PUBLIC CONSULTATION PAPER NO. 2/2025:

DATA PROTECTION BY DESIGN GUIDELINE

Start Date: 20 March 2025

End Date: 19 May 2025

PART 1: INTRODUCTION AND BACKGROUND

1.1 Section 5 of the Personal Data Protection Act 2010 (“**Act 709**”) provides that the processing of personal data by a data controller shall be in compliance with the prescribed Personal Data Protection Principles[1] (“**PDP Principles**”) (“**PDP Principles Compliance Requirement**”). The Personal Data Protection (Amendment) Act 2024 has imposed an obligation on data processors to comply with the Security Principle as specified in section 9 under Act 709. However, there is no explicit requirement for data controllers and data processors to implement “data protection by design” (“**DPbD**”).

1.2 DPbD is a well-established concept and has been expressly codified in the legislation of the European Union General Data Protection Regulation (“**EU GDPR**”) and the Philippines’ National Privacy Commission Circular 2023-06 on Security of Personal Data in the Government and the Private Sector (“**Philippines NPC Circular**”). Some of the principles in the DPbD concept have also been incorporated into data privacy laws worldwide, including the Act 709. Among these principles are:

(i) purpose specification — the purposes for which personal data is processed must be communicated to the data subject at or before the time the data is collected (*notice and choice principle*);

(ii) use, retention, and disclosure limitation — the use, retention, and disclosure of personal data must be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law (*general principle*);

(iii) security — measures must be applied to assure continued confidentiality, integrity and availability of the personal data and accuracy (*security principle*); and

(iv) data integrity — personal data must be as accurate, complete and up-to-date as is necessary to fulfil the specified purposes (*integrity principle*).

Thus, while DPbD is not a concept that is currently expressly referenced in the Act 709, its principles are inherently reflected in the PDP Principles.

1.3 The adoption of a DPbD approach is vital in moving from reactive data protection to proactive data protection by encouraging data controllers to integrate privacy considerations into all aspects of their personal data management **from the beginning to the end and by default**. It helps data controllers to ensure effective compliance with the PDP Principles and strengthen protection of data subject rights.

[1] The seven personal data protection principles as set out in Sections 6 to 12 under Act 709.

1.4 To ensure that Malaysia's personal data protection framework remains current, effective and aligned with the global data protection regulatory landscape, it is proposed that a guideline ("**DPbD Guideline**") is issued to provide guidance on how to adopt a DPbD approach in complying with the PDP Principles.

1.5 Pursuant to the above, this public consultation paper ("**PCP**") seeks to gather public feedback regarding aspects that will be or should be included and addressed in the DPbD Guideline.

PART 2: PROPOSED DPBD REQUIREMENT

2.1 As an overview, Part 2 of this PCP is categorised as follows:

(a) Definition of DPbD;

(b) Seven foundational principles of DPbD;

(c) How to implement DPbD in each of the PDP Principles; and

(d) Protecting children's privacy.

[A] Definition of DPbD

2.2 **Background:** DPbD is an approach that calls for the incorporation of data protection measures into the design and development of projects, systems, programmes, processes and technologies **from the beginning**, rather than as an afterthought. It requires privacy considerations to be taken into account **at all stages of a data processing operation**, from inception through to the development and implementation phases. It advocates a **proactive stance** to personal data protection, emphasising the importance of anticipating and preventing privacy breaches, rather than reacting to data protection issues after they have occurred.

Example of DPbD in practice

A marketing team has a database of email addresses collected from customers signing up for email newsletters, placing product orders and registering for product exhibitions. The Act 709 requires personal data to be permanently deleted when it is no longer required for the purpose it was processed for (*retention principle*). To comply with the Act 709, the team belatedly creates a database query to find out when the email addresses were collected and adds a standard timeframe for when the addresses might no longer be needed. Email addresses that reach the expiry of that timeframe would be flagged for manual review by the team to decide if they should be deleted.

This approach creates gaps in data protection — the team struggles to track when and for what purpose the email addresses were collected for; some email addresses are retained for longer than necessary because the standard timeframe is arbitrarily decided.

A DPbD approach may be to instead design the database so that each email address is automatically assigned an appropriate retention period when it is added to the database. Then, once an email address reaches the end of its retention period, it is automatically deleted, or at least automatically blocked from further use until its reviewed.

2.3 The EU GDPR defines DPbD as follows:

Article 25 of the EU GDPR:

"Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

2.4 In the Philippines NPC Circular, DPbD is defined as below:

> **<u>The Philippines NPC Circular:</u>**
>
> *“O. **“Privacy-by-Design”** refers to an approach to the development and implementation of projects, programs, and processes that integrate into the design or structure safeguards that are necessary to protect and promote privacy unto the design or structure of a processing activity or a data processing system;*
>
> *P. **“Privacy-by-Default”** refers to the principle according to which the PIC/PIP ensures that only data necessary for each specific purpose of processing is processed by default, without the intervention of the data subject;”*
>
> *“7. A PIC or PIP shall consider Privacy-By-Design principles in its processing activities and enable Privacy-By-Default in its data processing systems without requiring any action from its data subjects.*
>
> *Further, a PIC or PIP must also conduct a PIA on its Off-The-Shelf Software, solutions, or data processing systems, as outlined in Section 5 of this Circular.*
>
> *Any functions that lack a lawful basis for processing or are incompatible with the general data privacy principles, must be switched off or deactivated.*
>
> *8. A PIC or PIP should incorporate data privacy requirements throughout the development and implementation of data processing systems."*

2.5 **<u>Proposal:</u>** DPbD is proposed to be defined as:

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

2.6 The proposed definition of DPbD is intended to:

(a) integrate and link the DPbD concept with the PDP Principles Compliance Requirement to adapt it to the Malaysian regulatory framework and facilitate understanding of the concept;

(b) be not overly prescriptive to allow organizations of varying sizes and nature to adapt their approach in implementing DPbD;

(c) adopt similar language to the EU GDPR to enable global a uniform approach to data protection practices and based on useful precedent and practices developed in other countries, including the EU.

