PERSONAL DATA PROTECTION

Presented by:

SSEK Law Firm

AGENDA

- **Legal Basis on Personal Data Protection**
- **Material to be discussed**

- ✓ Types of Personal Data
- ✓ Personal Data Processing and Principles
- ✓ Lawful Basis of Personal Data Processing
- ✓ Consent-based Personal Data Processing
- ✓ Third Party Data Sharing
- ✓ Subjects of Personal Data Protection
- ✓ Rights of Data Subject
- ✓ Obligations of Data Controller and Data Processor
- ✓ Data Protection Impact Assessment
- ✓ Data Protection Officer
- ✓ Cross-Border Data Transfer
- ✓ Corporate Actions
- ✓ Failure of Personal Data Protection
- ✓ Other Notable Provisions
- ✓ Sanctions

LEGAL BASIS ON PERSONAL DATA PROTECTION

- Law No. 27 of 2022 on Personal Data Protection ("**PDP Law**");
- Law No. 11 of 2008 regarding Electronic Information and Transaction as amended by Law No. 19 of 2016 ("**EIT Law**");
- Government Regulation ("**GR**") No. 71 of 2019 regarding Organization of Electronic System and Transaction ("**GR 71/2019**");
- Minister of Communication and Information ("**MOCI**") Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic System ("**MOCI Reg. 20/2016**");
- MOCI Regulation No. 5 of 2020 regarding Organizer of Electronic System on Private Matters as amended by MOCI Regulation No. 10 of 2021 ("**MOCI Reg. 5/2020**").

LEGAL BASIS FOR SECTOR-SPECIFIC PERSONAL DATA PROTECTION

- **Law Number 36 of 1999 on Telecommunications (September 8, 1999) as lastly amended by Government Regulation in Lieu of Law Number 2 of 2022 on Job Creation (December 30, 2022)** which prohibits the tapping of information transmitted through telecommunications networks. Telecommunications service operators must maintain the confidentiality of any information transmitted or received by a telecommunications subscriber through a telecommunications network or telecommunications service provided by the respective operator;
- **Law Number 36 of 2009 on Health (October 13, 2009) as lastly amended by Government Regulation in Lieu of Law Number 2 of 2022 on Job Creation (December 30, 2022)** which stipulates that, in principle, every person is entitled to the confidentiality of their personal health information that has been provided to or collected by healthcare providers (Health Law);
- **Financial Services Authority (OJK) Regulation No. 6/POJK.07/2022 of 2022 on Consumer and Public Protection in the Financial Services Sector (April 14, 2022) (POJK 6/2022)**. OJK Regulation 6/2022 prohibits financial service providers from disclosing customer data or information to third parties without written consent from the customer or unless they are required to make such disclosure by law; and
- **Financial Services Authority (OJK) Circular Letter No. 14/SEOJK07/2014 of 2014 on Secrecy and Security of Consumers Personal Data and/or Information** which stipulates that personal data consisting of a name, address, date of birth or age, telephone number or the name of the subject's biological mother can only be shared with third parties with the consent of the owner of the personal data or as required by laws and regulations.

PDP Law

- Law No. 27 of 2022 on Personal Data Protection
  - ✓ Enacted on October 17, 2022.
  - ✓ 2 (two) years of transition period to adjust with the data processing practice since the enactment date (October 2024).
  - ✓ The scope covers (a) every Person (individual and legal entity) (b) Public Agency; and (c) International Organization which exercise legal actions as follow:
    i. Under the jurisdiction of Indonesia;
    ii. Outside the jurisdiction of Indonesia but having a legal impact in Indonesia; and/or towards Subjects of Indonesian Citizen outside the jurisdiction of Indonesia.

PDP Law

- **Personal Data is defined under the PDP Law as follows:**

  ✓ Data regarding individuals who are identified or can be identified separately or in combination with other information, either directly or indirectly through an electronic or non-electronic system.

  ➢ Includes electronic or non-electronic data processing.

TYPES OF PERSONAL DATA

General Personal Data

- Personal Data which is used as an identity to be known in the society.
- Including full name, gender, citizenship, religion, marital status, and/or combined personal data to identify a person.

