



Indonesia
Humanitarian
Logistics
Lab

Data Protection and Information Security Policy

Kebijakan Perlindungan Data dan Keamanan Informasi

**Version: 1.0 | Approved by: Indonesia Humanitarian Logistics Lab Chairperson |
Effective: January 1st, 2026**

Versi: 1.0 | Disetujui oleh: Ketua Indonesia Humanitarian Logistics Lab |
Berlaku mulai: 1 Januari 2026

This Policy establishes the standards and obligations governing the collection, processing, storage, disclosure, and protection of personal data and organizational information managed by Indonesia Humanitarian Logistics Lab. It outlines the principles of legality, transparency, data minimisation, integrity, confidentiality, and accountability, and provides clear requirements for information security, data subject rights, breach reporting, and responsible data governance. The Policy ensures that all individuals handling data within Indonesia Humanitarian Logistics Lab uphold the highest ethical and professional standards in managing and safeguarding information.

Kebijakan ini menetapkan standar dan kewajiban terkait pengumpulan, pemrosesan, penyimpanan, pengungkapan, dan perlindungan data pribadi serta informasi organisasi yang dikelola oleh Indonesia Humanitarian Logistics Lab. Kebijakan ini menjabarkan prinsip legalitas, transparansi, minimalisasi data, integritas, kerahasiaan, dan akuntabilitas, serta memberikan ketentuan yang jelas mengenai keamanan informasi, hak pemilik data, pelaporan pelanggaran, dan tata kelola data yang bertanggung jawab. Kebijakan ini memastikan bahwa seluruh individu yang menangani data di lingkungan Indonesia Humanitarian Logistics Lab menjunjung tinggi standar etika dan profesionalisme dalam mengelola dan melindungi informasi.

Table of Contents

Daftar Isi

Table of Contents.....	2
I. Purpose	2
II. Scope	3
III. Key Definitions	3
IV. Data Protection Principles	4
V. Types of Data Processed	4
VI. Data Collection and Processing	5
VII. Data Storage, Retention, and Disposal.....	5
VIII. Data Disclosure and Sharing	6
IX. Information Security Requirements	7
X. Rights of Data Subjects	7
XI. Data Breach Management	8
XII. Data Protection Focal Point.....	8
XIII. Training and Compliance.....	9
XIV. Relationship with Other Policies	9
XV. Legal Precedence in Case of Dispute	10
XVI. Review and Amendment	10
XVII. Entry into Force	10
Acknowledgment (Statement of Understanding and Compliance)	10

I. Purpose

Tujuan

This Data Protection and Information Security Policy establishes the standards for the lawful collection, use, storage, disclosure, and protection of personal data and organizational information processed by Indonesia Humanitarian Logistics Lab.

The Policy ensures compliance with national regulations and reflects internationally recognized principles of responsible data management, integrity, confidentiality, and accountability.

Kebijakan Perlindungan Data dan Keamanan Informasi ini menetapkan standar terkait pengumpulan, penggunaan, penyimpanan, pengungkapan, dan perlindungan data pribadi serta informasi organisasi yang dikelola oleh Indonesia Humanitarian Logistics Lab secara sah dan bertanggung jawab.

Kebijakan ini memastikan kepatuhan terhadap peraturan nasional serta mencerminkan prinsip-prinsip perlindungan data, integritas, kerahasiaan, dan akuntabilitas yang diakui secara internasional.

II. Scope

Ruang Lingkup

This Policy applies to all individuals associated with Indonesia Humanitarian Logistics Lab, including employees, consultants, volunteers, interns, board members, partner organizations, contracted service providers, and visitors who handle personal data or organizational information.

This Policy covers all data processed in both physical and digital form across programs, operations, administrative systems, research activities, and capacity-building functions of Indonesia Humanitarian Logistics Lab.

Kebijakan ini berlaku bagi seluruh individu yang terhubung dengan Indonesia Humanitarian Logistics Lab, termasuk pegawai, konsultan, relawan, peserta magang, anggota dewan, organisasi mitra, penyedia jasa kontraktual, dan pengunjung yang menangani data pribadi atau informasi organisasi.

Kebijakan ini mencakup semua data yang diproses dalam bentuk fisik maupun digital di seluruh program, operasi, sistem administrasi, kegiatan penelitian, dan kegiatan pengembangan kapasitas Indonesia Humanitarian Logistics Lab.

