SEKOLAH TINGGI HUKUM INDONESIA JENTERA

PSHK Pusat Studi Hukum & Kebijakan Indonesia

LeIP

Executive Summary

Legal & Institutional Assesment of the Implementation of Personal Data Protection in Indonesia's Criminal Justice System

Executive Summary

Legal & Institutional Assesmen of the Implementation of Personal Data Protection in Indonesia's Criminal Justice System

April 2026
Sekolah Tinggi Hukum Indonesia Jentera

EXECUTIVE SUMMARY

1. Background

Digital transformation in Indonesia's criminal justice system has advanced rapidly over the past decade, marked by the increasing use of electronic systems in case management and data exchange among law enforcement institutions. Initiatives such as the integration of the Technology-Based Integrated Criminal Justice System (SPPT-TI) reflect a move toward greater efficiency and coordination. However, this development has also increased the scale, complexity, and sensitivity of personal data processed throughout all stages of criminal proceedings.

Personal data within this system includes highly sensitive information, such as the identities of suspects, victims, and witnesses, as well as social, economic, and health data. This data is not only collected but also flows across institutions—from investigation to correctional services—forming a large-scale data governance ecosystem. Without adequate safeguards, this condition poses significant risks, including data breaches, misuse, disproportionate profiling, and violations of the rights to privacy and a fair trial.

The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents a key milestone in establishing a national legal framework. However, the primary challenge lies in its implementation, particularly within the complex, multi-agency context of the criminal justice system.

Personal data protection is rooted in constitutional guarantees of the right to privacy, as reflected in the 1945 Constitution, which protects personal integrity, dignity, and honor. The enactment of the Personal Data Protection Law reinforces this guarantee by consolidating principles, rights, and obligations within a comprehensive legal framework. Accordingly, personal data protection is not merely an administrative or technical issue, but forms part of the State's obligation to uphold and protect

mental rights and the legitimacy of the criminal justice system.

2. Objectives and Approach of the Study

This study aims to provide an initial mapping of the current state of personal data management within the criminal justice system, identify risks arising in institutional practices, and offer a basis for policy development and institutional capacity strengthening. Accordingly, this report is not merely descriptive but is intended to support more targeted policy interventions.

The methodological approach combines doctrinal analysis of the legal framework with institutional analysis of existing practices. Data collection was conducted through document review, stakeholder interviews, and focus group discussions. This approach enables triangulation between legal norms and actual practices, resulting in a more comprehensive understanding of the current state of personal data protection.

3. Key Findings

3.1. Regulatory Fragmentation and Implementation Gaps

The study shows that personal data protection within the criminal justice system remains fragmented. Prior to the PDP Law, data protection provisions were scattered across various sectoral regulations, each developed from different logics, such as evidentiary needs, victim and witness protection, and public information disclosure. As a result, data protection did not evolve within a unified conceptual framework but rather developed in an incidental and inconsistent manner.

Although the PDP Law has been fully in force since 2024, it has not yet become the primary reference in practice. This is due to the absence of implementing regulations and cross-institutional operational standards, the tendency to interpret law enforcement exceptions broadly, and the continued dominance of sectoral regula-

tions in daily practice. In this situation, the PDP Law risks functioning merely as a declarative normative framework, while actual practices continue to be shaped by existing institutional logics.

3.2. Information Disclosure Paradigm and Weak Data Protection Perspective

Another key finding is that personal data protection is still largely understood within the framework of public information disclosure (KIP-centric), rather than as an independent substantive right. In practice, the primary focus often lies on whether information can be disclosed or exempted from public access, rather than on the more fundamental question of the legitimacy of data processing.

As a result, core data protection principles—such as purpose limitation, data minimization, and accountability—have not been fully internalized in institutional practices. The paradigm shift envisioned by the PDP Law, from a disclosure-oriented logic toward rights-based data governance, remains at an early stage.

3.3. Data Governance and Cross-Institutional Accountability

The criminal justice system fundamentally operates as a cross-institutional data exchange ecosystem, where data continuously flows from one stage to another. However, this extensive data flow is not accompanied by clear allocation of responsibilities among institutions.

