Deloitte.

Reforming Indonesia's Personal Data Protection Landscape

October 2022

MAKING AN IMPACT THAT MATTERS since 1845

Abbreviation list

API	Application Programming Interface
BI	Bank Indonesia (Central Bank of Indonesia)
BPJS	Badan Penyelenggara Jaminan Sosial (Social Health Insurance Administration Body)
BRI	Bank Rakyat Indonesia
BSSN	Badan Siber dan Sandi Negara
COVID-19	Corona Virus Disease-2019
DBA	Database Administrators
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPM	Data Privacy Management
DPO	Data Protection Officer
DPOaaS	Data Protection Officer-as-a-Service
DPR RI	Dewan Perwakilan Rakyat Republik Indonesia (House of Representatives of Republic of Indonesia)
e-HAC	electronic Health Alert Card
EU	European Union
EUR	Euro
FinTech	Financial Technology
GB	Gigabyte
GDPR	General Data Protection Regulation
GR	Government Regulation (Peraturan Pemerintah – PP)
ICT	Information and Communication Technology
ID	Identification/Identity
IDR	Indonesian Rupiah
IP	Internet Protocol
IT	Information Technology
KK	Kartu Keluarga (Family Card)
Kominfo/MoCI	Kementerian Komunikasi dan Informatika/Ministry of Communication and Informatics
KPU	Komisi Pemilihan Umum (General Election Committee)
KTP	Kartu Tanda Penduduk (National ID Card)
MoCI Reg.	Minister of Communication and Informatics Regulation (Peraturan Menteri Komunikasi dan Informatika – Permen Kominfo)

Abbreviation list

NIK	Nomor Induk Kependudukan (National ID Card Number)
NPWP	Nomor Pokok Wajib Pajak (Tax Acount Number)
OJK	Otoritas Jasa Keuangan (Financial Services Authority)
PDP	Personal Data Protection
PIA	Privacy Impact Assessment
PLN	Perusahaan Listrik Negara (State-owned Electricity Company)
PUJK	Pelaku Usaha Jasa Keuangan (Financial Services Business Actors)
REST	Representational State Transfer
RUU	Rancangan Undang-undang (Bill)
SDK	Software Development Kit
SNAP	Standar Nasional Open API Pembayaran (National Open API Payment Standard)
USD	United States Dollar

Table of Contents

Foreword

The enactment of Personal Data Protection (PDP) Law in Indonesia, passed on 20 September 2022, is welcomed by the public, including industries, that has been in deliberation for quite a long time. The PDP Law will play an important role in digital business processes and is beneficial for digital business players, as well as the general public who are getting used to digital services especially since the pandemic began. Moreover, the number of data breaches that have occurred in Indonesia in recent years has made the PDP Law increasingly urgent to enforce.

Deloitte Indonesia welcomes the passage of the PDP Law in Indonesia. In this respect, the legal team (Hermawan-Juniarto & Partners) and the risk advisory team (PT Deloitte Konsultan Indonesia) initiated a publication discussing the protection of personal data.

The PDP Law is expected to encourage public confidence in carrying out activities through digital services. It is also expected that the PDP Law will improve security systems and encourage the emergence of better, more effective alternatives in approaching data protection.

In this publication, we will discuss several aspects of the importance of data and the approach to its use, including data ownership, key principles in data management, data acquisition and data exchange, as well as cybersecurity compliance.

We will also discuss the important roles of data protection officers to manage technology platforms in accordance with the provisions required by the PDP Law. This discussion aims to ensure that the organisation's implementation of the Data Privacy Management (DPM) can take place in an effective and efficient manner.

This publication is expected to be a starting point and reference in preparing various organisations to implement the PDP Law by conducting comprehensive data management. We hope that you gain insight from this publication and thereby help you prepare your business to become a leading digital business within your industry.

Cornel B. Juniarto
Senior Partner
Hermawan Juniarto & Partners

Alex Siu Hang Cheung
Risk Advisory Partner
PT Deloitte Konsultan Indonesia

Introduction

Buoyed by a market of nearly 211 million Internet users[1], Indonesia possesses the largest and fastest-growing digital economy in Southeast Asia. According to recent estimates, the economic potential of its digital economy has been forecasted to reach USD146 billion by 2025, and thereafter more than double to a whopping USD330 billion in the next five-year period to 2030.[2]

In order to reap the full potential of this growth, however, Indonesia must first address the growing issue of data privacy. In recent years, personal data breaches have become a regular occurrence in the news, with the result that many Indonesian consumers are becoming increasingly wary of sharing their personal data. To foster consumer trust – and thereby encourage greater investment and innovation in the digital economy – Indonesia urgently needs to fortify its personal data protection (PDP) framework.

