Grant Thornton

Personal Data in Indonesia: Data Subject Perspective

July 2024

Personal Data in Indonesia: Data Subject Perspective

Personal data is an important asset for individuals and organizations that must be protected. In this digital era, personal data often becomes an easy target for irresponsible individuals and organizations. Therefore, it is essential for people to understand what personal data is, the rules governing personal data in Indonesia, and the risks of deviations from established rules, standards, or norms regarding the handling of personal data.

According to Personal Data Protection (PDP) Act No. 27 of 2022, as the primary regulation on personal data protection, personal data is defined as any information about an individual that can be identified directly or indirectly from that data, either alone or in combination with other data.

Data categories under this Act are divided into two categories, General Personal Data and Sensitive Personal Data. General Personal Data includes non-sensitive information such as names, addresses, dates of birth, and telephone numbers. Sensitive Personal Data requires additional protection and includes information such as health data, biometric data, genetic data, and financial data.

Nowadays, many misuses of personal data can be found, for example:

1. Stolen health data can be used to file fraudulent insurance claims, leading to insurance fraud, either by fabricating non-existent medical treatments or by inflating the cost of actual treatments. Such incidents result in increased insurance premiums for everyone.
2. Stolen biometric data such as fingerprints or facial recognition data, can lead to identity theft. This stolen data can be used to impersonate someone, gaining unauthorized access to secure systems, buildings, or devices.
3. A common misuse of genetic data is discrimination against potential or current employees based on their genetic predisposition to certain illnesses or conditions. This unfairly influences hiring, promotion, or termination decisions.
4. Misuse of financial data continues to occur, such as in the case of ATM card data skimming. In this scenario, the perpetrators copy customer ATM card data and information, allowing them to withdraw funds from accounts at other locations.

The above cases often violate personal data protection and can be subject to civil and criminal sanctions. However, it is important to note that while criminal sanctions under the PDP Act have been effective since 2022, civil sanctions will come into force once the PDP Supervisory Agency is established, which is anticipated to be in mid-2024.

The types of sanctions according to the PDP Act include:

1. Criminal Sanctions:

The PDP Act stipulates various criminal sanctions for violators, including fines and imprisonment. These sanctions are designed to deter illegal activities and ensure that Indonesians' personal data are adequately protected.

a. Criminal sanctions involving imprisonment

- Article 67
  Any person who intentionally and unlawfully obtains or collects personal data that does not belong to them by any means, resulting in harm to the data subject, shall be punished with imprisonment of up to 5 (five) years.
- Article 68
  Any person with deliberate intent and unlawfully discloses personal data that does not belong to them, resulting in harm to the data subject, shall be punished by a maximum imprisonment of 5 (five) years.
- Article 69
  Any person who intentionally and unlawfully uses personal data which does not belong to them to obtain the benefit for themselves or another person, resulting in harm to the data subject, shall be punished by a maximum imprisonment of 7 (seven) years.

b. Criminal sanctions involving fines

- Article 67
  Violations specified in this article may also be subject to a maximum fine of Rp 5 billion.
- Article 68
  Violations specified in this article may also be subject to a maximum fine of Rp 5 billion.
- Article 69
  Violations specified in this article may also be subject to a maximum fine of Rp 7 billion.

2. Civil Sanctions:

The following articles address the civil sanctions related to compensation that a vialator must pay the data subject:

- Article 51
  Every data subject shall have the right to bring a civil action in court against the personal data controller and/or the personal data processor in the event of a violation of personal data protection resulting in harm to the data subject.
- Article 52
  A personal data controller and/or personal data processor who violates the provisions on personal data protection and causes damages or loss to a data subject shall be obligated to provide compensation corresponding to the damage suffered by the data subject.

3. Administrative Sanctions:

The authorities will impose administrative sanctions to ensure that individuals and organizations who violate the provisions are held accountable and comply with applicable rules immediately. As stated in Chapter VII, the administrative sanctions include:

a. Written warning
b. Temporary suspension of personal data processing activities
c. Deletion or destruction of personal data
d. Administrative fine

Moreover, the agency will give administrative sanctions as fines at a maximum of 2 (two) per cent of the organization's annual revenue.

As a data subject, people must be fully aware of these incidents. Therefore, the way people can keep their data secured is by using:

Strong passwords
Make sure to use a solid and unique password for each account. Do not use passwords that are easy to guess, such as date of birth or name.

Two-Factor authentication (2FA)
Users should activate two-factor authentication (2FA) for an extra layer of security to their accounts. This involves requiring a second form of verification, such as an authentication app, hard token or SMS, in addition to their password.

Regularly update application/software
Users should keep their software and applications up to date to avoid security vulnerabilities that could be exploited by irresponsible or unauthorized parties.

Exercise caution
Users should protect their personal information from careless sharing on social media, messaging, applications, platforms, or websites. They should share only what is necessary, the less the better. Users should take advantage of several techniques to protect their personal data, such as colouring, masking, or blurring.

Being mindful of public Wi-Fi
Users should exercise caution when using public Wi-Fi and refrain from accessing sensitive accounts such as banking, financial, and e-commerce accounts over these networks. Using a VPN is recommended where necessary.

Ultimately, personal data is one of the most valuable and vulnerable assets in this digital era. Protecting personal data is about keeping information from irresponsible hands and maintaining one's identity, privacy, and security as well as that of those closest to them. Understanding the importance of personal data and implementing the proper preventive measures will reduce the risk of misuse or a breach and ensure that one's privacy rights are well protected. It is imperative to stay vigilant and always handle personal data with extra care.

Written by:
Kaifa Raihana Fatah
Associate IT Consultant

Reference:
Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi
GDPR: https://gdpr-info.eu/issues/personal-data/

grantthornton.co.id