Question 1

(a) What are your views on the proposed definition of DPbD? Is the definition too open-ended or too prescriptive?

(b) What are your views on the proposed example?

[B] Seven foundational principles of DPbD

2.7 **Background:** There are seven foundational principles[2] which guide the practical application of DPbD. They are:

(a) proactive not reactive; preventative not remedial;

(b) privacy as the default setting;

(c) privacy embedded into design;

(d) full functionality – positive sum, not zero sum;

(e) end-to-end security – full lifecycle protection;

(f) visibility and transparency – keep it open; and

(g) respect for user privacy – keep it user-centric.

2.8 **Proposal:** It is proposed that the DPbD Guideline will reference the seven foundational principles[3] of DPbD as a guiding framework for how to implement DPbD and provide illustrations on how to operationalize these foundational principles in practice. These foundational principles and illustrations are not intended to be mandatory or exhaustive.

[2] See https://www.ipc.on.ca/sites/default/files/legacy/2018/01/pbd.pdf.

[3] Based on https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

[B.1] DPbD Principle 1: Proactive not reactive; preventative not remedial

2.9 DPbD Principle 1, **"proactive not reactive; preventative not remedial"**, is about anticipating and preventing privacy risks before they occur and actively building processes to prevent data breaches instead of reacting to them when they happen.[4]

2.10 Data controllers / data processors must begin with an explicit recognition that protecting privacy is more effective when done early and continuously, rather than later on. This means:

(a) making a clear commitment, at the highest levels of the organization, to set and enforce high standards of privacy;

(b) making a privacy commitment that is shared by all stakeholders, in a culture of continuous improvement; and

(c) establishing methods to recognise poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive and systematic ways.

Operationalizing "proactive not reactive; preventative not remedial"[5]

- Having senior leadership commit to and participate in establishing a strong, proactive privacy programme in the organization, including by:
  - ensuring that there is someone with personal data protection expertise on the board and that directors receive appropriate training in personal data protection;
  - ensuring directors allocate adequate resources to the personal data protection programme;
  - designating at least one senior manager to be accountable for the organization's personal data protection compliance;
  - incorporating personal data protection compliance as part of senior management's performance evaluation and compensation;
  - requiring personal data protection assessments and audits to be undertaken and reported to the board on a regular basis; and

[4] Based on https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

[5] Based on https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf.

    - asking senior management the right questions about personal data protection practices in the organization.

- Conducting regular audits on personal data protection policies to verify their effectiveness in practice.

- Developing systematic methods including personal data protection impact assessments to assess personal data protection risks to correct any negative impacts before they occur.

- Fostering a culture and environment where all stakeholders including users are encouraged to suggest improvements to personal data protection practices, and these suggestions being systematically reviewed and appropriately adopted.

Question 2

What are your views on adopting DPbD Principle 1 as one of the guiding principles for how to implement DPbD?

[B.2] DPbD Principle 2: Privacy as the default setting

2.11 DPbD Principle 2, **"privacy as the default setting"**, is about ensuring personal data is automatically protected in any given system[6]. This means that, **even if an individual does nothing, their privacy remains secure**. No action is required on the part of the individual to protect their privacy − it is built into the system, by default. This privacy-by-default approach can be distilled into the following key practices:

(a) **Purpose specification:** The purposes for which personal data is collected, used, retained and disclosed must be communicated to the data subject at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

(b) **Collection limitation:** The collection of personal data must be lawful and limited to that which is necessary for the specified purposes.

(c) **Data minimization:** The collection of personal data must be kept to a strict minimum. The design of programs, information and communications

[6] Based on https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

technologies and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and associability (capability of being linked) of personal data should be minimized.

(d) **Use, retention and disclosure limitation:** The use, retention, and disclosure of personal data must be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal data must be retained only as long as necessary to fulfil the stated purposes, and then securely destroyed.

(e) **Where the need or use of personal data is not clear, there shall be a presumption of privacy and the precautionary principle shall apply:** the default settings shall be the most privacy protective.

Operationalizing "privacy as the default setting"[7]

- Begin with no collection of personal data, unless and until a specific and compelling purpose for data collection is defined. Adopt as narrow and specific a purpose(s) for personal data collection as possible. Adopt opt-in consent systems.

- Minimize the collection of data at the outset to only what is strictly necessary for the identified purpose(s).

- Limit the use and retention of personal data to the specific purposes for which it was collected.

- Create technological, policy and procedural barriers to data linkages with personal data. For example, isolate personal data processed for different purposes by default in separate databases or systems that prevent exchange of data. This includes putting in place access controls to ensure only those who need to access the data are allowed access. For online platforms, refrain from making user profiles publicly viewable until the user takes affirmative steps to allow it.

Question 3

What are your views on adopting DPbD Principle 2 as one of the guiding principles for how to implement DPbD?

[7] Based on https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf.

[B.3] DPbD Principle 3: Privacy embedded into design

2.12 DPbD Principle 3, **"privacy embedded into design"**, is about integrating privacy into technologies, operations, and information architectures in a holistic, integrative and creative way[8]. This involves:

(a) taking a systemic, principled approach to embedding privacy - one that relies upon established standards and frameworks, which allow for external reviews and audits, and that applies the PDP Principles consistently throughout the design and operation processes;

(b) conducting, wherever possible, detailed data protection impact assessments, which clearly document the privacy risks and all measures taken to mitigate those risks, including considering alternatives; and

(c) ensuring personal data protections that minimize the privacy risks of the resulting technology, operation or information architecture, and should not be easily compromised through use, misconfiguration or error.

Example of "privacy embedded into design" in practice

A fashion retailer is looking to launch an online store to sell its clothing and accessories to customers. At the start of the development of the website, the design team sets out privacy as one of the objectives of the website. The team carefully evaluates web development and web design tools and frameworks for privacy-enhancing options and ensures that the website meets established information security system standards.

A dedicated database system that employs multi-layered encryption protocols is utilised to store and process customers' personal data. A user-centric identity management system is implemented to provide a unified user experience across different devices with readily accessible personal data protection notices and built-in features that allow users to easily access, delete and correct their personal data.

