personal data is not, or is no longer necessary for the purpose, personal data shall be anonymised and/or permanently deleted. There shall be clear internal procedures and functionalities for deletion and/or anonymisation.

(c) **Effectiveness of anonymisation/ deletion:** The data controller shall ensure that it is not possible to re-identify anonymised data or recover deleted data, and shall test whether such re-identification or recovery can be performed.

(d) **Automation:** Deletion of certain personal data shall be automated.

(e) **Retention criteria:** The data controller shall determine what personal data and its length of retention is necessary.

(f) **Justification:** The data controller shall be able to justify why such identified retention period is necessary and be able to disclose the rationale of the retention period, including its legal grounds.

(g) **Enforcement of retention policies:** The data controller shall enforce internal retention policies and conduct tests to ensure they are properly enforced.

(h) **Backups/logs:** The data controller shall determine what personal data and retention periods are necessary for backups and logs.

(i) **Data flow:** The data controller shall be aware of the flow of personal data and the storage of any copies thereof and seek to limit their temporary storage. The personal data flow shall be made efficient enough to not create more copies than necessary.

Example 1:

The database storing customer personal data is designed such that the retention period of each personal data is automatically generated upon its addition to the database and personal data that reaches the expiry of its retention period are automatically deleted.

Example 2:

A local social media platform collects user-generated content[6], location data and behavioural analytics to personalise feeds and serve targeted advertisements. The platform enforces clear personal data retention rules for example, deleting deactivated accounts and associated personal data after a defined period. When a data subject deletes posts or messages, the personal data is securely wiped from both live and backup systems. Personal data shared with advertisers is aggregated

[6] Digital material such as in text, image, video or audio formats created by social media platform users.

and anonymised, ensuring that such the data subject cannot be re-identified, while still enabling business insights.

9.3 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Retention Principle*:*

	Retention Principle Checklist	Y/N
1.	**Data minimisation.** Minimise the collection and processing of personal data to only what is strictly necessary for the identified purpose(s).	
2.	**Abstraction.** If the purpose of the processing (e.g., to compile statistics) does not require the final dataset to refer to an identified subject data, anonymise and/or delete the personal data as soon as identification is no longer necessary.	
3.	**Access limitation.** Implement access controls to ensure that access to personal data is granted only to authorised parties with a legitimate need.	
4.	**Security.** Implement security measures to protect personal data throughout its entire lifecycle so that all personal data is collected, processed, transferred, stored and destroyed in a secured manner.	

PART H: DPbD FOR DATA INTEGRITY PRINCIPLE

10. Data Integrity Principle

Section 11 of Act 709 outlines the Data Integrity Principle:

"*A data controller shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed*."

10.1 The Data Integrity Principle requires the data controller to take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date by having regard to the purpose for which the personal data was collected and further processed.

10.2 A DPbD approach in compliance with the Data Integrity Principle further requires the data controller to take reasonable steps regarding the personal data of data subjects under the age of eighteen (18) years. This includes ensuring that the sourcing and rectification of such personal data are made easily accessible to the parent, guardian or person who has parental responsibility for that data subject.

10.3 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Data Integrity Principle. They are not prescriptive or

exhaustive and shall be adapted by the data controller based on the specific risk profile and the personal data processing operations.

(a) **Data source:** Sources of personal data shall be reliable to ensure personal data accuracy.

(b) **Degree of accuracy**: Each personal data element shall be as accurate as necessary for the specified purposes.

(c) **Attributable recording:** The data controller shall have identifiable records of when and why a personnel or system inserts personal data during the sourcing stage.

(d) **Verification:** Depending on the nature of the personal data, in relation to how often it may change, the data controller shall verify the correctness of personal data with the data subject before and at different stages of the processing (for example, verification requirements depending on attaining retirement age).

(e) **Rectification:** The data controller shall facilitate the rectification of inaccurate data without delay upon the request of the data subject.

(f) **Error-propagation avoidance:** The data controller shall mitigate the effect of accumulated errors in the processing chain.

(g) **Access:** The data subject shall be provided with information and given effective access to personal data in accordance with the Access Principle to ensure accuracy and to rectify as needed.

(h) **Continued accuracy:** Personal data shall be accurate at all stages of the processing and tests as to accuracy shall be carried out at critical steps of processing.

(i) **Up-to-date:** Personal data shall be updated if necessary for the purpose of processing.

(j) **Data design:** The data controller shall use technological and organisational design features to minimise inaccuracy, for example by presenting concise predetermined choices instead of free-text fields.

Example:

A fintech company offers a platform for personal loans. To ensure personal data integrity, the company implements a robust system to verify the accuracy of customer information, as the integrity of this personal data is critical for accurate credit risk assessment and loan disbursement. When a customer applies for a loan, the platform uses a "know your customer" (KYC) verification process that cross-references the personal data provided (name, NRIC number, address) with reliable government and financial databases. This serves as a primary personal data source verification, reducing the risk of errors.

