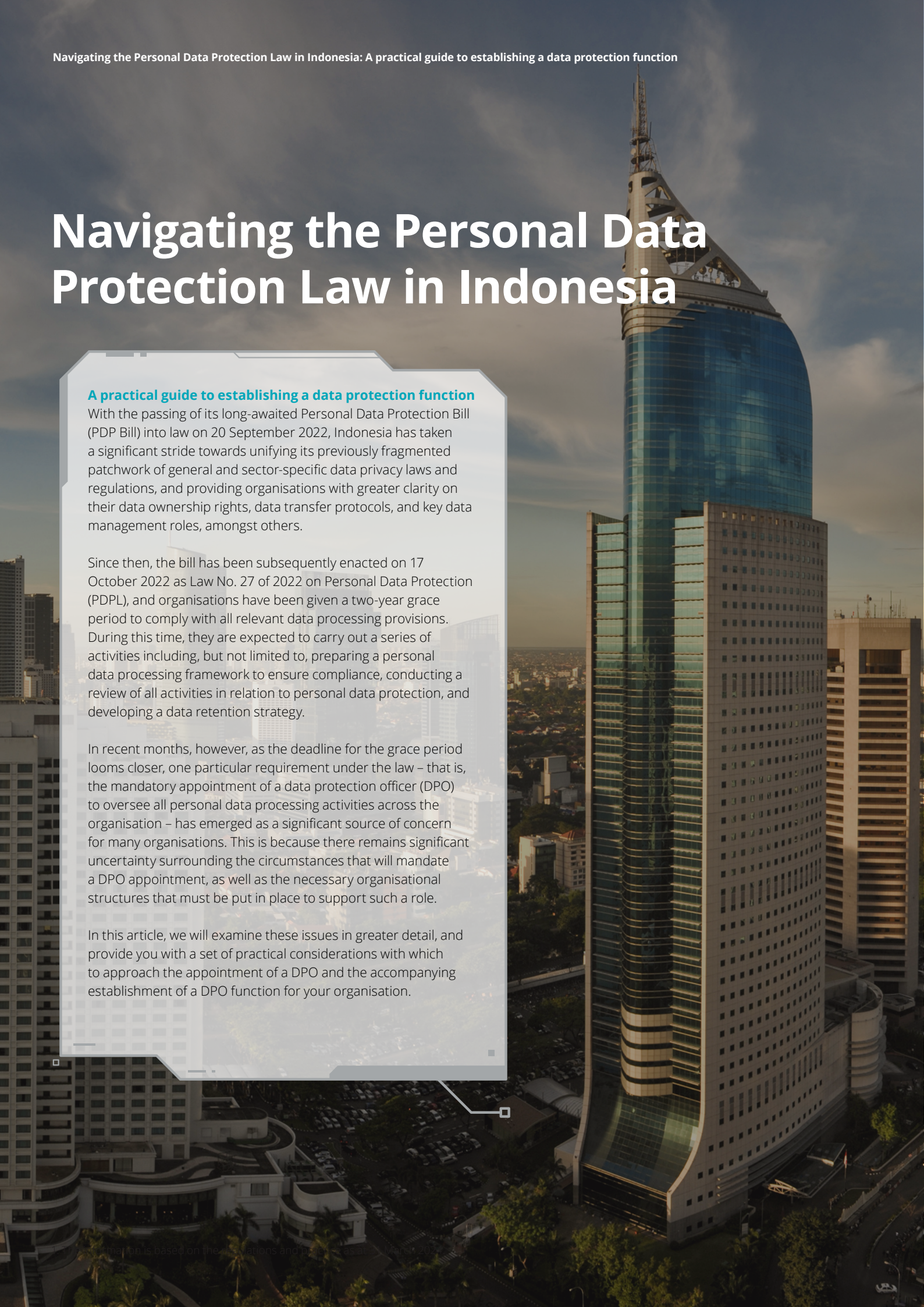
Deloitte.

Navigating the Personal Data Protection Law in Indonesia: A practical guide to establishing a data protection function

June 2024

MAKING AN IMPACT THAT MATTERS since 1845

Navigating the Personal Data Protection Law in Indonesia



A practical guide to establishing a data protection function

With the passing of its long-awaited Personal Data Protection Bill (PDP Bill) into law on 20 September 2022, Indonesia has taken a significant stride towards unifying its previously fragmented patchwork of general and sector-specific data privacy laws and regulations, and providing organisations with greater clarity on their data ownership rights, data transfer protocols, and key data management roles, amongst others.