Before launching the online store, the team conducts a data protection impact assessment on the IT infrastructure to identify any privacy risks. Measures are put in place to mitigate the identified privacy risks. Routine audits and assessments are conducted post-launch to ensure the ongoing effectiveness of the privacy features.

[8] Based on https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

Question 4

What are your views on adopting DPbD Principle 3 as one of the guiding principles for how to implement DPbD?

[B.4] DPbD Principle 4: Full functionality – positive sum, not zero sum

2.13 DPbD Principle 4, **"full functionality – positive sum, not zero sum"**, is about accommodating all legitimate interests and objectives in a manner that benefits all stakeholders, without making unnecessary trade-offs against privacy[9]. It rejects false concepts that privacy cannot coexist with other legitimate business interests. This means:

(a) when embedding privacy into a given technology, process, or system, it should be done in such a way that full functionality is not impaired and all requirements are optimized to the greatest extent possible; and

(b) all interests and objectives, desired functions and metrics should be clearly articulated, documented, agreed upon and applied, and trade-offs should be rejected in favour of finding a solution that enables multi-functionality.

Operationalizing "full functionality – positive sum, not zero sum"[10]

- Acknowledge that multiple, legitimate business interests can coexist.
- Engage in communication, consultation and collaboration to better understand multiple and, at times, opposing interests.
- Pursue innovative solutions and options to achieve multiple functionalities.

Example of "full functionality – positive sum, not zero sum" in practice[11]

A building is upgrading its old video surveillance system to enhance both efficiency and security. The old system relies on security personnel to monitor a large number of live video screens to manually track intruders and observe restricted areas of the building.

[9] Based on https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.
[10] Based on https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf.
[11] Based on https://www.researchgate.net/publication/284780818_How_Is_Positive-Sum_Privacy_Feasible.

To simultaneously achieve the objectives of privacy, efficiency and security, the new video surveillance system features two operational modes:

(i) a less privacy-invasive default operational mode for intrusion detection in restricted areas; and

(ii) a highly invasive alert mode for tracking and locating of intruders.

In the default mode, the system performs relatively non-invasive intrusion detection. Human detection and tracking algorithms are only running on specific cameras that cover restricted areas and the cameras' video streams are not shown to the operator. No personal data is recorded in this default mode. Only when an intruder is detected does the system switch to alert mode, which enables tracking of the intruder and recording of the camera footage.

Question 5

What are your views on adopting DPbD Principle 4 as one of the guiding principles for how to implement DPbD?

[B.5] DPbD Principle 5: End-to-end security – full lifecycle protection

2.14 DPbD Principle 5, **"end-to-end security – full lifecycle protection"**, emphasizes ensuring data security throughout the entire lifecycle of the personal data involved — all data should be securely retained, and then securely destroyed at the end of the process, in a timely fashion. There should be no gaps in either protection or accountability. This means:

(a) assuming responsibility for the security of personal data throughout its entire lifecycle, based on the degree of sensitivity and consistent with established data security standards; and

(b) among others, implementing methods of secure destruction, appropriate encryption, and strong access controls and logging methods to ensure the confidentiality, integrity and availability of personal data throughout its lifecycle.

Operationalizing "end-to-end security – full lifecycle protection"[12]

An e-commerce retailer uses Transport Layer Security (TLS) encryption technology (a cryptographic protocol) to safeguard data inputted by customers during the checkout process, ensuring data is secure during transmission.

Data stored at rest in the retailer's database is encrypted using Advanced Encryption Standard (AES)-256 technology, with encryption keys securely managed in a dedicated key management system. Automated, encrypted backups ensure data integrity, and a comprehensive disaster recovery plan is established to restore operations quickly and recover customer data in case of a data breach or system failure.

Secure APIs and end-to-end encryption protect data transmitted between the retailer's systems and external partners, such as payment processors and logistics service providers.

Staff use multi-factor authentication to log into the e-commerce platform. Role-based access control ensures only authorized personnel can access specific data – sales representatives only have access to customer orders specifically assigned to them to provide personalized customer service, inventory managers only have access to stock levels to monitor product availability, marketing managers only have access to customer demographic data, purchasing trends and campaign performance analytics to tailor marketing strategies and promotions. Anonymization and data aggregation techniques are used for marketing analytics to protect customer identities while still gaining valuable insights. Endpoint protection measures are employed to secure devices accessing customer data. Staff receive ongoing training on privacy and data security best practices to minimize the risk of human error.

Clear data retention policies are established to dictate how long customer data is kept. Upon reaching the defined data retention period, secure deletion methods are employed to completely remove customer data.

Question 6

What are your views on adopting DPbD Principle 5 as one of the guiding principles for how to implement DPbD?

[12] Based on https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf.

[B.6] DPbD Principle 6: Visibility and transparency – keep it open

2.15 DPbD Principle 6, **"visibility and transparency – keep it open"**, is about demonstrating accountability for personal data processing activities. Personal data should be handled in accordance with stated promises and objectives, subject to independent verification. This involves:

(a) **Accountability:** The collection of personal data entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures should be documented and communicated as appropriate and assigned to a specified individual. When transferring personal data to third parties, ensure that equivalent personal data protection is in place through contractual or other means;

(b) **Openness:** Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal data should be made readily available to individuals; and

(c) **Compliance:** Complaint and redress mechanisms should be established and clearly communicated to individuals, including how to escalate issues. Measures to monitor, evaluate and verify compliance with personal data protection policies and procedures should be taken.

Example of "visibility and transparency – keep it" in practice

An e-commerce platform delivers 'just-in-time' personal data protection notices when customers are prompted to provide their personal data, e.g. when they create a user account or make an order. The said notice is written in clear and concise language and organised in a layered manner – key points are emphasized using different font size and style and a link is provided to more detailed information. A pop-up personal data protection notice is also displayed on the platform to inform customers about personal data that is automatically collected when the customer accesses the platform, such as cookies, web beacons, tracking scripts and other applications used by the platform. On all web pages of the platform, there is an easily visible link to a comprehensive personal data protection notice.

