

## Outline of the System Reform Policy under the Triennial Review of the Act on the Protection of Personal Information (APPI)

- Based on the **“triennial review”** provision under the 2020 Amendment to the APPI, the Personal Information Protection Commission (PPC) assessed the current situation and identified key issues, through hearings with relevant organizations and experts.
- Considering the rapid advancement of information and communication technologies, as well as international trends, **amendments of the APPI in a comprehensive and balanced manner are needed**. These amendments include revisions to the rules regarding the involvement of data subject and the establishment of measures to ensure effective compliance with the APPI.
- The amendment bill is **expected to be submitted to the Diet** as early as **spring 2026** and, if approved, would come into **effect approximately two years later**.

### System Reform Policy

#### Promotion of the Appropriate Data Utilization

- Data subject's consent shall not be required** where the data is used solely **for generating statistics (including AI development**, to the extent that it is categorized as the generation of statistics), with respect to the provision of personal data to third parties and the acquisition of published sensitive personal information.
- Revising **provisions regarding exceptional rules allowing the handling of personal information without consent** as follows:
  - Consent is not required** where, based on the circumstances of acquisition, **it is evident that the handling does not go against the data subject's intent** and does not harm the individual's rights or interests.
  - For purposes such as the protection of life or the improvement of public health, **the requirement is relaxed** from “where obtaining consent is difficult” to **“where there are reasonable grounds for not obtaining consent.”**
  - Clarifying that **institutions or organizations providing medical services are included within “academic institutions”** eligible for the exceptional rule.

#### Establishment of Regulations that Appropriately Address Risks

- Where the data subject is under 16, consent and notifications shall be addressed to the legal representative**, and the requirements for requesting cessation of use of the minor's personal data are relaxed. In addition, a responsibility provision is established to give priority to the best interests of minors in handling their personal information.
- With respect to facial feature data, business operators are required to inform specified matters regarding its handling**, the requirements for requesting cessation of use are relaxed, and the provision of such data to third parties on opt-out basis (opt-out scheme) is prohibited.
- With respect to business operators entrusted with data processing, the **obligations concerning the proper handling of entrusted personal data are reviewed**.
- In the event of a personal data breach, the obligation to notify the data subject is relaxed** where **the risk to the data subject's rights and interests is considered low**.

#### Prevention of Inappropriate Use

- With respect to information that does not constitute personal information but enables targeting of a specific individual, inappropriate use and improper acquisition are prohibited**.
- Regarding the opt-out scheme, an obligation is imposed** to verify the identity of recipients and the purpose for which they intend to use the data.

#### Ensuring the Effective Enforcement of Compliance Obligations

- The requirements for issuing the orders are revised** to enable prompt rectification of violations, and **recommendations or orders may also be issued to require measures necessary to protect the data subject's rights and interests**, such as notification to or publication for the data subject regarding the relevant violations.
- A statutory basis is established to request third parties** who assist or are otherwise involved in relation to a violation, **to take the necessary measures to cease such a violation**.
- With respect to criminal penalties for the improper provision of personal information databases, **provision with intent to cause harm is subject to punishment, statutory penalties are increased, and penalties are introduced for the fraudulent or improper acquisition** of personal information.
- To effectively deter serious violations** involving the large-scale, economically motivated handling of personal information, **the PPC is authorized to impose administrative monetary penalties** equivalent to the pecuniary benefits obtained through such violations, including cases where individuals' rights and interests are significantly infringed.

Outside the scope of the APPI amendments, further consideration is given to streamlining data breach reporting and enhancing cooperation among relevant stakeholders to better protect the rights and interests of data subject.