The good news is that this work is already underway. Developed by the Ministry of Communication and Informatics, Indonesia's long-awaited PDP law draft – referred to as the Personal Data Protection Bill (PDP Bill – RUU Perlindungan Data Pribadi) - was passed into law at the Plenary Meeting of the DPR RI on 20 September 2022. PDP Law will automatically take effect after thirty (30) days following the passing of the Bill.

The PDP Law is expected to replace previous PDP regulations – which are primarily composed of a fragmented patchwork of general and sector-specific laws and regulations – with a single, comprehensive approach to personal data protection, and provide businesses with greater clarity on data ownership rights, data transfer rules, and key data roles, amongst others.

In this report, we will take a look at Indonesia's PDP landscape and approach to PDP regulation. Then, we will examine some of the key aspects of the PDP Law, before discussing several actions that we believe organisations should consider taking as they prepare for compliance with the PDP Law.

[1] "Pengguna Internet di Indonesia Tembus 210 Juta pada 2022". Kompas.com, 10 June 2022.
[2] "Presiden Jokowi: Potensi Ekonomi Digital Indonesia Sangat Prospektif". Cabinet Secretariat of RI. 01 March 2022.

Overview of Indonesia's PDP landscape

The concept of PDP refers to an individual's right to claim, preserve, and control their personal or private information – including but not limited to general personal identification information, IP addresses, as well as biometrics and health records – and for this information to be protected by a set of regulations. Specifically, the individual should be given control over the flow of their data – for example, whom they want to share their information with, for how long, for what purpose, and the extent to which they or other parties are allowed to modify the data.

A series of high-profile personal data breaches

Across the globe, we have witnessed numerous high-profile breaches that have brought to light the devastating implications of data misuse – which can manifest in the form of the accidental or unlawful destruction, loss, alteration, or disclosure of personal data – and the significant impacts of such actions on individuals. Closer to home in Indonesia, we have similarly observed several personal data breaches that have made headlines in recent years (see Figure 1).

Broadly, these breaches can be classified into three main categories[3]:

- Confidentiality breach: Unauthorised disclosure or accidental access of personal data.
- Availability breach: Loss of access or destruction of personal data, often a result of cyber attacks that destroy or prevent access to data records.
- Integrity breach: Unauthorised alteration of personal data.

Figure 1: A Non-Exhaustive List of Recent Personal Data Breaches That Have Made Headlines in Indonesia[4,5]

Year	Month	Occurance
2020	**February**	Hacking of a journalist's bank account, as a result of a personal telephone data breach at a telecommunications service provider
	March	Data breach involving 91 million users at Tokopedia
	May	Data breach involving the personal information of 2.3 million citizens at the General Election Committee (KPU)
	November	Data leak of 2.9 million users at Cermati and Lazada
2021	**May**	Data leak involving 279 million users at BPJS Kesehatan, with personal information sold online
	July	Data leak involving more than 400,000 customers at BRI Life, with personal information such as electronic ID, account numbers, birth certificates, and medical records sold on the dark web
	August	Data leak involving 1.3 million users of the Indonesia Health Alert Card (eHac) system, the national COVID-19 travel health declaration platform
	September	Data leak involving Ministry of Health data from the PeduliLindungi platform, the national COVID-19 contact tracing mobile application, with personal information sold to a raid forum

[3] "GDPR: Reporting Data Breaches". The Medical Defence Union.
[4] "6 Kasus Kebocoran Data Pribadi di Indonesia". Tempo.co.id. 03 September 2021.
[5] "Pembobolan Rekening Ilham Bintang, Libatkan Karyawan Bank hingga Pembuatan KTP Palsu". Kompas.com. 06 February 2020.

Year	Month	Occurance
2021	**October**	Hacking of a National Malware Centre Site of the State Cyber and Cipher Agency (BSSN)
	November	Data leak involving 28,000 documents of the Indonesian National Police information, such as ID number, graduation certificate, family card (KK), and birth certificate
2022	**January**	• Ransomware attack involving 228 GB of stolen data from 513 computers of Bank Indonesia (BI) • Data breach involving the personal information of 160,000 job applicants at Pertamina
	August	• Data leak involving 347 GB of crucial documents from 21,000 Indonesian and international companies, with personal information such as electronic ID (KTP), tax account number (NPWP), family card (KK), account numbers, and financial statements sold on the dark web • Data leak involving 17 million users at State-owned Electricity Company (PLN), with personal data sold online • Data leak involving 26 million users at the IndiHome Telkom with personal information such as passwords, domain, platform, browser history, IP, geographic location, email, and national ID card number (NIK) sold on a hacker forum • Data leak involving 252 GB of users' data at Jasa Marga, with personal information such as customers and employee's information, company information, and financial statement sold on a hacker forum
	September	• Data breach involving the personal information of 105 million citizens at the General Election Committee (KPU) • Data leak involving 247 million of medical record information from BPJS Kesehatan, with personal information sold online • Data leak involving 1.3 billion data at the Ministry of Communication and Informatics (Kominfo), with SIM card registration information sold on a hacker forum