Question 7

What are your views on adopting DPbD Principle 6 as one of the guiding principles for how to implement DPbD?

[B.7] DPbD Principle 7: Respect for user privacy – keep it user-centric

2.16 DPbD Principle 7, **"respect for user privacy – keep it user-centric"**, is about keeping the interests of the individual by offering measures such as strong privacy defaults, appropriate notice, and empowering user-friendly options.

2.17 Projects, products, services, systems and processes should be consciously designed around the interests and needs of individual users, who have the greatest vested interest in the management of their own personal data. This involves:

(a) **Consent:** The individual's free and specific consent is required for the collection, use or disclosure of personal data, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.

(b) **Accuracy:** Personal data must be as accurate, complete, and up-to-date as is necessary to fulfil the specified purposes.

(c) **Access:** Individuals should be provided access to their personal data and informed of its uses and disclosures. Individuals should be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

(d) **Compliance:** Organisations should establish complaint and redress mechanisms and communicate information about them to the public, including how to access the next level of appeal.

Example of "respect for user privacy – keep it user-centric" in practice

A mobile app focussed on fitness support presents users with clear, straightforward options regarding what personal information they wish to share when they create or update their profile. The app employs a separate consent for different data processing purposes, enabling users to toggle access to specific data points – such as gender, relationship status, location, fitness history, etc. The app also has a privacy dashboard which provides users with insights into what data is collected and how it is used and options to customize their personal data protection preferences, e.g. for sharing of data for analytical purposes or personalized content recommendations. In-app notifications about updates to personal data protection policies are communicated timely and openly, ensuring users are informed before any changes affect their personal data.

Question 8

What are your views on adopting DPbD Principle 7 as one of the guiding principles for how to implement DPbD?

[C] How to implement DPbD in each PDP Principles

2.18 **Background:** The EU Guidelines 4/2019 on Article 25 Data Protection by Design and by Default ("**EU Guidelines**") were issued by the European Data Protection Board in 2020 to provide guidance on the interpretation of the DPbD obligation under Article 25 of the GDPR, examples of the design and default elements of each data protection principle and recommendations on how controllers, processors and producers can cooperate to achieve DPbD.

2.19 **Proposal:** Similar to the position in the EU, it is proposed that the DPbD Guideline will describe and provide practical examples of how to implement DPbD for the seven **PDP Principles** under the Act 709 similar to the position in the EU.

2.20 The PbD Guideline will outline key elements on how to operationalize DPbD for each of the **PDP Principles** drawing from the EU Guidelines.

[C.1] General Principle

2.21 **The general principle**[13] requires that data controllers:

(a) identify a valid legal basis for the processing of personal data;

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

(c) only process personal data that is adequate, relevant and limited to what is necessary for the purpose.

2.22 Data controllers should shape the design of their data processing operations by what is necessary to achieve the purpose(s) of the data processing operations. Measures and safeguards should be in place to ensure that the whole processing lifecycle is in line with the relevant legal grounds and purposes of processing.

[13] Act 709, s. 6.

2.23 Key DPbD elements for this principle include:

(a) **Data minimization:** Data controllers should first of all determine whether they even need to process personal data for their relevant purposes. Data controllers should verify whether the relevant purposes can be achieved by processing less personal data or having less detailed or aggregated personal data or without having to process personal data at all. Such verification should take place before any processing takes place.

Data minimization can also refer to the degree of identification. If the purpose of the processing does not require the final set of data to refer to an identified or identifiable individual (such as in statistics), but the initial processing does (e.g. before data aggregation), **then the data controller should delete or anonymize personal data as soon as identification is no longer needed**. Or, if continued identification is needed for other processing activities, personal data should be pseudonymized to mitigate risks for the data subjects' rights.

(b) **Predetermination:** The purposes and the legal basis of processing should be established before the **processing** takes place. These should guide the design of the processing and set the processing boundaries.

(c) **Specificity:** The purposes of **processing** should be specified and explicit.

(d) **Data avoidance:** Data controllers should avoid processing personal data altogether when this is possible for the relevant purpose. Aggregated data should be used when possible.

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

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

(g) **Necessity:** The purpose determines what personal data is necessary for the processing. Each type of personal data must be necessary for the specified purposes and should only be processed if it is not possible to fulfil the purpose by other means.

(h) **Limitation:** Data controllers should limit the amount of personal data collected to what is necessary for the purpose. There should be no further processing for purposes beyond the purposes for which they were collected and processed. Technical measures, including hashing and encryption, and organisational measures, such as policies and contractual obligations, should be implemented to limit the possibility of repurposing personal data.

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

(j) **Cessation:** If the legal basis and purpose of processing ceases to apply, the processing must cease accordingly.

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

(l) **Allocation of responsibility:** If more than one data controller is involved in the processing, the parties should apportion in a clear and transparent way their respective responsibilities vis-à-vis the data subject and design the measures of the processing in accordance with this allocation.

(m) **Privacy enhancing technologies:** Data controllers are recommended to apply up to date and appropriate technologies for data avoidance and minimisation.

(n) **Consent:** Where consent is the legal basis, data controllers should ensure that consent is freely given, specific, informed and unambiguous. The processing operation should facilitate withdrawal of consent and make withdrawal as easy as giving consent.

Example of applying DPbD to the General Principle in practice[14]

A café intends to launch an online ordering system with a customer loyalty programme to allow customers to order ahead of time and pick up their orders and enjoy certain membership benefits. Before it launches the system, it lists the reasons for requiring customers' personal data, which are to:

- process orders
- process payments
- notify customers when their order is ready for pickup
- verify that the correct customer is picking up the order
- allow members to enjoy membership benefits, including birthday rewards

[14] Based on https://ethyca.com/blog/data-minimization-a-privacy-engineers-guide-on-getting-started.