Since then, the bill has been subsequently enacted on 17 October 2022 as Law No. 27 of 2022 on Personal Data Protection (PDPL), and organisations have been given a two-year grace period to comply with all relevant data processing provisions. During this time, they are expected to carry out a series of activities including, but not limited to, preparing a personal data processing framework to ensure compliance, conducting a review of all activities in relation to personal data protection, and developing a data retention strategy.

In recent months, however, as the deadline for the grace period looms closer, one particular requirement under the law – that is, the mandatory appointment of a data protection officer (DPO) to oversee all personal data processing activities across the organisation – has emerged as a significant source of concern for many organisations. This is because there remains significant uncertainty surrounding the circumstances that will mandate a DPO appointment, as well as the necessary organisational structures that must be put in place to support such a role.

In this article, we will examine these issues in greater detail, and provide you with a set of practical considerations with which to approach the appointment of a DPO and the accompanying establishment of a DPO function for your organisation.

[illegible] information is based on the [illegible] regulations and [illegible] as at [illegible] 2022.

Appointing a DPO

Elucidation of PDPL defines DPO as officials or officers who are responsible for ensuring compliance with the Personal Data Protection principles and mitigating the risk of personal Data Protection breach. Under the PDPL, an organisation is obliged to mandatorily appoint a DPO, or an officer functioning in a similar capacity, in the event that it is involved in the processing of personal data for public services, the core activities of its personal data controller have the nature, scope, and/or purposes that require regular and systematic monitoring of Personal Data on a large scale, and where the core activities of its personal data controller involve the regular and large-scale processing of specific personal data and/or personal data relatedto criminal activities.

While there remains some uncertainty on the specific thresholds of these conditions that will need to be addressed through further guidance from the Ministry of Communications and Informatics (MCI) and/or the forthcoming Indonesia PDP supervisory authority, it is likely that a significant number of organisations will be impacted. Based on MCI estimates, Indonesia is likely to require approximately 140,000 DPOs in its workforce, nearly twice that of the 75,000 DPOs in the European Union (EU) following its implementation of the General Data Protection Regulation (GDPR) in 2018[1].

To err on the side of caution, it would therefore be prudent for organisations to carefully consider their specific circumstances and take the necessary steps to prepare for the appointment of a DPO. Even if the organisation does not met the condition where a DPO appointment is strictly mandated,an organisation could still benefit from the guidance of a DPO in navigating the complexities of the PDPL and enhancing their overall data protection readiness.

Roles and responsibilities of a DPO

Under Article 53 of the PDPL, organisations are required to appoint a DPO based on their "professionalism, knowledge of the law, PDP practices, and ability to fulfil their duties". Briefly, a non-exhaustive list of responsibilities for a DPO, as outlined by Article 54 of the PDPL, includes:

1. Advising the data controller or processor to comply with the PDPL;
2. Monitoring and ensuring the compliance of the controller or processor with the PDPL and the controller or processor's policies;
3. Assessing impacts on personal data protection and monitoring the performance of the data controller and processor; and
4. Coordinating and acting as a liaison for issues related to the processing of personal data.

It is worth noting that the PDPL does not limit the role of the DPO to individuals possessing legal qualifications. Any individual with the necessary technical expertise and managerial experience may be appointed to the role, provided they possess an adequate understanding of the legal framework of the PDPL. Nevertheless, while the PDPL and its draft implementing regulations do not specify the required skillsets and qualifications for a DPO, Decree No. 103 of 2023 issued by the Ministry of Manpower on 23 June 2023 offers some insight into the required competencies for this role.