PDP regulatory landscape

Globally, the European Union's (EU) General Data Protection Regulation (GDPR) is considered the gold standard for PDP regulation. Enacted in 2018, it is currently the world's more stringent privacy and security law, as it imposes obligations on any organisation that targets or collects data from users in the EU, regardless of where the organisation is located.

In 2022 alone, the EU's Data Protection Authorities (DPAs) – which are independent public authorities supervising the application of the data protection law – received over 1,300 reports of PDP violations across the EU and issued hundreds of fines to perpetrators[6]. In one prominent case, a clothing retailer was fined EUR35.3 million for collecting and using the personal data of its employees without their consent[7].

In contrast to this coherent approach employed in the EU, Indonesia's PDP regulatory landscape remains relatively more fragmented prior to the enactment of PDP Law, considering at that time, there are no PDP-specific laws and regulations; instead, PDP aspects tend to be covered in more sector-specific legislation. These include, for instance, Law No. 11 of 2008 on Electronic Information and Transaction as amended by Law No. 19 of 2016; Government Regulation No. 71 of 2019 on Administration of Electronic Transaction and System (GR 71/2019); Minister of Communication and Informatics Regulation No. 5 of 2020 on Private Electronic System Providers; and Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection on Electronics System (MoCI Reg. 20/2016).

[6] "GDPR Enforcement Tracker". CMS.Law.
[7] "3 Years Later: An Analysis of GDPR Enforcement". CSIS. 13 September 2021.

Most notably, MoCI Reg. 20/2016 requires the data collection process to observe the following rules:

- The electronic system operator must obtain the approval of the data owner; and
- The personal data obtained and collected by the electronic system operator must be directly verified with the owner of the data. If obtained and collected indirectly, the personal data must be verified with other data processing sources.

In recent years, several sectoral institutions have also issued updates to their respective regulations relating to PDP. For example, the financial services authority – Otoritas Jasa Keuangan (OJK), and the central bank – Bank Indonesia (BI) – recently enacted a number of regulations to protect personal data in the financial services sector (see Figure 2). These regulations are a recognition of the PDP challenges posed by the use of technology in the sector, particularly with the rise of FinTech and acceleration of digital transformation.

Figure 2: PDP regulation enacted in the financial services sector

Regulation	Details
OJK Regulation No. 6/POJK.07/2022 on Consumer and People Protection in the Financial Services Sector	The regulation stipulates several provisions to strengthen the protection of assets, privacy, and consumer data. It includes the establishment of several prohibitions and/or limitations for Financial Services Business Actors (PUJK) relating to the processing of personal information of both individual and corporate customers.
OJK Regulation No. 11/POJK.03/2022 on Implementation of Information Technology by Commercial Banks	The regulation stipulates provisions covering all aspects of the IT implementation process at commercial banks relating to data processing and PDP, including the classification of data constituting personal data; rights and obligations of the parties involved in the exchange of personal data; personal data exchange agreement; means of exchanging personal data; and personal data security.
Decree of the Governor of Bank Indonesia No.23/10/KEP. GBI/2021 dated 16 August 2021 on Stipulation of Payment Open Application Programming Interface (API) Standards	The decree covers technical and security standards; data standards and technical specifications; and PDP relating to the processing of data in the pre-transaction, initiation, or authorisation phases within the context of services rendered under BI's National Open API Payment Standard (SNAP).

Key aspects of the PDP Law

Recognising the need for a unified and singular approach to PDP, the Government has finalized and enacted the PDP Law on 20 September 2022, which aims to guarantee the data protection rights of every individual.

Briefly, the PDP Law – which references the provisions set out under the EU's GDPR – applies to every person, public entity, organisation, or institution carrying out a defined set of actions both within and outside the jurisdiction of the Republic of Indonesia. Looking ahead, this legislation is expected to increase the competitiveness of Indonesia's information and communication technology (ICT) sector, and encourage the overall growth of the digital economy.

In this section, we will examine some of the key aspects covered under the PDP Law.

