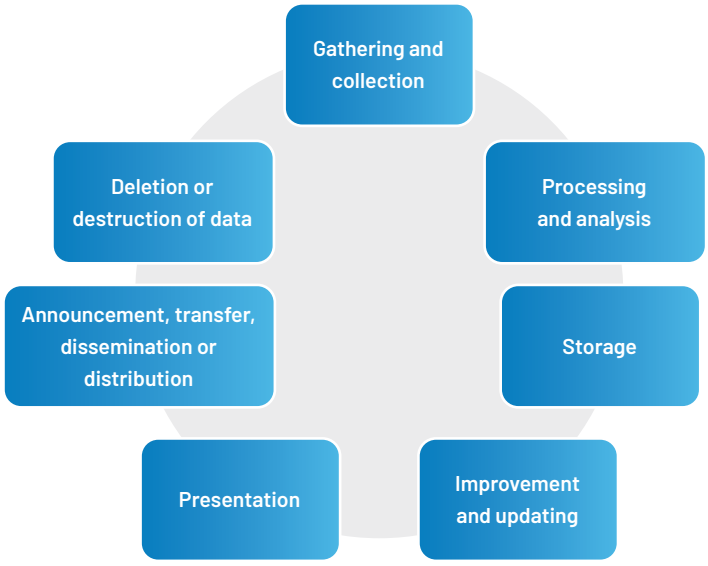
Controlled Secondary Data Processing

TelkomGroup strives to process customer personal data responsibly in accordance with the PDP Law. Telkom does not process personal data without a proper processing basis, unless required for service completion, legal compliance, or adherence to applicable regulations.

Figure 100. Data Processing Cycle



All customers' personal data is processed according to the principles of personal data processing, and managed systematically and in accordance with the law to ensure transparency and compliance. To assist in ensuring the completeness, current, and up-to-date personal data compliance accuracy, TelkomGroup implements personal data accuracy compliance guidelines that cover the fulfillment aspects of confidentiality, integrity, availability, verification, update/improvement, Service Level Agreement (SLA), and notifications. These personal data protection compliance guidelines serve as a reference to control the processing of personal data.

One of the fundamental aspects in adhering to the implementation of the Personal Data Protection Principles is to oversee the role of each party within the personal data processing ecosystem. TelkomGroup commits to continuously overseeing external entities that process personal data through assessments before involving data processors, monitoring data processing, and post-monitoring after the completion of personal data processing agreements.

Any request for personal data by external parties has to go through the Data Governance (DG) Council, a hearing process to ensure data processing compliance, from the processing purpose, data transfer methods, to data encryption. This process is carried out as part of Telkom's commitment to uphold transparency, security, and compliance in every customer data management activity.

As personal data controller and processor, Telkom also ensures third-party data processing is conducted in accordance with the principles of Personal Data Protection, with responsibilities stipulated in transparent data protection agreements, in order to safeguard customer security and privacy.

In 2025, 100% of data requests from the Government and Law Enforcement Authorities (APH) were fulfilled in accordance with compliance principles, while there were no requests from third parties for monetization or business consulting purposes. In the case of third-party data requests, the entire data disclosure process is conducted with strict protection through a Non-Disclosure Agreement (NDA), which aligns with the Data Governance policy, Data Control Standards, and the PDP Law. [SASB TC-TL-230a.2, TC-TL-220a.4]

> **In 2025, there were 117 use cases of data transfers that were handled securely, encrypted, and in accordance with TelkomGroup's procedures.**

Tackling Cyber Threats

The escalating cyber threats in the increasingly interconnected digital era have elevated information security to a strategic priority. In light of this, TelkomGroup takes proactive steps in anticipating cyber risks.

Telkom, through the Network Directorate, has the Network Strategy & Architecture Function Unit and the Cybersecurity Function Unit at the BOD-1 level (Vice President level), each of which is responsible for the governance and operation of cybersecurity. The implementation of cybersecurity is guided by Telkom's cybersecurity policies, which are aligned with the ISO/IEC 27001:2022 standard. [SASB TC-TL-230.a.2, TC-SI-230a.2, TC-IM-230a.2]

Telkom has obtained ISO 27001:2013 certification since 2022, valid until April 11, 2025. As a continuation of the existing certification, on February 13, 2025, Telkom updated its ISO 27001:2022 certification (valid until February 12, 2028) to align the implementation of information security standards with the latest practices.

Preventive strategies are conducted through the identification and mapping of threats, such as a lack of stakeholder awareness, various motives for cyberattacks, and potential vulnerability in the technology supply chain. As a mitigation effort, Telkom improves information security resilience through regular cybersecurity awareness-raising programs for employees, vulnerability evaluations, periodic penetration tests, and daily monitoring of IT infrastructure.

Advancing Cybersecurity Competence

Security awareness programs are held monthly through various media, such as posters, podcasts, and webinars. All TelkomGroup employees are required to take mandatory Cybersecurity Training. In 2025, a total of 4,844 employees participated in the training, of which 4,817 successfully passed, resulting in a graduation rate of 99.4%.

Cyber Incident Handling

The Computer Security Incident Response Team (CSIRT) is responsible for handling and responding to cybersecurity incidents. CSIRT also functions as a reporting escalation channel for employees to report suspected personal data protection incidents. Since 2023, CSIRT has been registered with the State Cyber and Cryptography Agency (BSSN) to strengthen system protection, improve incident response capabilities, and expand collaboration and exchange of cyber threat information.

Cyber Incident Quick Response

To enable a rapid response to cyber incidents, the Cybersecurity Operation Center (CSOC) operates 24/7 to proactively detect, monitor, and handle threats.

Throughout 2025, although Telkom faced frequent cyber threats, no incidents occurred that disrupted operations. Nevertheless, sustained vigilance and continuous monitoring are maintained to safeguard information security and ensure uninterrupted service for customers.