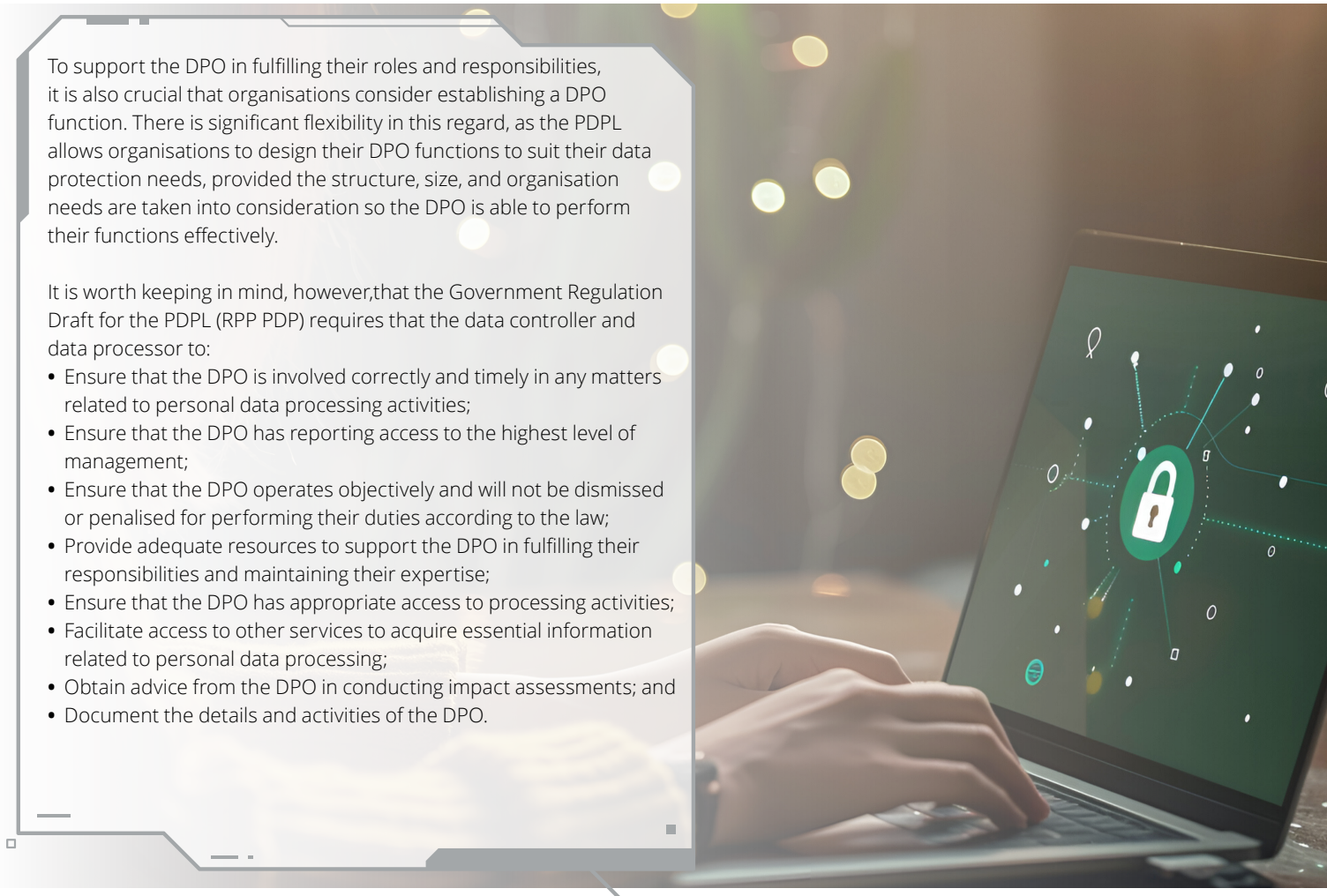
1. "Bakal Jadi Profesi Baru, Inilah Empat Tugas PPDP". Ministry of Communications and Informatics. 29 October 2022; "Study: GDPR's global reach to require at least 75,000 DPOs worldwide". International Association of Privacy Professionals. 9 November 2016.

Known as Standar Kompetensi Kerja Nasional Indonesia (SKKNI), the standard sets forth a total of 19 competencies across four key functions that DPOs should possess in order to fulfil their roles and responsibilities as mandated by the PDPL (see Figure 1). Looking ahead, SKKNI is also set to become the primary reference framework for DPO training and certification programs to be developed by the National Professional Certification Agency (BNSP) or other BNSP-approved agencies.

Figure 1: The SKKNI framework

Unit	Competency	Main function	Key function
Unit 1	Determining the groundwork for personal data protection work program	Preparing the personal data protection work program	Planning the personal data protection work program
Unit 2	Determining the structural needs of the personal data protection team		
Unit 3	Determining the personal data protection framework	Preparing the personal data protection framework	
Unit 4	Identifying laws and regulations related to personal data protection		
Unit 5	Determining the personal data protection strategy		
Unit 6	Establishing the personal data protection risk matrix criteria	Handling risk management analysis on personal data processing	Managing the personal data protection work program
Unit 7	Conducting the personal data protection impact assessment		
Unit 8	Testing the effectiveness of the personal data protection work program		
Unit 9	Establishing personal data protection governance	Handling the governance of personal data protection that is integrated into the existing system	
Unit 10	Establishing personal data protection management on its domain		
Unit 11	Implementing the personal data protection work program		
Unit 12	Conducting compliance supervision on personal data protection work program against the regulations	Monitoring the implementation of the personal data protection program	Ensuring the sustainability of the personal data protection program
Unit 13	Formulating advice to related management		
Unit 14	Managing audits related to personal data protection work program	Handling audits of the personal data protection work program	
Unit 15	Ensuring follow-up actions of audit results		
Unit 16	Formulating the process of obtaining consent for personal data collection	Realising information requests from data subjects and personal data protection authority	Responding to information requests and personal data protection
Unit 17	Providing responses towards personal data information requests in accordance with the provision		
Unit 18	Ensuring that personal data protection has been integrated into incident response management	Realising incident response related to personal data protection disclosure	Failure incidents
Unit 19	Ensuring the management of personal data protection failure incidents		