The company also builds features to facilitate user-led data accuracy. During the application process, the platform displays a summary of the provided information, prompting the user to review and confirm its accuracy before submission, thereby providing an opportunity for rectification. For certain dynamic personal data points,

such as an applicant's residential address, the system includes a periodic verification prompt. For instance, six months after a loan is disbursed, the customer receives a notification to confirm if their address or contact details are still up to date, ensuring the personal data remains accurate for ongoing communications and account management.

Furthermore, the company's internal systems are designed to prevent the propagation of errors. Any change to a customer's personal data, whether initiated by the customer or the company's personnel, undergoes an automated validation check before being committed to the central database. This ensures that any inaccuracies are caught at the point of entry and not carried forward into other linked processes, such as credit scoring models or disbursement instructions. This approach safeguards the integrity of the personal data throughout its lifecycle, from collection to processing, thereby protecting both the company from financial risk and the customer from receiving a misleading or inaccurate service.

10.4 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Data Integrity Principle*:*

	Data Integrity Principle	Y/N
1.	**Accessibility.** Put in place mechanisms that enable the data subject to easily access his own personal data.	
2.	**Data design.** Use technological and organisational design features to minimise inaccuracy, for example by presenting concise predetermined choices instead of free-text fields.	
3.	**User Control.** Ensure that mechanisms enabling the data subject to exercise his rights are provided in clear and plain language, easily accessible, contextually appropriate and where applicable, communicated through multiple channels or media.	
4.	**Rectification**. Facilitate the rectification of inaccurate personal data without delay upon the request of the data subject.	
5.	**Review.** Conduct regular accuracy tests on personal data.	

PART I: DPbD FOR ACCESS PRINCIPLE

11. Access Principle

Section 12 of Act 709 outlines the Access Principle:

"*A data subject shall be given access to his personal data held by a data controller and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up to date, except where compliance with a request to such access or correction is refused under this Act*."

11.1 The Access Principle requires data controller to allow the data subject to access his personal data and to correct any data that is inaccurate, incomplete, misleading or not up-to-date upon receiving correction requests pursuant to Section 34 of Act 709. The data subject shall be informed of the designated point of contact to whom such requests should be submitted. Contact information shall be easily accessible and located in strategic locations such as within user accounts, in contextual information (e.g., information displayed during the use of services), personal data protection notices (privacy notices), Frequently Asked Questions (FAQs) and other appropriate channels.

11.2 A DPbD approach in compliance with the Access Principle further requires the data controller to design appropriate systems for personal data belonging to the data subject under the age of eighteen (18) years. Such systems shall ensure that access to such personal data is easily accessible to the data subject's parent, guardian or person who has parental responsibility for that data subject.

11.3 The following concepts and applications are intended to guide the implementation of DPbD in complying with the Access Principle. They are not prescriptive or exhaustive and shall be adapted by the data controller based on the specific risk profile and the personal data processing operations.

(a) **Clarity:** Information on how to exercise the data subject's right shall be provided in clear, plain, concise and intelligible language.

(b) **Accessibility:** Mechanisms for exercising the data subject's rights shall be easily accessible to the data subject.

(c) **Contextual:** Mechanisms for exercising the data subject's rights shall be provided at the relevant time and in the appropriate form.

(d) **Universal design:** Mechanisms for exercising the data subject's rights shall be accessible to the data subject, including the use of machine-readable languages to facilitate and automate readability and clarity.

(e) **Comprehensible:** The data subject shall have a fair understanding of what he can expect with regards to the extent to which he can exercise his personal data rights.

(f) **Multi-channel:** Mechanisms to exercise the data subject's rights shall be provided through various channels and media, not limited to textual form, to increase the likelihood of the information reaching the data subject effectively.

Example:

The café ensures that customers can easily exercise their rights regarding their personal data. Within their respective account profiles, quick access options are available for customers to download their personal data in an accessible format, update their data or delete accounts. Customers will be notified immediately upon receipt of their request and provided with instructions on how to track their request status until the verification stage. In addition, contact details are provided should customers require further support.

11.4 The following checklist sets out a range of non-exhaustive measures for applying a DPbD approach in complying with the Access Principle:

	Access Principle Checklist	Y/N
1.	**Accessibility.** Provide mechanisms that enable the data subject to easily access his own personal data.	
2.	**User-centred design.** Design systems that respect the data subject's interests through strong privacy defaults and personal data protection notices (privacy notices) that are easily accessible and located in appropriate places.	
3.	**User Control.** Ensure that mechanisms enabling the data subject to exercise his rights are provided in clear and plain language, easily accessible, contextually appropriate and where applicable, communicated through multiple channels or media.	

12. Checklist

12.1 A checklist has been developed to guide the implementation of the DPbD approach. The checklist as provided in **Annex A**, outlines non-exhaustive measures for implementing DPbD, organised into two (2) categories:

(a) **Data-Oriented Measures:** focusing on the technical aspects of data processing; and

(b) **Process-Oriented Measures:** focusing on the organisational and procedural aspects of data processing.