TYPES OF PERSONAL DATA

Specific Personal Data

- Personal Data which more sensitive and has a higher risk when it is possessed by a non-entitled person.
- Including health data and information, biometric data, genetic data, criminal records, child data, personal financial data, and/or others.

Specific Personal Data

- Personal Data of Children: Consent by parents and/or guardians
- Personal Data of Person with Disabilities: Through special measure of communication in accordance with the laws and regulations (not yet regulated).
- Must be informed to Data Subjects: Data processing might need an appointment of Data Protection Officer and implementation of Data Protection Impact Assessment

PERSONAL DATA PROCESSING AND PRINCIPLES

Type of Personal Data Processing;

- Acquisition and collection;
- Processing and analysis;
- Storage;
- Rectification and update;
- Display, announcement, transfer, dissemination, or disclosure; and/or
- Deletion or destruction.

Principles of Personal Data Protection

1. Personal Data collection shall be carried out in a limited and specific, legal and valid, and transparent manner;
2. Personal Data processing shall be carried out in accordance with its purpose;
3. Personal Data processing shall be carried out by ensuring the rights of the Personal Data Subject;
4. Personal Data processing shall be carried out in an accurate, complete, not misleading, up-to-date, and in an accountable manner;
5. Personal Data processing shall be carried out by protecting the security of Personal Data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or loss of Personal Data;
6. Personal Data processing shall be carried out by notifying the processing purposes and activities, as well as the failure of Personal Data Protection;
7. Personal Data shall be destroyed and/or deleted after the expiry of the retention period or at the request of the Personal Data Subject, unless otherwise stipulated by laws and regulations; and
8. Personal Data processing shall be carried out responsibly and can be evidenced clearly.

LAWFUL BASIS OF PERSONAL DATA PROCESSING

- **Consent**;
- **Contract**;
- **Legal Obligation**;
- **Vital Interest**;
- **Public Task; and/or**
- **Legitimate Interest**

LAWFUL BASIS OF PERSONAL DATA PROCESSING

PDP Law requires personal data controllers to have a basis for data processing, which includes:

1. valid and unequivocal consent of the personal data subject for one or several specific purposes submitted by the personal data controller to the personal data subject;
2. fulfillment of contractual obligations the personal data subject is a party to, or to fulfill the request of the personal data subject at the time of entering into the agreement;
3. fulfilment of the legal obligations of the personal data controller in accordance with the provisions of laws and regulations; fulfillment of the protection of vital interests of the personal data subject;
4. carrying out duties in the context of public interest, public services, or exercising the authority of the personal data controller based on laws and regulations; and/or
5. fulfillment of other legitimate interests by taking into account the purposes, needs, and balance of interests of the personal data controller and the rights of the personal data subject.

CONSENT-BASED PERSONAL DATA PROCESSING

In carrying out Data Processing based on a Consent, the Personal Data Controller must submit information regarding:

- Legality of the Personal Data processing;
- Purpose of Personal Data processing;
- The type and relevance of the Personal Data to be processed;
- The retention period of documents containing Personal Data;
- Details regarding the Information collected;
- Period of Personal Data processing;
- Rights of the Personal Data Subject.

Consent can be provided out through written or recorded consents, either electronically or non-electronically.

In the event there are changes on the provided information, the Data Controller must notify the Data Subject before any change in Information made.

THIRD PARTY DATA SHARING

- When processing personal data with consent, a data controller must provide comprehensive information, including the purpose of the data processing. If the consent includes additional purposes, the consent request must meet the following criteria:
    1. It must be clearly distinguishable from other matters;
    2. It should be presented in an easily accessible and understandable format; and
    3. It must use simple and straightforward language
- A controller that wishes to share data to a third party which purposes falls outside the scope of the initial consent, must obtain a separate consent
- Consent must be documented either in writing or recorded form, whether electronically or non-electronically.

SUBJECTS OF PERSONAL DATA PROTECTION

- **Personal Data Controller ("Data Controller") :** any person, public entity, and international organization acting individually or jointly in determining the objectives and exercising control over the processing of Personal Data.
- **Personal Data Processor ("Data Processor")** : any person, public entity, and international organization acting individually or jointly in Personal Data processing on behalf of the Personal Data Controller.
- **Personal Data Subject ("Data Subject")** : every individual to whom the Personal Data is attached.