1. General overview

The PDP Law defines personal data as any electronic and/ or non-electronic data that may directly or indirectly identify a person – whether in isolation, or in combination with other information. Personal data falls into two categories:

- General: A person's full name; gender; nationality; religion; marital status ; and/or other personal data that may identify a person
- Specific: A person's health data and information; biometric data; genetics data; Criminal record; children's data; personal financial data; and/ or Other data in accordance to the laws and regulations.

A data subject is defined as any individual with associated personal data. The PDP Law grants data subject 9 rights, including but not limited to the (i) rights to be informed; (ii) right to rectification; (iii) right of access; (iv) right to erasure; (v) right to withdraw; (vi) right to avoid automated decision-making; (vii) right to restrict processing; (viii) right to object; (ix) right to data portability.

In this context, personal data processing covers the following actions relating to data: acquisition and collection; processing and analysis; storage; corrections and updates; appearance, announcement, transfer, dissemination, or disclosure; and removal or destruction.

2. Key principles of data governance

The PDP Law sets out several key principles of data governance as follows:

a. Data processing principles

Firstly, collection of personal data should be limited, specific, legally valid, appropriate, and transparent. Secondly, personal data processes should guarantee the rights of the data subject, and be accurate, complete, current, accountable, clearly proven, and fit for purpose. Finally, personal data should be destroyed and/or deleted after the retention period ends, or at the request of the data subject.

b. Definition of key roles in data processing

The data controller is the party that determines the objectives and controls the processing of personal data; the data processor is the party that processes personal data on behalf of the personal data controller; and the data subject is the individual or data subject with the associated personal data.

c. Explicit consent

Explicit written or recorded verbal consent must be obtained from the data subject for the processing of data for any purpose. An explicit consent clause must also be included in any agreement relating to the processing of personal data, or the agreement will be deemed null and void.

d. Visual data processing

An installation for the purposes of visual data processing may be made in public places and/or facilities for the purposes of security, disaster prevention, and traffic management. However, the installation must inform users that the visual data processing or processing device has been installed in the area and cannot be used to identify any individuals with the exception in the prevention of criminal acts and law enforcement processes in accordance with the prevailing laws and regulations.

e. Response periods

The relevant response periods that data controllers are to account for are as follows: three days for rights to access; three days for withdrawal of consent; two days for processing restrictions; and one day for data repair or correction.

f. Data breach notification

In the event of personal data breach, the data controller must notify the data subject and the MoCI within three days and issue a public notice if there is an impact on public interest.

While the PDP Law does not impose penalties on personal data breaches, data controllers will be held accountable for their personal data processing and must demonstrate their commitment towards the implementation of the personal data protection principles. This means that data controllers must compensate data subject who have been harmed by a personal data breach.

g. Data retention

Data processors may only hold onto personal data for a stipulated period of time. Following that, the data must be deleted unless otherwise required by law or requested by the respective data subject. The PDP Law does not specify a fixed retention period; however, Article 15 of the MoCI Reg. 20/2016 states the retention period of stored personal data as a minimum of five years unless stipulated otherwise.

h. Data storage

Data, records, and/or statements received by a corporation in carrying out its activities (including contracts), whether in written or other forms of media that can be seen, read, or heard, are classified as corporate documents, and regulated under the Corporate Documents Law.

Certain types of corporate documents – for example, supporting documents (e.g., contracts) used for the bookkeeping process – must be stored for a period of 10 years from the end of a financial year. If these documents are destroyed before this period is over, all risks arising from the destruction of the relevant documents shall be borne by the company.

The data storage period of 10 years is also clearly stipulated in Taxation Law, which applies to all records and documents that form the basis for bookkeeping, including the results of any data processing that is conducted electronically or online.