PART J: BEST PRACTICES FOR DPbD GOVERNANCE

13. Best practices

13.1 DPbD is about establishing an organisational culture that adopts a principled, proactive approach to personal data management. This approach shall be applied across the organisation and reflected in its products, services, governance and operations. This shall involve:

(a) a clear commitment from senior management to set and enforce high standards of data protection;

(b) fostering a culture where all stakeholders share a commitment to continuous improvement in data protection standards; and

(c) establishing processes to identify gaps in current designs and practices and address issues before they occur proactively and systematically.

13.2 The following illustration outlines best practices for implementing DPbD governance. These are non-mandatory and intended to guide organisations, which are encouraged

to apply them using a risk-based approach aligned with their respective risk profile and operational context.

(a) Ensuring senior leadership commitment and their active participation in establishing a robust and proactive personal data protection framework, such as by:

  (i) ensuring the Board of Directors includes members with data protection expertise or ensuring directors receive adequate training in the field;

  (ii) ensuring directors allocate sufficient resources to DPbD measures, including for technological enhancements;

  (iii) designating at least one senior manager or Head of Department to be responsible for the organisation's personal data compliance;

  (iv) incorporating personal data protection compliance into senior management performance evaluation;

  (v) mandating regular personal data assessments and audits to be reported to the Board of Directors;

  (vi) hold regular meetings with the organisation's Data Protection Officer (DPO), where applicable.

(b) Conducting periodic audits of personal data protection policies to verify their practical effectiveness and operational compliance.

(c) Developing systematic methods, including Data Protection Impact Assessments (DPIA) to identify and assess risks to ensure any negative impacts are mitigated before they occur.

(d) Fostering a culture and environment where all stakeholders including users, are encouraged to suggest improvements to data protection practices, and ensuring such suggestions are systematically reviewed and adopted where appropriate.

ANNEX A: DATA-ORIENTED AND PROCESS-ORIENTED MEASURES CHECKLIST

Data-Oriented Measures		Y/N
1.	**Predetermination.** Establish the purposes and the legal basis for processing before the processing takes place.	
2.	**Specificity.** Define the purpose(s) for processing as narrowly and specifically as possible.	
3.	**Data minimisation.** Minimise the collection and processing of personal data to only what is strictly necessary for the identified purpose(s).	
4.	**Separation.** Establish technological, policy and procedural controls to prevent combining personal data sets obtained from different sources, commonly referred to as data linkages. For example, isolate personal data processed for different purposes in separate databases by default.	
5.	**Abstraction.** If the purpose of the processing (e.g., to compile statistics) does not require the final dataset to refer to an identified subject data, anonymise and/or delete the personal data as soon as identification is no longer necessary.	
6.	**Access limitation.** Implement access controls to ensure that access to personal data is granted only to authorised parties with a legitimate need.	
7.	**Security.** Implement security measures to protect personal data throughout its entire lifecycle so that all personal data is collected, processed, transferred, stored and destroyed in a secured manner.	
8.	**User-centred design.** Design systems that respect the data subject's interests through strong privacy defaults and personal data protection notices (privacy notices) that are easily accessible and located in appropriate places.	
Process-Oriented Measures		
9.	**Consent.** Where consent is the legal basis, ensure it is obtained through an opt-in mechanism, easily withdrawn and not using misleading or vague language.	
10.	**Notice.** Provide a personal data protection notice (privacy notice) in both the National Language and English, using clear and plain language and ensure that the notice is easily accessible and, where applicable, communicated through multiple channels or media.	
11.	**User Control.** Ensure that mechanisms enabling the data subject to exercise his rights are provided in clear and plain language, easily accessible, contextually appropriate and where applicable, communicated through multiple channels or media.	
12.	**Top-level commitment.** Ensure that top management recognises that personal data protection can coexist with legitimate business interests, and	

	establishes a clear commitment to define and enforce high standards of personal data protection.	
13.	**Accountability.** Establish a dedicated function within the organisation (e.g. the Data Protection Officer) responsible for documenting, communicating, overseeing and implementing all personal data protection policies and procedures.	
14.	**Assessment.** Conduct a Data Protection Impact Assessment (DPIA) before the processing to identify personal data risks and implement appropriate mitigation measures.	
15.	**Review.** Conduct regular reviews throughout the lifecycle of the personal data to verify whether the processing remains necessary for the purpose(s) for which the personal data was collected and whether the legal bases continue to apply.	
16.	**Risk assessment and audit.** Conduct regular risk assessments and audits to identify any potential vulnerabilities and compliance gaps.	
17.	**Third-Party Management**: Ensure that third parties have adequate personal data protection measures in place through contractual agreements or other means before transferring personal data to such parties.	
18.	**Breach management.** Establish adequate procedures and resources to detect, contain, handle, report and learn from personal data breaches.	