Data Controller vs. Data Processor

Determines the objective and purposes of personal data processing	Can only process personal data upon the appointment and instruction of Controller (s)
Must directly obtain consent from Data Subjects	Does not obtain direct consent from Data Subjects
Responsible for personal data processing, including to the processing conducted by the Data Processor it appointed	As long as the personal data processing is carried out in accordance with the instruction of the Data Controller, does not independently responsible for the personal data processing

RIGHTS OF DATA SUBJECT

Rights of Transparency of data usage	Rights to revise	Rights to access
Rights of deletion	Rights to withdraw consent	Rights to object on automatic processing
Rights to postpone or limit data processing	Rights to bring claim and to be indemnified	Rights to obtain and use Personal Data

The rights can be excluded for:

- Interest on national defense and security
- Interest on legal enforcement
- Public interest in context of state administration
- Interest on supervising the financial sector, monetary, payment systems, and financial system stability carried out in the context of state administration.
- Interest on statistics and scientific research

OBLIGATIONS OF DATA CONTROLLER AND DATA PROCESSOR

To have a basis for data processing	To process in a limited and transparent manner	Ensure accuracy, completeness, and consistency of personal data	Update/rectify inaccuracies of personal data 3z24 hours since the request
To record data processing activities	Provide access 3 x24 hours since the request	Carry out a DPIA in certain cases	Ensure the security of Personal Data
Maintain the confidentiality of Personal Data	Supervise parties involved in data processing activities	Protect Personal Data from unlawful processing	Protect from and Mitigate unauthorized access of Personal Data
Cease Personal Data processing 3 x 24 hours since the request	Postpone/restrict Personal Data processing 3 x 24 hours since the request	Terminate Personal Data processing (e.g. reaches the data retention period)	Erase and/or destroy Personal Data and notify it to the Data Subject
Notify the Data Subject and DPA in case of data breach	Be responsible and able to demonstrate its accountability	Notify Data Subject in case of corporate actions	Comply with the order of DPA

**light blue boxes also apply to Data Processor*

OBLIGATIONS OF DATA CONTROLLER AND DATA PROCESSOR (Cont.)

The obligations of Data Controller can be exempted for the purpose of:

- Interest on national defense and security
- Interest on legal enforcement
- Public interest in context of state administration
- Interest on financial sectors
- Interest on statistics and scientific research

DATA PROTECTION IMPACT ASSESSMENT

A DPIA must be carried out before Personal Data processing that has high potential risk to the Data Subject, which include:

1. automatic decision-making that has legal consequences or significant impact on the Personal Data Subject;
2. processing of specific Personal Data;
3. processing of large-scale Personal Data;
4. processing of Personal Data for systematic evaluation, scoring or monitoring activity of Personal Data Subjects;
5. processing of Personal Data for the activity of matching or combining a group of data;
6. the use of new technologies in the processing of Personal Data; and/or
7. processing of Personal Data that limits the exercise of the rights of the Personal Data Subject.

DATA PROTECTION OFFICER

- Data Controller and Data Processor is required to appoint a DPO if:
  a. Personal Data processing is carried out for the benefit of public services;
  b. the core activities of the Controller have the nature, scope, and/or objectives that require regular and systematic supervision of Personal Data on a large scale; and
  c. the core activities of the Controller consist of Personal Data processing on a large scale for Personal Data that is specific in nature and/or Personal Data related to criminal acts.

- Duties of DPO include:
  a. to inform and advise the Data Controller or Data Processor to comply with the PDP Law;
  b. to monitor and ensure compliance with this Law and the policies of the Data Controller or Data Processor;
  c. to provide advice on DPIA and monitor the performance of the Data Controller and Data Processor; and
  d. to coordinate and act as liaison officer for issues relating to the processing of Personal Data.

DATA PROTECTION OFFICER FOR CORPORATION

- Data Protection Officers can be internal or external parties
- Officers of officials who carry out personal data protection are appointed based on professionalism, legal knowledge, personal data protection practices, and the ability to fulfill their duties. They can be appointed internally or externally as controllers of personal data or processors of personal data. Further provisions regarding officials or employees who carry out the function of protecting personal data are regulated by government regulations.