3. Data acquisition and data exchange

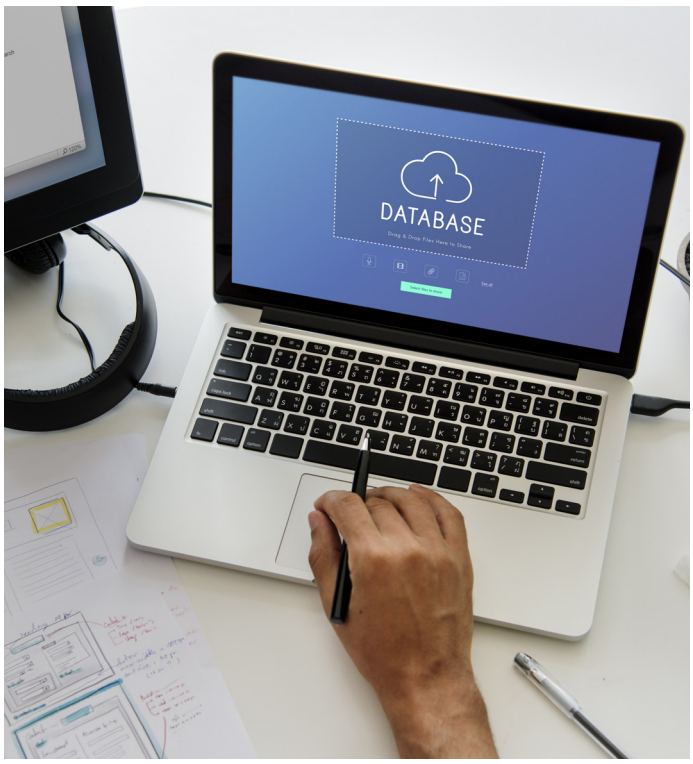
Under the Indonesian PDP laws and regulations prior to the enactment of PDP Law – in particular, the MoCI Reg. 20/2016 – any personal data that is managed by a data processor may be transferred outside of the jurisdiction of the Republic of Indonesia if they fulfil the following requirements:

a. Coordination of the data transfer process with MoCI, which includes:

   i. Submitting a report on the implementation plan for the personal data transfer, including details such as the receiving country, recipient's identity, date of implementation, and purpose of transfer;
   ii. Requesting advocacy (if necessary); and
   iii. Submitting a report on the transfer implementation.

b. Implementation of all applicable provisions governing cross-border data transfers under Indonesian laws and regulations.

In practice, the consent for any border transfer should be included in the initial consent agreement between the data processer and data subject. Therefore, once consent has been obtained from the data subject, the data processor may carry out a cross-border data transfer, either to the processors' affiliates or a third-party data processor in other jurisdictions. Nevertheless, compliance to the requirements as stipulated by MoCI Reg. 20/2016 remains low. This can be attributed at least in part to the lack of coordination between MoCI and data processors, as well as inadequate sanctions for non-compliance.



This, however, looks set to change with the PDP Law. Under the new PDP Law, data controllers must obtain explicit consent from the data subject before transferring personal data to any other data controller located within or outside the jurisdiction of the Republic of Indonesia, in accordance with the following criteria:

a. The quality of PDP regulations in the receiving jurisdiction must be equal or higher than the PDP Law;
b. There is an international agreement between the jurisdictions;
c. There is a contract between the data controllers with PDP standards and/or guarantees in accordance with the PDP Law;
d. Explicit consent has been obtained from the data subject.

Furthermore, the PDP Law also spells out several possible administrative sanctions in the event of failure the above-mentioned criteria for cross-border data transfer. These include:

a. Written warnings;
b. Temporary suspension of personal data processing activities;
c. Deletion or destruction of personal data;
d. Indemnification of losses; and/or
e. Administrative fines.

It is therefore advisable that data subject take measures to safeguard their PDP rights with the appropriate and adequate personal data processing agreements. This is to avoid any potential pitfalls, particularly with regards to the necessary pre-requisite approval for a cross-border data transfer.

4. Cybersecurity compliance

Prior to the enactment of PDP Law, administrative sanctions could potentially be imposed on Electronic Service Providers who fail to comply with PDP provisions relating to the processing of personal data. However, they do not include criminal sanctions for the violations of any provisions or prohibitions.

With the PDP Law, however, new provisions are included to allow criminal sanctions – either imprisonment or fines – to be imposed on any individual failing to comply with the relevant provisions. These include:

a. Intentionally and unlawfully obtains or collects personal data that does not belong to him with the intention of benefiting himself or another person which may result in loss of the data subject;
b. Intentionally and unlawfully discloses personal data that does not belong to him;
c. Intentionally and unlawfully uses personal data that does not belong to him; and /or
d. Intentionally creates false personal data or falsifies personal data with the intention of benefiting himself or another person which may result in harm to others.

The criminal sanctions for individuals range from a fine of between IDR4 billion and IDR6 billion, and/or imprisonment for 4 to 6 years. For companies, the penalty is ten times the maximum fine imposed on individuals. Additional sanctions may also include the confiscation of profits and/or assets; freezing of all or a portion of the corporation's business; permanent prohibition of certain actions; closure of all or part of a business place and/or activity; performing the previously neglected obligation; payment of compensation; revocation of license; and/or corporate dissolution.