Establishing a DPO function



To support the DPO in fulfilling their roles and responsibilities, it is also crucial that organisations consider establishing a DPO function. There is significant flexibility in this regard, as the PDPL allows organisations to design their DPO functions to suit their data protection needs, provided the structure, size, and organisation needs are taken into consideration so the DPO is able to perform their functions effectively.

It is worth keeping in mind, however,that the Government Regulation Draft for the PDPL (RPP PDP) requires that the data controller and data processor to:

- Ensure that the DPO is involved correctly and timely in any matters related to personal data processing activities;
- Ensure that the DPO has reporting access to the highest level of management;
- Ensure that the DPO operates objectively and will not be dismissed or penalised for performing their duties according to the law;
- Provide adequate resources to support the DPO in fulfilling their responsibilities and maintaining their expertise;
- Ensure that the DPO has appropriate access to processing activities;
- Facilitate access to other services to acquire essential information related to personal data processing;
- Obtain advice from the DPO in conducting impact assessments; and
- Document the details and activities of the DPO.

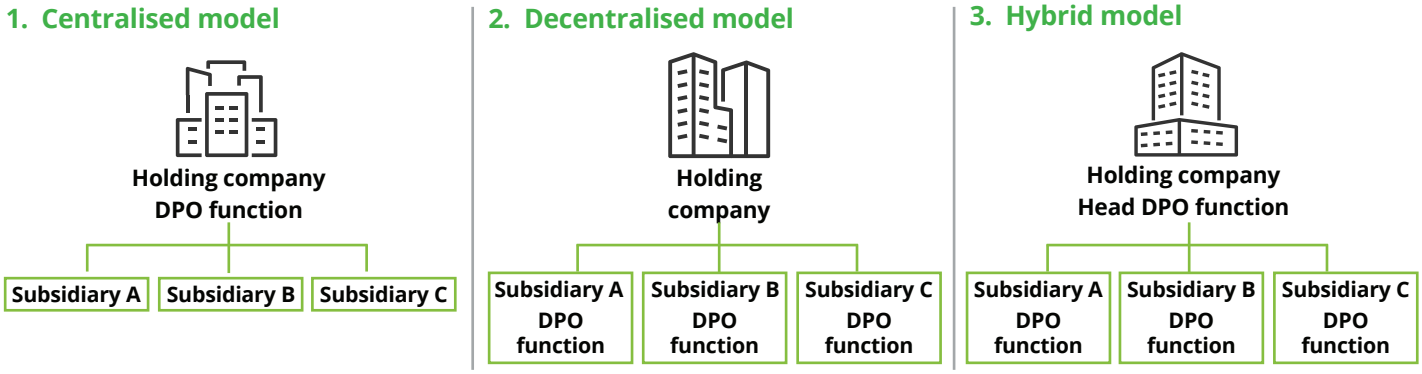
Four DPO function archetypes

There are two main considerations that organisations and their DPOs should take into account when designing and structuring their DPO function. First and foremost, in order to ensure that they can effectively meet evolving compliance requirements, the function must be capable of accommodating the ongoing identification of resource constraints – for example, in terms of expertise, personnel, or technology – and ensuring that active steps are taken to mitigate and overcome these limitations.

Second, to ensure consistency in data protection practices across business units, the function needs to be capable of overseeing the implementation of standardised data protection policies, and maintaining unified data inventories between the DPO function and other functions such as IT, marketing, human resources, and legal. To this end, a universal data processing and management system may be required for the management and storage of all personal data, activity logs, and audit trails, and regular training should also be conducted to ensure that DPOs and the relevant stakeholders are well-informed about the specific data protection requirements of their respective jurisdictions.