III. Key Definitions

Definisi Kunci

- **Personal Data:** Information relating to an identified or identifiable individual.
 - **Sensitive Personal Data:** Data requiring enhanced protection, including information related to health, vulnerabilities, children, or other protected categories under national law.
 - **Data Subject:** An individual whose personal data is collected or processed.
 - **Data Controller:** Indonesia Humanitarian Logistics Lab as the entity determining the purpose and means of data processing.
 - **Data Processor:** Any individual or external entity that processes data on behalf of Indonesia Humanitarian Logistics Lab.
 - **Data Breach:** Any incident that results in accidental or unlawful loss, alteration, disclosure, or unauthorized access to personal data or organizational information.
-
- **Data Pribadi:** Informasi mengenai individu yang teridentifikasi atau dapat diidentifikasi.
 - **Data Pribadi Sensitif:** Data yang memerlukan perlindungan lebih tinggi, termasuk informasi terkait kesehatan, kerentanan, anak, atau kategori lain yang dilindungi oleh hukum nasional.
 - **Pemilik Data:** Individu yang data pribadinya dikumpulkan atau diproses.
 - **Pengendali Data:** Indonesia Humanitarian Logistics Lab sebagai pihak yang menentukan tujuan dan cara pemrosesan data.
 - **Pemroses Data:** Setiap individu atau entitas eksternal yang memproses data atas nama Indonesia Humanitarian Logistics Lab.
 - **Pelanggaran Data:** Insiden yang mengakibatkan hilangnya, berubahnya, terungkapnya, atau akses tidak sah terhadap data pribadi atau informasi organisasi.

IV. Data Protection Principles

Prinsip-Prinsip Perlindungan Data

Indonesia Humanitarian Logistics Lab adheres to the principles of lawfulness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability in the collection, processing, storage, and management of all personal data and organizational information.

Indonesia Humanitarian Logistics Lab menerapkan prinsip legalitas dan transparansi, pembatasan tujuan, minimalisasi data, akurasi, batas penyimpanan, integritas dan kerahasiaan, serta akuntabilitas dalam pengumpulan, pemrosesan, penyimpanan, dan pengelolaan seluruh data pribadi dan informasi organisasi.

V. Types of Data Processed

Jenis Data yang Diproses

5.1. Personal Data

General personal information, such as names, contact details, identification documents, and employment or training-related information.

5.2. Sensitive Personal Data

Information relating to health, vulnerabilities, children, or demographic categories that require heightened protection.

5.3. Organizational and Operational Information

Contracts, procurement materials, internal reports, financial information, correspondence, and other sensitive organizational documents.

5.4. Digital Information Systems

Email communications, shared drives, cloud-based platforms, electronic documents, and system authentication credentials.

5.1. Data Pribadi

Informasi umum seperti nama, kontak, dokumen identitas, serta informasi terkait pekerjaan atau partisipasi pelatihan.

5.2. Data Pribadi Sensitif

Informasi terkait kesehatan, kerentanan, data demografis tertentu, atau kategori lain yang memerlukan perlindungan lebih tinggi.

5.3. Informasi Organisasi dan Operasional

Kontrak, dokumen pengadaan, laporan internal, informasi keuangan, korespondensi, dan dokumen sensitif organisasi lainnya.

5.4. Sistem Informasi Digital

Email, penyimpanan bersama, platform berbasis cloud, dokumen elektronik, dan sistem autentifikasi kredensial.

VI. Data Collection and Processing

Pengumpulan dan Pemrosesan Data

6.1. Legal Basis

Data may only be collected based on consent, legitimate operational purposes, contractual obligations, or compliance with legal requirements.

6.2. Notification

Data subjects will be informed of the purpose of data collection and their rights under this Policy.

6.3. Accuracy

Data subjects may request the correction or updating of inaccurate or incomplete information.

Upon receipt of a report, Indonesia Humanitarian Logistics Lab will conduct an initial assessment to determine whether the allegation falls within the scope of this policy or should be referred to:

- the Prevention of Sexual Exploitation, Abuse and Harassment Policy,
- the Safeguarding Policy,
- the Human Resources disciplinary mechanism, or
- relevant legal authorities.