- collect feedback from customers to improve service
- send customers marketing emails about new products and promotions

The café identifies the types of customer personal data collected and verifies whether each type of personal data is necessary for the purposes of processing. For example, it finds that it is not necessary for customers to create an account to make an order. Successful orders automatically generate a unique code, which the customers can use to identify themselves when picking up their orders. It thus collects only the minimum personal data necessary for customers to make an order, i.e. their first name and email address, in case a customer fails to record down the unique code. The café also discovers that, while the membership form collects the birth date, including the day, month and year, of customers in order to allow members to redeem rewards on their birthday, there is in fact no need to collect the birth year of the members.

It 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	● Process orders ● Process payments ● Notify customers when their order is ready for pickup ● Verify that the correct customer is picking up the order ● Allow members to enjoy membership benefits, including birthday rewards
Consent	● Collect feedback from customers to improve service ● Send customers marketing emails about new products and promotions

The café makes sure that separate and specific 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 receiving marketing emails when they make an order. This checkbox is by default unchecked.

Customers providing feedback via the website's online feedback form are explicitly reminded 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 makes sure that by default only the strictly necessary cookies are active. More cookies are activated only when the customer explicitly consents to them.

<u>Question 9</u>

What are your views / suggestions on the key DPbD elements for the General Principle?

[C.2] Notice and Choice Principle

2.24 **The notice and choice principle**[15] requires data controllers to be clear and open with data subjects about how they will collect, use and share their personal data.

2.25 Key PbD elements for this principle include:

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

(b) **Semantics:** Communication should have a clear meaning to the audience in question.

(c) **Accessibility:** Information should be easily accessible for the data subject.

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

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

(f) **Universal design:** Information should be accessible to all data subjects, include use of machine-readable languages to facilitate and automate readability and clarity.

[15] Act 709, s. 7.

(g) **Comprehensible:** Data subjects should have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups.

(h) **Multi-channel:** Information should be provided in different channels and media, to increase the probability for the information to effectively reach the data subject.

(i) **Layered:** The information should be layered in a manner that resolves the tension between completeness and understanding, while accounting for data subjects' reasonable expectations.

2.26 There must be no **deceptive design patterns,** i.e. interfaces and user journeys that aim to influence users into making unintended, respectively unwilling, and/or potentially harmful decisions, often toward an option that is against the users' best interests and in favour of the data controller's interest.

2.27 Examples of deceptive design patterns include:

(a) **Overloading:** Users are confronted with an avalanche / large quantity of requests, information, options or possibilities in order to prompt them to share more data or unintentionally allow personal data processing against the expectations of data subject.

(b) **Skipping:** Designing the interface or user journey in a way that the users forget or do not think about all or some of the data protection aspects.

(c) **Stirring:** Affects the choice users would make by appealing to their emotions or using visual nudges.

(d) **Obstructing:** an obstruction or blocking of users in their process of getting informed or managing their data by making the action hard or impossible to achieve.

(e) **Fickle:** The design of the interface is inconsistent and not clear, making it hard for users to navigate the different data protection control tools and to understand the purpose of the processing.

(f) **Left in the dark:** An interface is designed in a way to hide information or data protection control tools or to leave users unsure of how their data is processed and what kind of control they might have over it regarding the exercise of their rights.

Example of applying DPbD to the Notice and Choice Principle in practice

The café makes sure that the customers are directed to the personal data protection / privacy notice when they make an order or create a membership account. The personal data protection / privacy notice is written in clear and concise language to make it easy for the customers to understand how their 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 notice. The personal data protection / privacy notice is made available and visible on all web pages of the website, so that the customer is always only one click away from accessing the information.

Question 10

(a) ***What are your views / suggestions on the key DPbD elements for the Notice and Choice Principle?***

(b) ***How do you think we can facilitate people with disabilities to access the personal data protection notice / privacy notice?***

[C.3] Disclosure Principle

2.28 **The disclosure principle**[16] requires that data controllers:

(a) obtain data subjects' 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 subjects.

2.29 Key DPbD elements for this principle include:

(a) **Predetermination:** The legal basis of disclosure should be established before the disclosure takes place. These should guide the design of the disclosure and set the disclosure boundaries.

[16] Act 709, s. 8.

(b) **Data avoidance:** Data controllers should avoid disclosing personal data altogether when this is possible for the relevant purpose. Pseudonymized or aggregated data should be used when possible.

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

(d) **Relevance:** The correct legal basis must be applied to the disclosure and clearly connected to the specific purpose of disclosure. The personal data disclosed should be relevant to the disclosure in question, and the data controller should be able to demonstrate this relevance.

(e) **Necessity:** The purpose determines what personal data is necessary for the disclosure. Each type of personal data must 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 should be conducted to verify whether the disclosure is necessary for the purposes for which the data is disclosed.

(g) **Cessation:** If the legal basis and purpose of disclosure ceases to apply, personal data shall no longer be disclosed. Measures and safeguards should be in place to ensure that the third parties to which the personal data were disclosed securely destroy the personal data.

(h) **Adjust:** If there is a valid change of legal basis for the disclosure, the actual disclosure should 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, should be in place to ensure that personal data is disclosed securely.

Example of applying DPbD to the Disclosure Principle in practice

The café maps the data flows to identify the types of personal data will be disclosed to third parties and confirm that there is a legal basis for such disclosure and that the customers were informed of such disclosure. As it will be disclosing personal data to the vendor of the online ordering system for purposes of maintaining back-ups and logs, it makes sure that its agreement with the vendor clearly outlines the roles and responsibilities of the parties in handling personal data and allows the café to conduct an audit to verify compliance with such responsibilities.

<u>Question 11</u>

What are your views / suggestions on the key DPbD elements for the Disclosure Principle?

[C.4] <u>Security Principle</u>

2.30 **The security principle**[17] requires that data controllers and data processors take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

2.31 Key DPbD elements for this principle include:

(a) **Information security management system (ISMS):** Have an 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 impact on individuals' rights and counter identified risks. For use in risk assessment; develop and maintain a comprehensive, systematic and realistic "threat modelling" and an attack surface analysis of the designed software to reduce attack vectors and opportunities to exploit weak points and 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, etc. to uncover vulnerabilities of the systems supporting the processing.

(e) **Access control management:** Only authorized personnel who need access to the personal data for their processing tasks should have access, and such access privileges should be differentiated.