CROSS-BORDER DATA TRANSFER

- Cross-border data transfer can be conducted if any of the following is fulfilled:
  - the receiving nation of the personal data has similar or higher level of personal data protection;
  - Ensure adequate and binding personal data protection; or
  - There is consent from the data subject.
- Sector-specific notification requirement may apply (e.g. the financial sector).
- An implementing regulation is to be expected.

Coordination requirement under MOCI Reg. 20/2016

- MOCI Reg. 20/2016 requires any transfer of personal data conducted by an Electronic System Provider domiciled in Indonesia to overseas must be carried out by coordinating with the MOCI.
- Coordination must be done before and after the transfer is carried out, which will contain, among others, the types of data being transferred, the purpose of transfer, and the destination.

CORPORATE ACTIONS

- Data controller must provide notification to data subject on the transfer of personal data in the event of a merger, spin-off, acquisition, consolidation or dissolution.
- Notification is given before and after the corporate action.
- Notification can be given to data subject personally or through mass media (e.g., newspaper announcement)

FAILURE OF PERSONAL DATA PROTECTION

In the event there is breach of data or failure of protection, the Controller must provide a written notification no later then 3 x 24 (three times twenty-four) hours to:

- The Personal Data Subject; and
- The institution (Data Protection Authority).

The written notification shall at least contain:

- the disclosed Personal Data;
- when and how Personal Data are disclosed; and
- efforts to handle and recover from the disclosure of Personal Data by the Personal Data Controller.

The Personal Data Controller must be responsible for Personal Data processing and must demonstrate accountability in fulfilling the obligations of implementing Personal Data Protection principles.

OTHER NOTABLE PROVISIONS

Data Protection Authority *(Institution)*

- Government may determine new agency to supervise the data protection sector.
- The agency has broad duties and authorities including:
  a. Formulating and promulgating policies and strategies for Personal Data Protection
  b. Supervising
  c. Enforcing administrative sanctions
  d. Facilitating an alternative dispute settlement

Dispute Settlement and Procedural Law

- Conducted in arbitration, court and alternative dispute resolution institutions
- Additional legal evidence in the form of electronic information and/or electronic documents
- The trial process will be conducted behind closed doors to protect personal data.

SANCTIONS

Administrative Sanctions

- Form of administrative sanctions:

a. A written reprimand;

b. Temporary suspension of Personal Data processing activities;

c. Erasure or removal of Personal Data; and/or

d. Administrative fines;

  - The maximum fines are 2 (two) percent of the annual income or annual revenue at the maximum against the violation variable.

Criminal Sanctions

- Imprisonment on 4 – 6 years;
- Fines on Rp 4 Billion – Rp 6 Billion;
- Additional sentences, as follows:
  - Confiscation of profits and/or assets obtained;
  - Confiscation of profits and/or assets obtained resulting from crimes; and
  - Compensation of payment.