Given Deloitte's extensive experience in supprting organisations on their data protection programs, we have developed systematic approaches to help organisations select and implement the right model for their circumstances. Briefly, there are four common archetypes that organisations can choose from, with each presenting its own set of advantages and challenges (see Figure 2).

Figure 2: Four archetypes



1 Centralised model

In a centralised model, a single DPO function holds full responsibility for data protection across the entire organisation, from setting policies and ensuring regulatory compliance, to handling data subjects' requests and conducting privacy impact assessments. This model is particularly effective for organisations with a strong, central governance structure, as it ensures consistency in policies and procedures across all departments and geographies.

2 Decentralised model

A decentralised model distributes multiple DPOs or privacy teams across different business units and/or geographies. This model is most appropriate for organisations that are highly diversified, operate in multiple jurisdictions with varying privacy laws, or those that prefer to give more autonomy to individual units. While this approach offers greater flexibility and enables higher responsiveness to local needs, it may require more effort to ensure consistency and compliance across the entire organisation.

3 Hybrid model

Combining elements of the centralised and decentralised models, a hybrid model comprises a central DPO team collaborating closely with local privacy officers or teams within various business units and/or geographies. This model allows the organisation to achieve a balance between centralised policy oversight and localised implementation that takes into account the specific needs and challenges of different parts of the organisation.

4 DPOaaS

As an alternative to establishing their own in-house DPO function, organisations can also consider outsourcing the function. This practice, known as DPOaaS, offers organisations an actionable and effective way to jumpstart and sustain their data protection programs, bridge the talent gap and other resource constraints, and keep pace with rapidly changing regulations (see sidebar "DPOaaS in Indonesia").

Other considerations for appointing a Data Protection Officer in your organisation

Although Indonesia's PDP regulation is similar to the European Union's GDPR, there are significant differences that may result in varying implementations within Indonesia.

Considerations	Points to consider
Which is preferable to appoint for the DPO role: a legal expert or a technical expert?	Ideally, DPO should possess a balanced combination of both legal and technical expertise. If such a candidate is not available, the organisation can appoint a DPO with strong skills in one area and provide support from other departments (e.g., legal team or IT department) to cover the other aspect. This collaborative approach ensures comprehensive compliance with data protection regulations. The guidance of role and competency for DPO in organisation has been listed briefly in PDPL and Standar Kompetensi Kerja Nasional Indonesia (SKKNI) for Data Protection Officer.
Are there any specific job certifications for DPOs in Indonesia?	Currently, there is no certification issued by Indonesia Government bodies specifically to certify DPOs. However, there are notable certifications that are well recognised under other jurisdictions. 1. Certified Information Privacy Professional/Europe (CIPP/E): Offered by the International Association of Privacy Professionals (IAPP), this certification focuses on European data protection laws and regulations, including GDPR. There is also jurisdictional variation of this certification such as US (CIPP/US), Canada (CIPP/C), and Asia (CIPP/A). 2. Certified Information Privacy Manager (CIPM): Also provided by IAPP, this certification emphasises privacy program management, making it highly relevant for DPOs. 3. Certified Information Privacy Technologis (CIPT): IAPP program that aims provide technical understanding and integrating privacy engineering skills for DPO. 4. ECPC-B DPO Certification: Provided by the European Centre on Privacy and Cybersecurity (ECPC), this certification focuses on the practical skills and knowledge required for a DPO. There are many more certifications offered by various institutions related to Privacy regulation and best practice which can be considered as option.
What is the role of the Data Protection Officer in the third line of defense model?	Given the primary tasks of advisory activities and compliance oversight, placing the DPO in the second line of defense is a best practice. Assigning or perceiving the DPO as responsible for first-line operational activities or as the person solely accountable for the organisation's privacy compliance could create problems, particularly in maintaining independent compliance monitoring. The role of the first line is to implement and effectively integrate privacy requirements into operational activities. This is typically carried out by operations, business, IT, and other related departments. The third line of defense, typically consisting of internal audit functions, helps the DPO comply with privacy regulation by providing independent assurance on the effectiveness of the organisation's data protection measures.
When an organisation assigns an existing function to handle the DPO responsibilities, what factors should be considered?	The EU GDPR envisions that the DPO performs their duties independently. In contrast, Indonesia's PDP regulations do not explicitly mention the independence of the DPO. However, avoiding conflicts of interest in the DPO designation is mandatory, as stated in RPP PDP Article 168 to ensure data protection function can run properly. It is essential to preserve the DPO's autonomy and avoid placing them in roles that could create conflicts of interest. This risk is higher for internal DPOs. Although the DPO can be assigned other tasks, these tasks should not involve determining the purposes and means of data processing, as this would conflict with the responsibilities of the data controller and compromise the DPO's independence. Therefore, companies should carefully consider the regulation concerns for appointing a DPO when assigning the role to an existing function, such as Compliance, Corporate Legal, Risk Management, etc.