Preparing for compliance with the PDP Law

Upon enactment of the PDP Law, organisations will be given a two-year period to comply with all relevant personal data processing provisions. During this period, they will need to carry out the following set of key actions:

a. Prepare a personal data processing framework to serve as a guideline for compliance with the provisions of the PDP Law;
b. Conduct a review of all activities carried out within the organisation in relation to personal data processing;
c. Conduct a review of existing personal data processing and protection policies to ensure compliance with the provisions of the PDP Law;
d. Conduct a review of all existing contracts and obtained consents in relation to personal data processing;
e. Assess and review the gaps between existing personal data processing and protection policies, and the provisions of the PDP Law; and
f. Develop a data retention strategy.

In addition, organisations should also consider appointing a data protection officer (DPO) – either on fixed short-term contracts, or in the form of DPO-as-a-Service (DPOaaS) – and implementing a privacy management technology platform:

1. Appointing a DPO

The EU introduced the role of the DPO in 2018 to oversee personal data processing activities within organisations. In a similar vein, the PDP Law is also expected to specify the role of the DPO in risk mitigation, particularly in the context of the following:

a. Processing of personal data for public services or public interest;
b. Large-scale coordination and systematic supervision of personal data; and
c. Large-scale processing of personal data for specific personal data and/or personal data relating to criminal records.

In addition, administrative sanctions may be imposed for the failure to appoint a DPO in the above-mentioned contexts. These may take the form of:

a. Written warnings;
b. Temporary suspension of personal data processing activities;
c. Deletion or destruction of personal data;
d. Indemnification of losses; and/or
e. Administrative fines.

2. Roles and responsibilities of the DPO

Under MoCI Reg. 20/2016, electronic service providers are required to designate a contact person to support data owners with the management of their personal data. There are, however, no specific stipulated provisions on the role of this contact person, and no explicit recognition of the role of the DPO.

In contrast, the PDP Law mandate the following responsibilities for the DPO regarding data protection:

a. Inform and advise the data controller or processor on specific provisions under previous PDP laws and regulations;
b. Supervise and ensure compliance with PDP laws and regulation, as well as data controller or processor policies, including assignment, responsibility, awareness, and training activities for parties involved in personal data processing and the relevant audits;
c. Advise on PDP-related impacts, and supervise the performance of the data controller and processor; and
d. Coordinate issues relating to personal data processing, including consultations regarding risk mitigation and/or other matters.

3. Skills and competencies of the DPO

The data controller and data processer are to appoint a DPO based on the candidate's professional qualifications, knowledge of PDP Law and practices, and ability to carry out their duties relating to the protection of personal data.

4. Alignment of DPO roles with other functions

The PDP Law does not set out specific provisions to regulate the role of the DPO, although these are expected to be defined in subsequent implementing regulations. In the EU, however, we have observed that the DPO is expected to play important and central roles within their organisations, with the following independence guarantees:

a. The DPO does not receive instructions regarding the performance of their duties;
b. There must not be any conflict of interest between an individual's duty as a DPO and their other duties, if any. It is further recommended that the DPO:

   i. Should not be a data controller in personal data processing activities;
   ii. Should not be an employee, that is, they should be on fixed short-term contracts;
   iii. Should not report to a direct supervisor, and instead report directly to management; and
   iv. Be responsible for managing their own budget.

c. The organisation should provide the necessary resources to support the DPO in carrying out their duties;
d. The DPO should be given access and the authority to investigate all personal data and data processing operations; and
e. The organisation should establish a minimum term of appointment and strict conditions for dismissal for a DPO appointment.

5. DPOaaS

Depending on an organisation's compliance obligations, the use of DPOaaS services could be one possible option for them to tap into outsourced data privacy expertise. Examples of services provided by DPOaaS service providers include information-as-a-service; training and awareness campaigns; risk monitoring and mitigation; as well as response to data breaches.

Implementing a Data Privacy Management technology platform

In order to efficiently manage all governance, management, and operational aspects relating to PDP regulatory compliance, organisations should consider the implementation of a comprehensive, integrated Data Privacy Management (DPM) solution. Briefly, this solution should meet the following functional and technical requirements:

- The solution should address all relevant PDP requirements, and be customised to the organisation's needs;
- The solution should be integrated in and of itself, and with the organisation's other applications where applicable; and
- The solution should accommodate the processes and metadata of the organisation's PDP program and be capable of evolving in tandem with future regulatory developments.