CRIMINAL SANCTIONS FOR CORPORATION

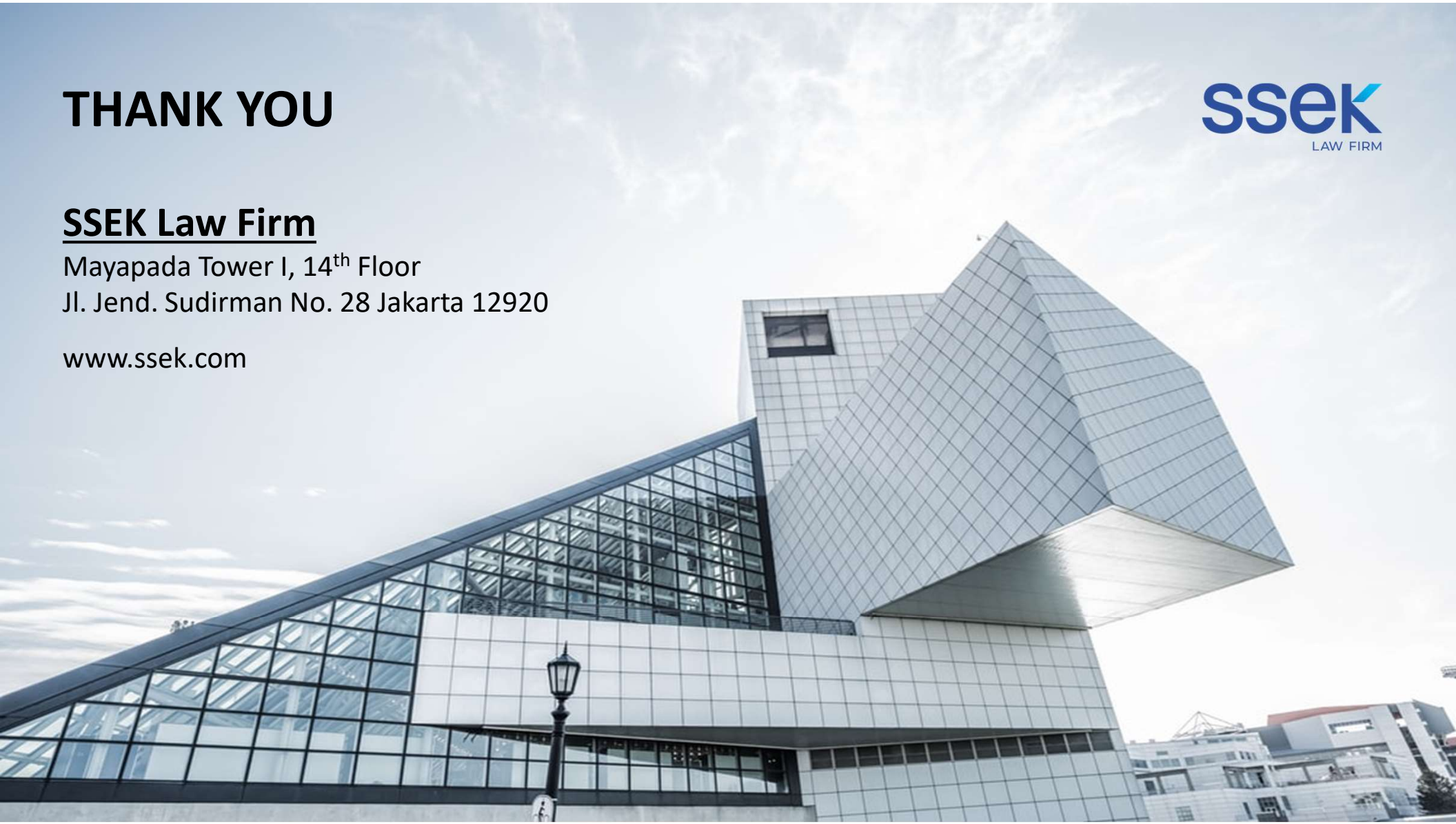
- In the event that a criminal act is committed by a Corporation, the penalty may be imposed on management, control holders, giver of orders, beneficial owners, and/or the Corporation.
- The fines imposed on a Corporation is maximum 10 (ten) times of the maximum sentence imposed.
- In addition to being sentenced to a fine, the Corporation may be imposed on additional sentences in the form of:
  (a) confiscations or profits and/or assets obtained or proceeds from crimes;
  (b) suspension of the entire or part of the Corporation's business;
  (c) permanent prohibition of doing certain actions;
  (d) shutdown of the entire or part of the Corporation's place of business and/or activities;
  (e) fulfill the obligations that have been neglected;
  (f) payment of compensation;
  (g) revocation of license; and/or
  (h) dissolution of the Corporation;.

Post PDP Law

Following the ratification of the PDP Law, the Indonesian government must prepare and issue several implementing regulations. This includes the creation of further provisions regarding:

- violations of the processing of personal data and the procedure for indemnity,
- rights of personal data subjects to use and send personal data;
- implementation of personal data processing;
- impact assessment of personal data protection;
- procedure to deliver a notification of the transfer of personal data to the personal data subject by a legal entity that performs a merger, separation, acquisition, consolidation, or dissolution;
- the duties and other specifications of officials or officers who carry out the personal data protection function;
- transfer of personal data;
- procedures for the imposition of administrative sanctions;
- establishment of an institution to implement personal data protection; and
- procedures for implementing the authority of the established institution.

THANK YOU



SSEK Law Firm

Mayapada Tower I, 14th Floor
Jl. Jend. Sudirman No. 28 Jakarta 12920

www.ssek.com