6.1. Dasar Hukum

Data hanya dapat dikumpulkan berdasarkan persetujuan, tujuan operasional yang sah, kewajiban kontraktual, atau ketentuan hukum yang berlaku.

6.2. Pemberitahuan

Pemilik data akan diinformasikan mengenai tujuan pengumpulan serta hak-hak mereka sesuai kebijakan ini.

6.3. Akurasi

Pemilik data dapat mengajukan permintaan koreksi atau pembaruan apabila data tidak akurat atau tidak lengkap.

Setelah laporan diterima, Indonesia Humanitarian Logistics Lab akan melakukan penilaian awal untuk menentukan apakah laporan tersebut berada dalam cakupan kebijakan ini atau perlu dialihkan kepada:

- Kebijakan Pencegahan Eksploitasi, Kekerasan, dan Pelecehan Seksual
- Kebijakan Perlindungan dan Pencegahan Risiko Kekerasan
- Mekanisme disiplin Sumber Daya Manusia
- Otoritas penegak hukum yang relevan

VII. Data Storage, Retention, and Disposal

Penyimpanan, Retensi, dan Pemusnahan Data

- Personal and organizational data must be stored securely in locked physical storage or password-protected digital systems.

- Access is restricted to authorized individuals with a legitimate operational need.
 - Retention schedules follow organizational, programmatic, or statutory requirements. Unless otherwise required by law, audit obligations, or dispute resolution processes, personal data and organizational information may be securely destroyed after a minimum retention period of **five (5) years**, provided that such data is no longer needed for operational, legal, or evidentiary purposes.
 - Secure disposal methods, including shredding or permanent deletion, must be applied to all data no longer required.
-
- Data harus disimpan secara aman dalam sistem digital yang diproteksi kata sandi atau dalam penyimpanan fisik yang terkunci.
 - Akses hanya diberikan kepada individu yang berwenang dan memiliki kebutuhan operasional yang sah.
 - Jadwal retensi mengikuti ketentuan organisasi, program, atau persyaratan peraturan perundang-undangan. Kecuali apabila diwajibkan oleh hukum, kewajiban audit, atau proses penyelesaian sengketa, data pribadi dan informasi organisasi dapat dimusnahkan setelah jangka waktu retensi minimum **lima (5) tahun**, sepanjang data tersebut tidak lagi diperlukan untuk keperluan operasional, hukum, atau pembuktian.
 - Pemusnahan data dilakukan secara aman melalui penghancuran fisik atau penghapusan permanen.

VIII. Data Disclosure and Sharing

Pengungkapan dan Berbagi Data

Data may only be disclosed to third parties when:

1. legally justified,
2. required for operational or programmatic purposes, or
3. subject to a written agreement ensuring compliance with this Policy.

Unauthorized disclosure of personal or sensitive data is strictly prohibited. Any violation of this provision may result in administrative or disciplinary action, including termination of employment or contract. Where applicable, such violations may also constitute a criminal offense under the laws of the Republic of Indonesia, including Law No. 11 of 2008 on Electronic Information and Transactions as amended by Law No. 19 of 2016 and further amended by Law No. 1 of 2024, and may be subject to legal proceedings.

Data hanya dapat diungkapkan kepada pihak ketiga apabila:

1. memiliki dasar hukum,
2. diperlukan untuk tujuan operasional atau programatik, atau
3. terdapat perjanjian tertulis yang memastikan kepatuhan terhadap kebijakan ini.

Pengungkapan data pribadi atau data sensitif tanpa izin dilarang keras. Setiap pelanggaran terhadap ketentuan ini dapat mengakibatkan tindakan administratif atau disipliner, termasuk pemberhentian kerja atau pemutusan kontrak. Apabila berlaku, pelanggaran tersebut juga dapat dikategorikan sebagai tindak pidana sesuai dengan peraturan perundang-undangan Republik Indonesia, termasuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah

IX. Information Security Requirements

Persyaratan Keamanan Informasi

9.1. Physical Security

Documents, devices, and identification materials must be stored securely, and access to office facilities and filing areas must be restricted.

9.2. Digital Security

Secure passwords, two-factor authentication where applicable, encryption of sensitive data, and prohibition of unauthorized software are mandatory security measures.