At most organisations today, DPM at best comprises a series of manual processes – for example, interviews conducted by internal auditors with database administrators (DBAs) or data owners on the type of data that is contained within a data archive, how it is processed, and what it may be used for. Such processes can conceivably lead to a variety of issues, including but not limited to:

- Siloed point products that solve only a small set of privacy requirements, and fragmented solutions where an organisation might rely on middleware to tie everything together;
- Custom middleware that is not scalable, resulting in complex systems that are prone to failure as the individual point products change in behaviour due to patches or upgrades;
- A lack of automation leading to slow turnaround and overreliance on manual, human processes which are error-prone; and
- Inability to keep up with increasing complexity of data privacy regulations.

As a case in point, many organisations that have previously attempted to automate the buildout of data inventories with the support of data loss prevention, data classification, or data discovery utilities are beginning to realise that while these tools are perfectly capable of identifying categories of personal data, they often lack the concept of a personal identity – and are therefore unable to connect all data fragments back to a single individual. This, in turn, results in operational efficiencies – for example, when a consumer exercises their right to a data subject access request. To overcome these issues, an integrated DPM solution should therefore be capable of performing the following functions:

- **Data discovery and mapping:** The DPM solution should be able to collect and record data into a single data repository, the DPM solution should enable an organisation to discover, manage, and protect its data across both on-premises and cloud platforms. It should also be able to identify sensitive data attributes, classify unstructured data, highlight the data risk of each dataset with a risk score, and automate security and privacy functions.

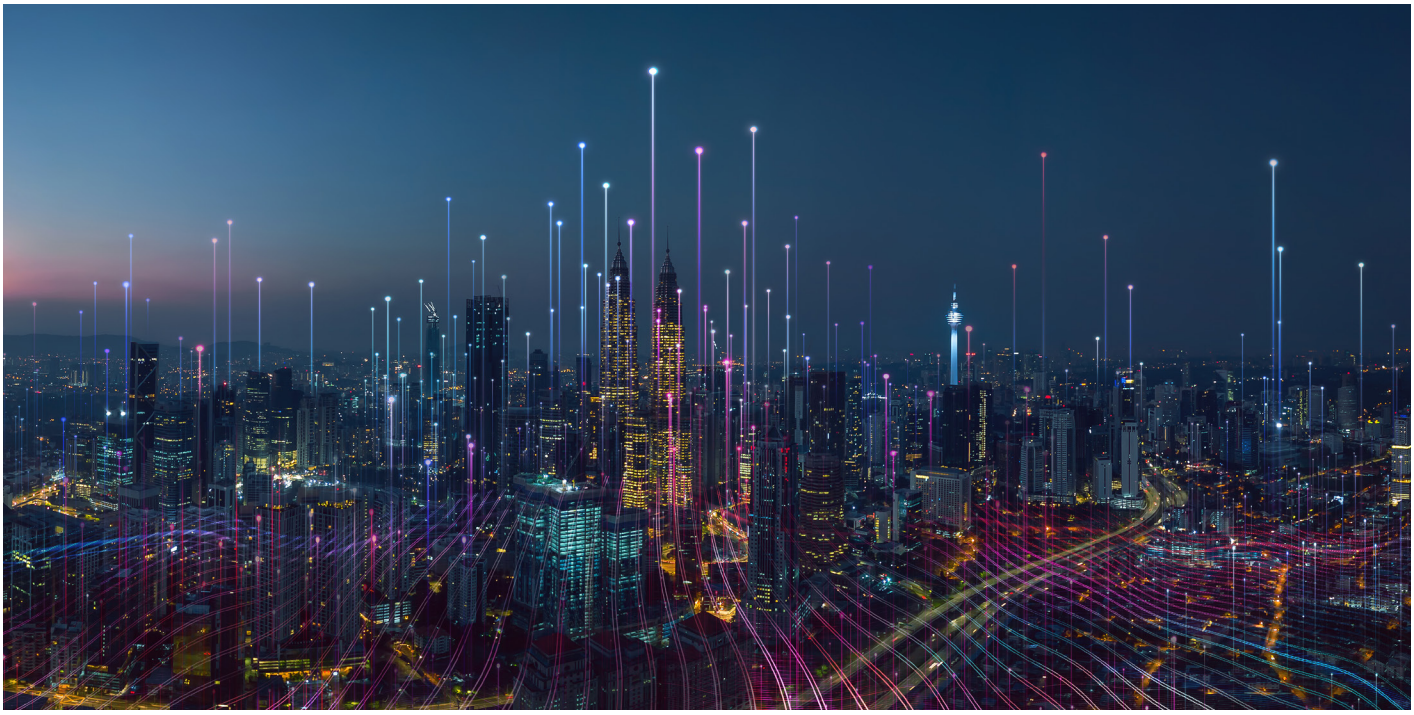
- **Assessment Automation:** The DPM solution should be capable of tracking and managing hundreds of assessments such as Privacy Impact Assessment (PIA), Data Protection Impact Assessment (DPIA), data breach assessment across various products or system. It should be able to map privacy risks into relevant personal data processing activities, track risks, and inform stakeholders to remediate the risks.