DPOaaS in Indonesia

Indonesia's PDPL allows for the outsourcing of the DPO role. Article 53 states that officials or officers carrying out the PDP function may come from within and/or outside the personal data controller or personal data processor. Furthermore, Article 166 of the RPP PDP also states that the DPO may consist of individuals, or groups of individuals, from within and/or outside the personal data controller and/or personal data processor.

While the specific services provided under a DPOaaS arrangement will vary according to an organisation's needs, they usually include the following:

Compliance monitoring and gap assessment

to facilitate regular and thorough assessments such as Data Protection Impact Assessment, Legitimate Interest Impact Assessment, Records of Processing Activities, and Transfer Impact Assessment to achievef the organisation's compliance with data protection regulations and provide detailed recommendations for improvements in critical areas;

Incident response

in the event of a data breach, including providing recommendations for crisis management, such as immediate response strategies to mitigate impacts and prevent future incidents; and

Technology assessment

to evaluate the organisation's technological infrastructure and processes to identify vulnerabilities, prevent cyber threats, and enhance overall IT security;

Training and awareness programs

to cultivate a culture of compliance with data protection laws across the organisation. DPOaaS could also provide the necessary resource and knowledge to enable the organization's effort in developing its own privacy team or DPO.

Embarking on the journey

From an operational perspective, the responsibility for data protection typically falls under the purview of risk management or cybersecurity teams. However, many of the decisions that an organisation must make along this journey are fundamentally strategic in nature and will require the inputs of the board and other C-suite stakeholders. When embarking on this journey, leaders would do well to consider the following strategic decision points:

1 Decide between an in-house DPO function or outsourcing

In weighing the decision to establish an in-house DPO function or outsource in the form of DPOaaS, leaders should assess their organisation's long-term data protection needs and resource availability. While building an in-house team may offer more direct control over the day-to-day operations, engaging a DPOaaS provider can offer greater flexibility and access to a broader range of specialised skills.

2 Evaluate investments in data security technology

To ensure compliance with the PDPL, new investments in data security technology may be required. As they evaluate these investments, leaders will need to ensure that data risk management (especially risks relating to data privacy and protection) is also embedded into their organisation's overarching ERM framework.