(f) **Access limitation:** Data processing should be shaped in a way that a minimal number of people need access to personal data to perform their duties.

(g) **Access limitation (content):** For each processing operation, limit access to only those attributes per data set that are needed to perform that operation. Also limit access to data pertaining to those data subjects who are in the remit of the respective personnel.

[17] Act 709, s. 9.

(h) **Access segregation:** Shape the data processing in a way that no individual needs comprehensive access to all data collected about a data subject, much less all personal data of a particular category of data subjects.

(i) **Secure transfers:** Transfers must be secured against unauthorized and accidental access and changes.

(j) **Secure storage:** Data storage must be secure from unauthorized access and changes. There should be procedures to assess the risk of centralized or decentralized storage, and what categories of personal data this applies to. Some data may need additional security measures than others or isolation from others.

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

(l) **Backups/logs:** Keep back-ups and logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control. These shall be protected from unauthorised and accidental access and change and reviewed regularly and incidents should be handled promptly.

(m) **Disaster recovery / business continuity:** Address information system disaster recovery and business continuity requirements to restore the availability of personal data following up major incidents.

(n) **Protection according to risk:** All categories of personal data should be protected with measures adequate with respect to the risk of a security breach. Data presenting special risks should, when possible, be kept separated from the rest of the personal data.

(o) **Security incident response management:** Have in place routines, procedures and resources to detect, contain, handle, report and learn from data breaches.

(p) **Incident management:** Have processes in place to handle breaches and incidents, in order to make the processing system more robust. This includes notification procedures to the supervisory authority and data subjects.

Example of applying DPbD to the Security Principle in practice[18]

The café makes sure that privacy is embedded in the online ordering system. Customers' personal data are stored and processed in a separate database system, which employs encryption keys of varying lengths based on the type of data. Additionally, before the launch of the system, a risk assessment is performed on the IT infrastructure to ensure that it works as expected before it goes live. This assessment is performed periodically even after the system goes live.

Question 12

What are your views / suggestions on the key DPbD elements for the Security Principle?

[C.5] Retention Principle

2.32 **The retention principle**[19] requires that data controllers not keep the personal data processed longer than is necessary for the fulfilment of that purpose.

2.33 Key DPbD elements for this principle include:

(a) **Data minimization:** When further processing personal data, data controllers should periodically consider whether processed personal data is still adequate, relevant and necessary, or if the data should be deleted. If the purpose of the processing does not require the final set of data to refer to an identified or identifiable individual (such as in statistics), but the initial processing does (e.g. before data aggregation), then the data controller should delete personal data as soon as identification is no longer needed.

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

(c) **Effectiveness of anonymization/deletion:** The data controller shall make sure that it is not possible to re-identify anonymized data or recover deleted data and should test whether this is possible.

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

[18] Based on https://www.dpoconsultancy.com/liveblog/a-practical-example-of-how-to-apply-privacy-by-design.
[19] Act 709, s. 10.

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

(f) **Justification:** The data controller shall be able to justify why the retention period is necessary for the purpose and the personal data in question and be able to disclose the rationale behind and legal grounds for the retention period.

(g) **Enforcement of retention policies:** The data controller should enforce internal retention policies and conduct tests of whether the organisation practices its policies.

(h) **Backups/logs:** The data controller should determine what personal data and length of retention is necessary for back-ups and logs.

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

Example of applying DPbD to the Retention Principle in practice

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

Question 13

What are your views / suggestions on the key DPbD elements for the Retention Principle?

[C.6] Data Integrity Principle

2.34 **The data integrity principle**[20] requires data controllers 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.

[20] Act 709, s. 11.

2.35 Key DPbD elements for this principle include:

(a) **Data source:** Sources of personal data should be reliable in terms of data accuracy.

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

(c) **Measurably accurate:** Reduce the number of false positives (e.g. a contact tracing app alerts the wrong individual that he / she has been identified as having been exposed to an infectious disease and is at high risk) / false negatives (e.g. a contact tracing app fails to alert an individual identified as high risk), for example biases in automated decisions and artificial intelligence.

(d) **Verification:** Depending on the nature of the data, in relation to how often it may change, the data controller should verify the correctness of personal data with the data subject before and at different stages of the processing (e.g. to age requirements).

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

(f) **Error propagation avoidance:** Data controllers should mitigate the effect of an accumulated error in the processing chain.

(g) **Access:** Data subjects should be given information about and effective access to personal data in accordance with the Access principle in order to control accuracy and rectify as needed.

(h) **Continued accuracy:** Personal data should be accurate at all stages of the processing, tests of accuracy should be carried out at critical steps.

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

(j) **Data design:** Use of technological and organisational design features to decrease inaccuracy, for example present concise predetermined choices instead of free text fields.

Example of applying DPbD to the Data Integrity Principle in practice

See the example provided under **C.7 (Access Principle)** below.

Question 14

What are your views / suggestions on the key DPbD elements for the Data Integrity Principle?

[C.7] Access Principle

2.36 **The access principle**[21] requires data controllers to allow data subjects to have access to their personal data and to correct data that is inaccurate, incomplete, misleading or not up to date[22] as well as to withdraw consent to the processing of their personal data[23]. Data subjects should easily know to whom they should address a claim when they want to exercise their rights. Contact information should be easily accessible and located in logical places, for example in the user account, in contextual information, personal data protection / privacy notice, FAQs, etc.

2.37 Key DPbD elements for this principle include:

(a) **Clarity:** Information about how to exercise data subject rights should be in clear and plain language, concise and intelligible.

(b) **Accessibility:** Mechanisms to exercise data subject rights should be easily accessible for the data subject.

(c) **Contextual:** Mechanisms to exercise data subject rights should be provided at the relevant time and in the appropriate form.

(d) **Universal design:** Mechanisms to exercise data subject rights should be accessible to all data subjects, include use of machine readable languages to facilitate and automate readability and clarity.

(e) **Comprehensible:** Data subjects should have a fair understanding of what they can expect with regards to the extent to which they can exercise their rights.

