

DATA PROTECTION POLICY

Introduction

PT BTI Indo Tekno, the registered company of BTI Defence is committed to the protection of personal data and upholds the highest standards of privacy and security in compliance with Indonesia's regulations. This detailed policy document outlines our steadfast principles and comprehensive responsibilities related to the management, use, storage, and disclosure of personal data, guaranteeing compliance with national laws and fostering trust among our stakeholders.

Scope and Legal Foundation

This Privacy and Data Protection Policy is crafted in strict accordance with the legal framework provided by the "Law of The Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions," as amended by the "Law of The Republic of Indonesia Number 1 of 2024 dated 02 January 2024," including but not limited to:

- Article 30 Sections (1) and (2) jo. Article 46.
- "Regulation of The Minister of Communications and Informatics Number 20 of 2016 concerning Data Protection in Electronic System."
- "Law of The Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection," specifically encompassing Articles 16, 20, 21, 69, and 70.

This policy is pertinent to all operational levels and personnel within PT BTI Indo Tekno, covering the entirety of personal data processes, whether they are stored electronically, on paper, or transmitted by the company, across all forms of media.

Definitions

- Personal Data: Personal identity data such as names, addresses, telephone numbers, birth dates, etc.
- Sensitive Data: Confidential data such as bank account details, medical records, biometric data, genetic data, etc.
- Data Owner: The individual and/or organization that owns the Personal and/or Sensitive Data collected, stored, or processed by BTI Defence.
- Data Processing: All forms of data handling such as collection, use, storage, transfer, modification, or deletion.

Data Protection Principles

The Data Owner must comply with BTI Defence's strategies and technical measures in providing high-level protection and security of personal data against accidental or unlawful destruction or alteration, theft, accidental loss, unauthorized disclosure or access, and any other form of unlawful or improper data processing. Protection of personal data is an integral part of BTI Defence's business operations to protect the rights of the Data Owner. These business activities include management policies, role and responsibility allocation, support or backup measures, security actions, policies for data deletion or destruction, and cybersecurity policies.

Rights of Data Subjects

Individuals are entitled to:

- Access their personal data stored by our company.
- Request rectification or deletion of inaccurate or incomplete data.
- Object to the processing of their personal data under certain conditions.
- Impose restrictions on the processing of their personal data.
- Seek the portability of their data to another service provider.
- Withdraw consent to data processing at any point, which does not impact the legality of any processing conducted prior to the withdrawal of consent.

Data Collection Practices

When BTI Defence and/or its legitimate partners receive personal or confidential data from the Data Owner, BTI Defence will:

- Inform the Data Owner about the purposes of data collection, the necessity of use, to whom the data will be communicated, and the duration of storage;
- Maintain the confidentiality and security of personal data, and only disclose such data to business partners or public authorities in accordance with applicable laws;
- Establish additional data protection measures and/or disclosure limits at the request of the Data Owner; and
- Obtain the Data Owner's consent to process the data, share it with affiliate companies within the BTI Defence Group, and official partners (such as payroll, insurance, or pension program providers).

Usage of Data

BTI Defence will not use personal information of the Data Owner without consent or if not permitted by law. Therefore, BTI Defence will only process personal information if there is a basis (i.e., consent or law), such as:

- Contract performance: when the use of the Data Owner's personal information is necessary to fulfill BTI Defence's obligations under the contract;
- Legal obligation: when BTI Defence is required to use personal data to comply with legal obligations, such as keeping data for tax purposes or providing information to public bodies or law enforcement agencies;
- Legitimate interest: BTI Defence will use personal data if it is in the legitimate interest of the company, provided that this does not override the interests and freedoms of the Data Owner;
- Vital interests: if the use of personal data is necessary to protect the vital interests of the Data Owner or another individual;
- Public interest: when personal data is needed for a task carried out for the public interest; or
- Consent of the Data Owner: in some cases, aside from contractual reasons, BTI Defence will ask for specific authorization to use some personal information based on the Data Owner's consent. The Data Owner can withdraw their consent at any time by contacting BTI Defence.

Data Security Measures

Robust security measures are in place to protect personal data from unauthorized access, alteration, disclosure, or destruction. This comprehensive security approach includes advanced technological solutions, stringent physical security measures, and rigorous organizational protocols.

Data Breach Notification Protocol

Should a data breach occur, PT BTI Indo Tekno is committed to promptly notifying all relevant authorities and the impacted individuals, in line with the obligations under Indonesian law.

Third-Party Data Sharing and Disclosure

We do not share personal data with third parties except under legal compulsion or with the explicit consent of the data subject, ensuring full transparency and control for individuals over their personal data.

Policy Compliance and Enforcement

PT BTI Indo Tekno actively monitors, reviews, and updates this policy to stay compliant with the latest legal requirements and best practice guidelines. We address any breaches of this policy with the utmost seriousness, potentially leading to stringent disciplinary actions to prevent recurrence.