3 Embed data risk management into ERM framework

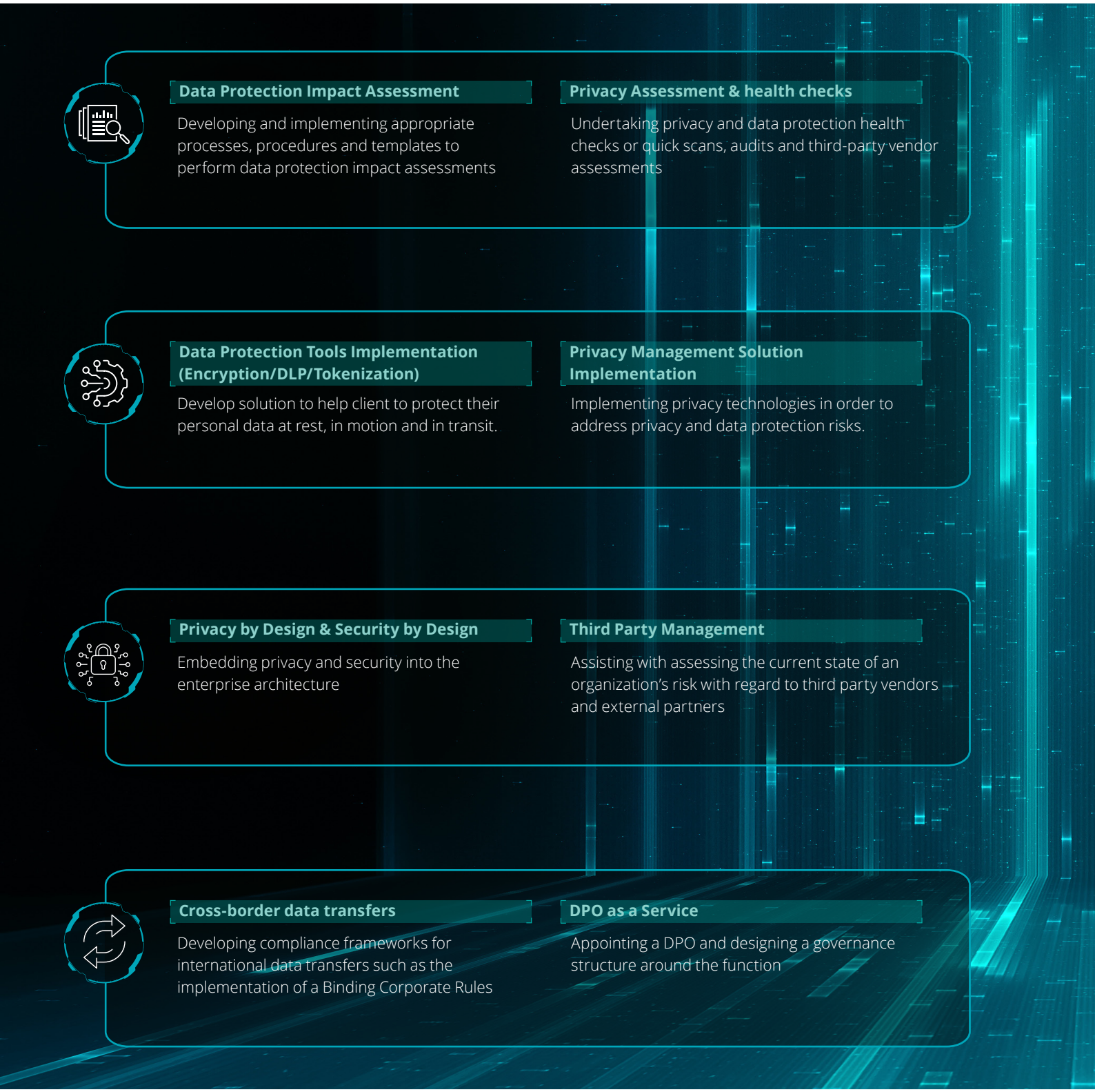
To enable data risks to be managed holistically and in alignment with all other strategic risks within the organisation, leaders will need to ensure that data risk management is also embedded into their organisation's overarching ERM framework.

4 Empower the DPO

For a DPO to perform their role effectively, it is imperative that leaders grant them autonomy through structural empowerment. This could include, for example, providing the DPO with direct access and a clear reporting line to top management to enable them to address data-related issues decisively and independently.

Deloitte Comprehensive Privacy and Protection Solutions

With years of experience assisting Indonesian companies in implementing their Indonesia PDP Law programs across various industries, Deloitte has refined and optimised our privacy service offerings to help organisations comply with the PDP Law.



Data Protection Impact Assessment

Developing and implementing appropriate processes, procedures and templates to perform data protection impact assessments

Privacy Assessment & health checks

Undertaking privacy and data protection health checks or quick scans, audits and third-party vendor assessments

Data Protection Tools Implementation (Encryption/DLP/Tokenization)

Develop solution to help client to protect their personal data at rest, in motion and in transit.

Privacy Management Solution Implementation

Implementing privacy technologies in order to address privacy and data protection risks.