(f) **Multi-channel:** Mechanisms to exercise data subject rights should be provided in different channels and media, not only the textual, to increase the probability for the information to effectively reach the data subject.

[21] Act 709, s. 6.
[22] Act 709, s. 12.
[23] Act 709, s. 38.

Example of applying DPbD to the Access Principle in practice

The café makes sure that customers are able to easily exercise their rights to their personal data. In their account profile, there are quick options for customers to download their personal data in an accessible format, to edit their personal data and to delete their account. Customers are immediately informed about the receipt of their request and how to track the progress of their request and contact the business if they require further support.

Question 15

What are your views / suggestions on the key DPbD elements for the Access Principle?

[D] Protecting children's privacy

2.38 **Background:** Children merit specific protection with regard to their personal data as they are often less aware (i.e. due to their age, maturity and developmental capacity) of the risks, consequences and safeguards, and their rights in relation to the processing of their personal data.

2.39 While privacy rights of children have traditionally been regarded as a matter for adults to determine, children's privacy needs may actually differ from and even conflict with those of adults. Adults' interpretations of children's privacy needs can constrain children's rights to privacy and autonomy. Examples being adult reliance on surveillance for protection and the growing trend of "sharenting" – where parents post information about their children online, effectively shaping their online identity long before they have capacity to give consent. Further, children without a stable home environment, such as homeless children, unaccompanied children, children in “out of home” care, and other children in other vulnerable situations, may lack the support and guidance needed from adults to protect their privacy.

2.40 Data controllers therefore hold a crucial responsibility in ensuring that the products and services that they offer protect children's personal data by design so as to allow children to safely benefit from participation both in the online and offline space.

2.41 **Proposal:** It is proposed that the DPbD Guideline will include specific guidance on and prescriptive requirements in relation to the implementation of DPbD for data processing operations involving children's personal data.

Question 15

What are your views / suggestions on addressing processing of children's personal data within the DPbD Guideline?

[D.1] Scope of application

2.42 **Proposal:** It is proposed that providers of products or services directed at, intended for or likely to be accessed by children will be required to comply with this section on protecting children's privacy in accordance with the DPbD.

2.43 In an offline context, this can include educational providers, sports and social clubs and communities and health and social support providers. In a digital context, this includes websites, apps and other internet-of-things services which provide social media, media sharing, gaming, entertainment, educational, advocacy, social support services. The scope should cover services that a significant number of children are in reality using, even if the product or service in question was not primarily intended for children or originally designed with them in mind.

Question 16

(a) What are your views / suggestions on the scope of application?

(b) Should any exemptions apply?

[D.2] The best interests of child

2.44 **Proposal:** It is proposed that data controllers have an obligation to take into account the best interests of children in the processing of children's personal data when their products or services are directed at, intended for or likely to be accessed by children.

2.45 The concept of the best interests of the child comes from Article 3 of the United Nations Convention on the Rights of the Child, which states:

> *"In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."*

2.46 Data controllers must consider how, in their use of children's personal data, they can:

(a) keep children safe from exploitation risks, including the risks of commercial or sexual exploitation and sexual abuse;

(b) protect and support children's health and wellbeing;

(c) protect and support children's physical, psychological and emotional development;

(d) protect and support children's need to develop children's own views and identity;

(e) protect and support children's right to freedom of association and play;

(f) support the needs of children with disabilities;

(g) recognise the role of parents in protecting and promoting the best interests of the child and support them in this task; and

(h) recognise the evolving capacity of the child to form their own view, and give due weight to that view.

2.47 Taking account of the best interests of the child does not mean that a data controller cannot pursue its own commercial or other interests. A data controller's commercial interests may not be incompatible with the best interests of the child, but the controller must account for the best interests of the child as a primary consideration where any conflict arises.

Question 17

(a) What are your views on the requirement for data controllers to have regard to the best interests of children in the processing of children's personal data when their products or services are directed at, intended for or likely to be accessed by children?

(b) What are your views on the elements that should be taken into account when assessing children's best interests?

[D.3] Age verification

2.48 **Proposal:** In line with the GDPR,[24] an explicit requirement should be introduced for data controllers to make reasonable efforts to verify that they have received consent

[24] GDPR, Art. 8(2).

to process personal data of children. This in certain circumstances entails the requirement to establish age verification mechanisms.

2.49 There is no one-size-fits-all solution to the issue of age verification. Appropriate age verification mechanisms are likely to vary from context to context, depending on, for example, factors such as the service being provided and the sensitivity of the personal data being processed. In any event, such measures should be proportionate and grounded on a risk-based approach. This means that there should be greater stringency and levels of certainty provided by the particular verification process where the processing of personal data undertaken by the organisation is of higher risk to the user. For example, self-declaration may be suitable for low-risk processing or when used alongside other techniques, while some online services that present a high risk arising from data processing may require more stringent methods of age verification.

2.50 Below is a list of the most common age verification mechanisms:[25]

(a) **Self-declaration:** This most common of all methods has been shown to be easily bypassed by children. Examples include self-declaring one's date of birth.

(b) **Credit card:** Here, users are required to verify the validity of their cards, for instance, by making a bank or card payment of RM0.01. This method is mostly used by e-commerce sites and apps selling adult products such as alcohol or adult content. Beyond the inherent risk of phishing, it is not possible to ascertain that the person using the card is the legitimate owner; moreover, the age for owning a credit card varies across countries.

(c) **Biometrics:** This method relies on artificial intelligence (AI), which powers the use of biometric technologies, including facial recognition applications. These may be used to analyse facial features with a selfie to ascertain that the individual requesting access is over 18. Establishing a person's age with accuracy is prone to errors; furthermore, underage individuals may use the face of someone older to gain unjustified access. What is more, authentication methods that use biometrics raise privacy issues because they may use sensitive personal data. Using applications to estimate a child's age can also lead to excessive data processing and to profiling.

(d) **Inferential age verification systems:** This involves using age verification systems by inference, such as importing the individual's internet browsing history or analysing their 'maturity' by means of a questionnaire or their online user-generated content or purchases.

[25] Reference: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf.