3.4. Limitations in Instruments and Institutional Capacity

The study also finds that many obligations under the PDP Law have not yet been operationalized within institutions. The appointment of Data Protection Officers (DPOs) has not been carried out, mechanisms for recording data processing activities are not yet in place, and Data Protection Impact Assessments (DPIAs) are

not commonly practiced.

Moreover, technical guidelines on data protection remain dispersed across various internal regulations and have not been integrated into a consistent operational framework. Institutional focus also tends to remain limited to technological security aspects, without being complemented by a broader data governance approach.

3.5. Risks in Data Management Practices

In practice, several key risks can be identified in personal data management. These include excessive data collection, use of data beyond its original purpose, weak access controls, and suboptimal anonymization mechanisms. These risks are particularly significant given that the data often relates to vulnerable groups, such as victims of crime, children, and witnesses.

These findings indicate that data protection is not solely a matter of technical security, but also concerns how data is used, shared, and stored throughout the law enforcement process.

3.6. Structural Issues in Data Protection

More broadly, the study confirms that personal data protection issues are structural in nature. They result from the interaction between rapid digitalization, the need for cross-institutional coordination, an unharmonized regulatory framework, and an institutional culture that does not yet treat data as an object requiring strict protection.

In this context, the implementation of the PDP Law remains at an early stage, while reliance on data continues to grow faster than the development of its protective framework. This creates systemic vulnerabilities that cannot be addressed through technical interventions alone.

4. Recommendations

Strengthening personal data protection in the criminal justice system requires a systemic and multi-dimensional approach, encompassing regulatory, institutional, operational, capacity, and oversight aspects. Based on the study findings, the following strategic recommendations are proposed:

1) Establishing a cross-institutional minimum standard framework

Data protection remains sectoral with varying standards and unclear responsibilities. A shared minimum standard framework is needed to ensure consistency in key principles such as purpose limitation, security, retention, and accountability, while bridging the gap between the PDP Law and operational practices.

2) Shifting the paradigm from disclosure toward a balanced approach with data protection

The current disclosure-oriented approach needs to shift toward a balance where data protection is treated as an equal principle. It should be integrated into internal policies, publication guidelines, and operational practices, becoming part of process design rather than a reactive measure.

3) Strengthening governance of data exchange within the criminal justice system

Major risks arise from cross-institutional data exchange. Clear designation of data controllers, purpose limitation, and accountability mechanisms are needed to ensure that integration does not increase the risk of violations.

4) Enhancing institutional accountability in data management

Data management remains poorly documented and lacks systematic data flow mapping and risk assessment. Institutions must adopt more structured approaches to ensure accountability.

5) Developing incident response and complaint mechanisms

The absence of clear mechanisms for handling data breaches and limited access to complaint channels represent significant gaps. Clear procedures for reporting, handling, and recovery, as well as accessible complaint mechanisms, are essential.

6) Prioritizing the protection of vulnerable groups

Data breaches disproportionately affect vulnerable groups. Protection must be designed in a differentiated manner, taking into account risks such as stigmatization, re-victimization, and safety threats.

7) Strengthening operational practices in data use and security

Risks also stem from daily practices, such as the use of insecure communication channels. Consistent operational standards are needed to ensure effective implementation.

8) Strengthening capacity and clarifying institutional roles in data management

Data management still depends on individual practices. Clear role definitions, including designated data management functions, and practical capacity-building are necessary to ensure proper internalization of data protection principles.

9) Strengthening coordination and oversight mechanisms

Limited cross-institutional coordination and weak oversight hinder effective implementation. Structured coordination mechanisms are needed to ensure policy consistency and accountability.

10) Integrating data protection into digital justice reform

Digitalization has outpaced the development of data protection governance. Data protection must be integrated from the system design stage to ensure that efficiency is aligned with accountability and rights protection.

5. Conclusion

This report underscores that personal data protection is a prerequisite for a fair, accountable, and human rights-oriented criminal justice system. Reform efforts must not focus solely on efficiency and digitalization but must also ensure that data use operates within a lawful, proportionate, and accountable governance framework. Accordingly, the future agenda is not only to accelerate system integration but also to build a data protection architecture capable of maintaining a balance between law enforcement interests and the protection of individual rights.

SEKOLAH TINGGI HUKUM
INDONESIA JENTERA

PSHK
Pusat Studi Hukum &
Kebijakan Indonesia

L e I P