Privacy by Design & Security by Design

Embedding privacy and security into the enterprise architecture

Third Party Management

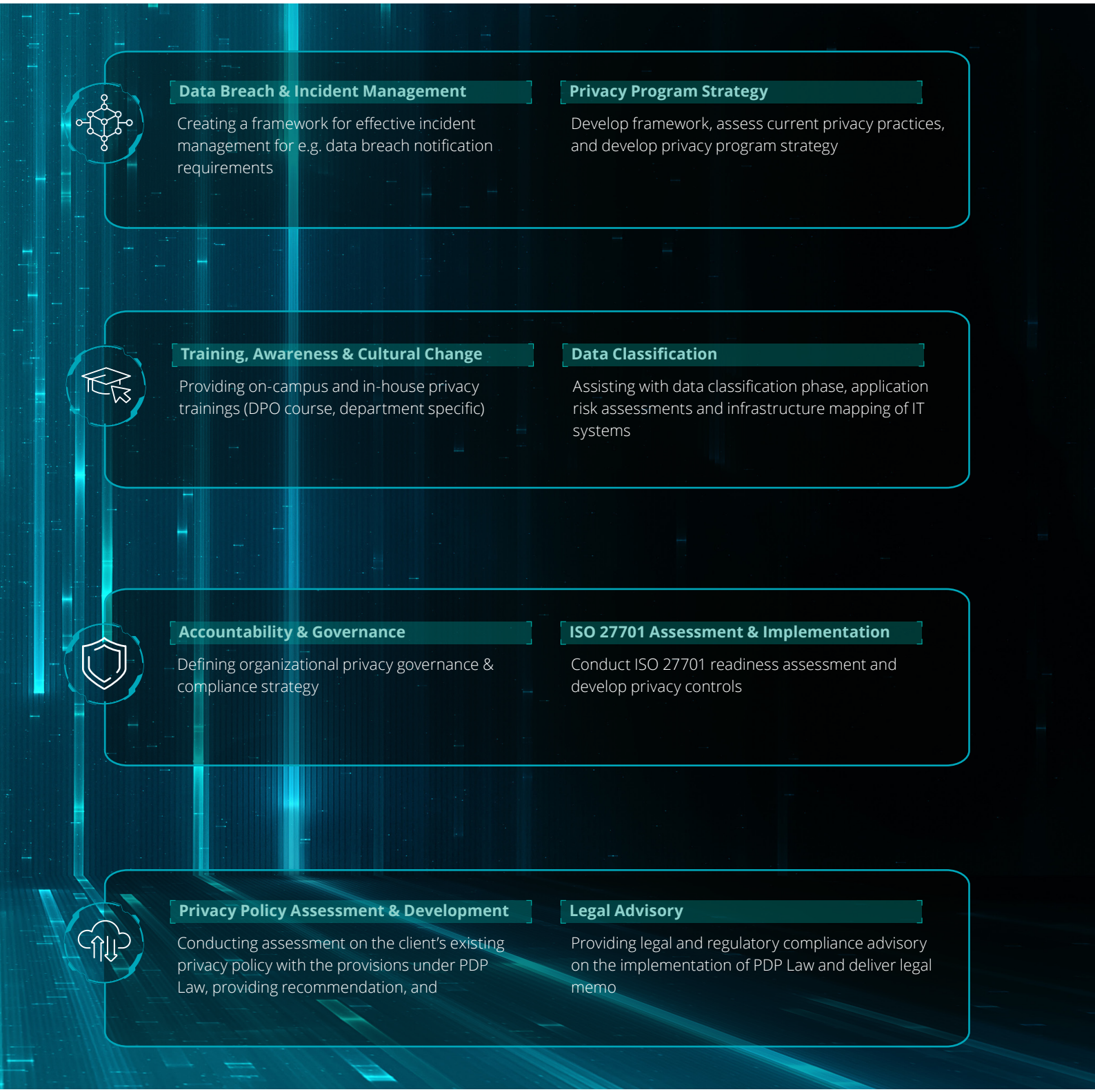
Assisting with assessing the current state of an organization's risk with regard to third party vendors and external partners

Cross-border data transfers

Developing compliance frameworks for international data transfers such as the implementation of a Binding Corporate Rules

DPO as a Service

Appointing a DPO and designing a governance structure around the function



Data Breach & Incident Management

Creating a framework for effective incident management for e.g. data breach notification requirements

Privacy Program Strategy

Develop framework, assess current privacy practices, and develop privacy program strategy

Training, Awareness & Cultural Change

Providing on-campus and in-house privacy trainings (DPO course, department specific)

Data Classification

Assisting with data classification phase, application risk assessments and infrastructure mapping of IT systems

Accountability & Governance

Defining organizational privacy governance & compliance strategy

ISO 27701 Assessment & Implementation

Conduct ISO 27701 readiness assessment and develop privacy controls

Privacy Policy Assessment & Development

Conducting assessment on the client's existing privacy policy with the provisions under PDP Law, providing recommendation, and

Legal Advisory

Providing legal and regulatory compliance advisory on the implementation of PDP Law and deliver legal memo

Contact Us

Alex Cheung
Technology & Transformation Partner
alecheung@deloitte.com

Stefanus Brian Audyanto
Legal Partner
saudyanto@deloittelegal-id.com

Hendro
Technology & Transformation Director
hhendro@deloitte.com

Tammy A. Wenas Kumontoy
Legal Managing Associate
tkumontoy@deloittelegal-id.com"

Adoeardo Soediono
Technology & Transformation Director
asoediono@deloitte.com

Budianto
Technology & Transformation Associate Director
bbudianto@deloitte.com

Priscilia Sinata
Technology & Transformation Associate Director
psinata@deloitte.com

Authors and Editors:
Hendro, Muhammad Deckri Algamar

Deloitte.

Design by Core Creative Services RITM1776222