(e) **Offline verification:** This is done using scratch cards or offline in-situ age checks by means of documents. For instance, the online service may require adult individuals to retrieve "scratch cards", allowing them to retrieve a login identifier and password that would give them access to age-restricted content. Such cards would be offered in certain sales outlets, such as supermarkets or tobacco shops, whose staff already carry out age verifications in connection with the sale of alcohol, cigarettes and gambling.

(f) **Verification of parental consent:** This might involve checking traditional identity (ID) documents.

(g) **Vouching:** This involves asking users other than the parents to vouch online as confirmation that a child seeking online access is of the right age.

(h) **Digital ID:** This method relies on tools offered by the state to verify individuals' identity and age before granting them access to digital services. For instance, China. Canada and Australia have introduced a digital ID for citizens. Some EU countries have also adopted this solution, and there is a proposal to create a European digital identity wallet.

2.51 It should be emphasized that compliance with the requirement in no way justifies the “locking out” of children from an online service or the provision of a two-tier approach with an inferior level of central services and features offered on the one hand to child users while on the other hand, the provision of a more superior service to adult users, simply on the basis of purported data protection compliance. Such an approach may be perceived by children as blocking them from the more complete “full” service offering, or as blocking them from accessing other features of the service they are seeking to use. It also risks driving children “underground” – where they feel compelled to lie about their age in order to access what they perceive to be as a more fulsome “adult” service. This in turn can be counter-productive on the organisation’s part in that it may result in child users circumventing age verification measures and accessing a service which does not adhere to the highest levels of data protection as required for children.

2.52 **Verification of parental consent:** The GDPR currently provides that a data user shall obtain consent from the parent, guardian or person who has parental responsibility on the data subject if the data subject is under the age of 18 years. In line with the GDPR,[26] an express requirement should be introduced for data controllers to make reasonable efforts to verify that consent was given by such parent / guardian / person with parental responsibility taking into consideration available technology. A proportionate and risk-based approach should be adopted such that greater stringency and levels of certainty is provided by the particular verification process where the processing of personal data undertaken by the organisation poses higher risks to the child. For instance, whereas low-risk processing by an organisation may only require verification consisting of

[26] GDPR, Art. 8(2).

sending a parent a confirmation email (to which they must respond), higher-risk processing might call for more thorough verification methods such as requesting proof of ID.

2.53 **Minimum user ages:** It is common practice among online service providers to apply a minimum user age. However, the setting of a minimum user age does not remove the requirement for such service providers to comply with their obligations towards child users below this age, where such children are nevertheless likely to use the service in question. Where a service provider stipulates that their service is not for the use of children below a certain age, they should take steps to ensure that their age verification mechanisms are effective at preventing children below that age from accessing their service. If the organisation considers that it cannot prevent children below its stipulated age threshold from accessing its service, then the organisation should ensure that appropriate standards of data protection measures are in place to safeguard the position of child users, both below and above the organisation's official user age threshold.

Question 18

(a) What are your views on the requirement for data controllers to make reasonable efforts to verify that they have received consent to process personal data of children?

(b) Do you foresee any practical difficulties in implementing this requirement?

[D.4] Implementing DPbD in the processing of children's personal data

2.54 Organisations should ensure that the strictest privacy settings apply to services directed at, intended for, or likely to be accessed by children. Consideration must be given to the DPbD principles and measures described in the section above on how to implement DPbD in each of the **PDP Principles**.

2.55 Particular consideration should be given to providing age-appropriate **notice and choice** for children.

2.56 The key DPbD elements include:

(a) **Language:** Data controllers must use clear, concise and child-friendly language to explain to children exactly what it is that they are doing with their personal data. Children are often unaware that personal data includes things like photos or videos of them, or that their personal data is being collected for specific reasons, such as providing customised in-app experiences and advertisements, or even that their personal data will be retained for a certain period of time.

(b) **Accessibility:** Information should be available in an obvious, easy-to-find place, e.g. not in tiny writing at the bottom of a webpage or app screen. Information should not appear in a way that nudges the user to accept, for example by appearing as a pop-up or making the option to consent more obvious or less obstructive to the user experience than the option to find out more or withhold consent. Children should not have to go searching for this information. Data controllers should also take into consideration the device used to access the service (e.g. smartphone, computer, connected devices or toys), whether non-textual methods of communication, such as cartoons and videos, might be more suitable than solely textual methods, or whether electronic means such as layered information notices, hover-over notices or pop-up notices are appropriate.

(c) **Context:** Information should not only be provided upon sign-up to a service or at the initial point of collection of personal data. Organisations should consider using methods such as just-in-time notifications to inform children and young people about the implications of sharing their personal data at a particular moment in time, for example just before they post or share something online or before they change default privacy settings.

(d) **Parental dashboard:** Where appropriate, provide parents with an overall view of activity (including any history of activity) and settings that their child has available to them. Child accounts should have available information on the functionality of such dashboards.

(e) **Exercising data subject rights:** Data controllers should have dedicated, clear and child-friendly user flows in place to enable children and/or their parents or guardians to easily exercise their data subject rights.

For organisations which use automated tools to manage data subject requests, it is important that they consider, up front at the design stage of their user flows, the circumstances where exceptions may arise which would call for individual assessments (i.e. non-automated, with human involvement in the assessment). Such evaluation should consider the specific context of the type of personal data they are processing and assess whether it would be generally appropriate to deal with a child data subject in an automated manner through self-service tools. In general terms, if an organisation deems it appropriate to engage with and offer services to child users above a certain age where the child user will generally autonomously interact with the service, those child users will likely be in a position to exercise their own data protection rights vis-à-vis that service / organisation.

Question 19

What are your views / suggestions on the key DPbD elements for the processing of children's personal data?

[D.5] <u>Prohibition of profiling or automated decision making concerning children</u>

2.57 **<u>Proposal:</u>** It is proposed that data controllers must not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/marketing purposes unless they can clearly demonstrate how and why it is in the best interests of children to do so.

Question 20

(a) What are your views on the prohibition of profiling or automated decision making concerning children?

(b) What are your views on when exemptions should apply?