- **Consent and preference management:** The DPM solution should be integrated with the organisation's existing personal data collection points in order to seamlessly manage the entire consent lifecycle from collection to withdrawal. This can be achieved by leveraging the use of software development kits (SDKs), representational state transfer (REST) APIs, or bulk data feed imports to record and store consent centrally within the solution – and then integrating them into the organisation's existing consent collection workflows.

  Such a process, in turn, not only enables users to manage their preferences, but also provides an audit trail with the pertinent consent-related information – including who gave consent, when they consented, what they were notified of when they consented, and how they consent – to enable the organisation demonstrate accountability with regulators.

- **Incident and breach management:** The DPM solution should be capable of managing incidents centrally, automating tasks, and keeping records for the purposes of compliance or notification. With context-aware, automated workflows, the incident and breach management feature also enable organisations to react accordingly to incidents by taking into account any applicable laws or specific use cases relevant to the context in question – and thereby meet a diverse set of breach notification requirements and accompanying timelines with flexible reporting and incident response audit trails. By assigning risk owners, setting deadlines and automating reminders, as well as tracking and prioritising mitigation efforts, the DPM solution should also help to elevate overall levels of accountability.

- **Risk Management for vendors/third parties:** The DPM solution should be capable of supporting the vendor due diligence process during the initial vendor onboarding phase, as well as the audit of existing vendors according to a risk-based schedule. Through the platform, vendor privacy and security assessment questions can be sent directly to the vendor or other third parties. This, in turn, generates a central record of all vendors, contracts, data transfers, as well as the legal basis for cross-border data transfers and the accompanying security obligations.



For more information, please contact:

Hermawan Juniarto & Partners

Cornel B. Juniarto
Senior Partner
cbjuniarto@hjplaw-deloitte.com

Stefanus Brian Audyanto
Partner
saudyanto@hjplaw-deloitte.com

Maulana Syarif
Senior Managing Associate
msyarif@hjplaw-deloitte.com

PT Deloitte Konsultan Indonesia

Alex Siu Hang Cheung
Partner
alecheung@deloitte.com

Hendro
Director
hhendro@deloitte.com

Eryk Budi Pratama
Associate Director
epratama@deloitte.com

Authors:
Cornel B. Juniarto, Stefanus Brian Audyanto, Maulana Syarif, Hardy Salim, Richard Ticoalu, Hendro, Eryk Budi Pratama, Eleonora Bergita, Agung Basawantara

Editors:
Alex Siu Hang Cheung, Steffi Goh, Monica Aditya

Contact Us

Claudia Lauw Lie Hoeng
CEO
clauw@deloitte.com

Business Leader

Elisabeth Imelda
Audit Leader
eimelda@deloitte.com

Rosita Uli Sinaga
Assurance Advisory Leader
rsinaga@deloitte.com

Edy Wirawan
Financial Advisory Leader
ewirawan@deloitte.com

Brian Indradjaja
Risk Advisory Leader
bindradjaja@deloitte.com

Melisa Himawan
Tax & Legal Leader
mehimawan@deloitte.com

Iwan Atmawidjaja
Consulting Leader
iatmawidjaja@deloitte.com

Services Desk Leaders

Dennis Li Yu Ying
Chinese Services Desk
yuyli@deloitte.com

Tenly Widjaja
Japanese Services Desk
twidjaja@deloitte.com

Bang Chi Young
Korean Services Desk
bangchiyoung@deloitte.com

Roy Sidharta Tedja
Deloitte Private Desk
roytedja@deloitte.com

Rosita Uli Sinaga
State Own Enterprise Desk
rsinaga@deloitte.com

Mark Woodley
US & European Desk
marwoodley@deloitte.com

Client and Industry Leaders

Brian Indradjaja
Technology, Media & Telecom Industry Leader
bindradjaja@deloitte.com

Steve Aditya
Life Sciences & Health Care Industry Leader
staditya@deloitte.com

Rosita Uli Sinaga
Financial Services Industry Leader
rsinaga@deloitte.com

Cindy Sukiman
Energy, Resources and Industrial Industry Leader
csukiman@deloitte.com

Henry Asril Arnoldi
Consumer Industry Leader
hasril@deloitte.com

Irawati Hermawan
Government & Public Services Industry Leader
irahermawan@hjp-deloitte.com

Deloitte.