9.3. Device and System Use

Use of organization-approved devices and cloud platforms is required. Lost or stolen devices must be reported immediately. Use of personal devices for storing organizational data is prohibited unless expressly authorized.

9.4. Keamanan Fisik

Dokumen, perangkat, dan identitas harus disimpan dengan aman, dan akses ke ruang kantor serta area arsip harus dibatasi.

9.5. Keamanan Digital

Penggunaan kata sandi yang kuat, autentikasi dua faktor (apabila tersedia), enkripsi data sensitif, dan larangan pemasangan perangkat lunak tidak sah merupakan langkah wajib keamanan.

9.6. Penggunaan Perangkat dan Sistem

Penggunaan perangkat dan platform cloud yang disetujui organisasi diwajibkan. Kehilangan atau pencurian perangkat harus segera dilaporkan. Penggunaan perangkat pribadi untuk menyimpan data organisasi dilarang kecuali telah mendapatkan izin.

X. Rights of Data Subjects

Hak-Hak Pemilik Data

Data subjects have the right to:

- receive information regarding the use of their personal data,
- request access to their data,
- request correction or updating of inaccurate or incomplete data,
- request deletion where legally permissible, and
- withdraw consent when applicable.

Pemilik data berhak untuk:

- menerima informasi mengenai penggunaan data pribadi mereka,
- meminta akses terhadap data mereka,

- meminta perbaikan atau pembaruan,
- meminta penghapusan apabila diperbolehkan oleh hukum, dan
- menarik persetujuan apabila berlaku.

XI. Data Breach Management

Penanganan Pelanggaran Data

11.1. Reporting

Any suspected or confirmed data breach must be reported immediately to the Data Protection Focal Point and through the official reporting channel: **report@indohumlog.org**

11.2. Investigation

Indonesia Humanitarian Logistics Lab will investigate, mitigate risks, notify affected individuals when necessary, and take appropriate corrective action.

11.3. Documentation

All breaches must be documented for accountability, organizational learning, and future prevention.

11.4. Pelaporan

Setiap dugaan atau konfirmasi pelanggaran data harus segera dilaporkan kepada Penanggung Jawab Perlindungan Data dan melalui kanal resmi: **report@indohumlog.org**

11.5. Investigasi

Indonesia Humanitarian Logistics Lab akan melakukan investigasi, mengurangi risiko, memberi pemberitahuan kepada pihak terdampak bila diperlukan, dan melakukan tindakan korektif.

11.6. Dokumentasi

Seluruh pelanggaran harus dicatat untuk akuntabilitas organisasi, pembelajaran, dan pencegahan di masa mendatang.

XII. Data Protection Focal Point

Penanggung Jawab Perlindungan Data

The designated focal point is responsible for:

- overseeing compliance,
- responding to data-related inquiries,
- coordinating investigations,
- maintaining relevant documentation, and
- leading mandatory staff training on data protection and information security.

Penanggung jawab bertugas untuk:

- mengawasi kepatuhan,
- menanggapi pertanyaan terkait data,

- mengoordinasikan investigasi pelanggaran,
- memelihara dokumentasi yang relevan, dan
- memimpin pelatihan wajib mengenai perlindungan data dan keamanan informasi.

XIII. Training and Compliance

Pelatihan dan Kepatuhan

All individuals handling personal or organizational data must complete mandatory data protection training.

Failure to comply with this Policy may result in disciplinary action or termination of contract.

Seluruh individu yang menangani data pribadi atau informasi organisasi wajib mengikuti pelatihan perlindungan data.

Ketidakpatuhan terhadap kebijakan ini dapat mengakibatkan tindakan disipliner atau pemutusan hubungan kerja atau kontrak.

XIV. Relationship with Other Policies

Hubungan dengan Kebijakan Lain

This Policy complements but does not replace the following policies of Indonesia Humanitarian Logistics Lab:

- Whistleblower Policy
- Safeguarding Policy
- Prevention of Sexual Exploitation, Abuse and Harassment Policy
- Code of Conduct
- Procurement Guidelines
- Human Resources Management Guidelines

In the event of any inconsistency, the standard providing higher protection to data subjects shall prevail.

Kebijakan ini melengkapi, tetapi tidak menggantikan, dokumen berikut:

- Kebijakan Whistleblower
- Kebijakan Perlindungan dan Pencegahan Risiko Kekerasan
- Kebijakan Pencegahan Eksploitasi, Kekerasan, dan Pelecehan Seksual
- Kode Etik
- Pedoman Pengadaan
- Pedoman Pengelolaan Sumber Daya Manusia

Apabila terdapat ketidaksesuaian, standar yang memberikan perlindungan lebih tinggi bagi pemilik data akan berlaku.

XV. Legal Precedence in Case of Dispute

Keberlakuan Hukum dalam Hal Perselisihan

In the event of a dispute, discrepancy, or differing interpretation between the English and Indonesian versions of this Policy, **the Indonesian version** shall prevail and be considered the legally binding reference.

Interpretation of this Policy shall follow the laws and regulations of the Republic of Indonesia and the governance principles of Indonesia Humanitarian Logistics Lab.

Apabila terjadi perselisihan, perbedaan tafsir, atau ketidaksesuaian antara versi Bahasa Inggris dan Bahasa Indonesia dari kebijakan ini, maka **versi Bahasa Indonesia** dianggap sebagai rujukan utama yang mengikat secara hukum.

Penafsiran kebijakan ini harus mengikuti peraturan perundang-undangan Republik Indonesia serta prinsip tata kelola Indonesia Humanitarian Logistics Lab.

XVI. Review and Amendment

Peninjauan dan Perubahan

This Policy will be reviewed at least once every two years, or sooner if required due to regulatory changes, risk considerations, or organizational development.

Amendments may be approved only by the Chairperson of Indonesia Humanitarian Logistics Lab.

Kebijakan ini ditinjau sedikitnya setiap dua tahun atau lebih cepat apabila diperlukan akibat perubahan regulasi, pertimbangan risiko, atau perkembangan organisasi.

Perubahan hanya dapat disetujui oleh Ketua Indonesia Humanitarian Logistics Lab.

XVII. Entry into Force

Ketentuan Berlaku

This Policy enters into force on 1 January 2026 and is binding upon all individuals associated with Indonesia Humanitarian Logistics Lab.

Kebijakan ini berlaku mulai 1 Januari 2026 dan mengikat seluruh individu yang terhubung dengan Indonesia Humanitarian Logistics Lab.

Acknowledgment (Statement of Understanding and Compliance)

Pernyataan Pemahaman dan Kepatuhan

I, the undersigned, hereby declare that I have read, understood, and agreed to all provisions contained in the Data Protection and Information Security Policy of Indonesia Humanitarian Logistics Lab. I acknowledge that compliance with this Policy is mandatory for all individuals handling personal data or organizational information, and I fully understand the administrative and disciplinary consequences arising from any violation.

I further commit to protecting all personal data and organizational information in accordance with the principles of legality, transparency, integrity, confidentiality, and accountability, and to performing all duties with professionalism and responsibility.

Note:

The signatory may choose to sign either the Indonesian or the English version of this statement. One signed version shall be considered valid and binding for administrative purposes.

Full Name: _____
Position / Title: _____
Signature: _____
Date: _____

Saya yang bertanda tangan di bawah ini menyatakan bahwa saya telah membaca, memahami, dan menyetujui seluruh ketentuan dalam Kebijakan Perlindungan Data dan Keamanan Informasi Indonesia Humanitarian Logistics Lab. Saya memahami bahwa kepatuhan terhadap kebijakan ini bersifat wajib bagi setiap individu yang menangani data pribadi atau informasi organisasi, serta menyadari sepenuhnya konsekuensi administratif dan disipliner dari setiap pelanggaran.

Saya juga berkomitmen untuk melindungi seluruh data pribadi dan informasi organisasi sesuai dengan prinsip legalitas, transparansi, integritas, kerahasiaan, dan akuntabilitas, serta melaksanakan tugas dengan profesionalisme dan tanggung jawab.

Catatan:

Penandatanganan dapat memilih untuk menandatangani versi Bahasa Indonesia atau versi Bahasa Inggris. Satu versi yang telah ditandatangani dianggap sah dan mengikat untuk kepentingan administratif.

Nama Lengkap: _____
Jabatan: _____
Tanda Tangan: _____
Tanggal: _____