PRIVACY STATEMENT

BIT B.V.
Version: 17 April 2025

1 Definitions

1.1 Legal Basis

The foundation on which data is processed. This may include consent, vital interests, legal obligation, performance of a contract, public interest, or legitimate interest.

1.2 Legitimate Interest

A balancing of the interests of BIT and the interests of the individuals whose personal data is being processed.

2 Principle

Your privacy is respected by BIT. The principles of privacy-by-design and privacy-by-default are adhered to. Unless necessary for the provision of services to you, no attempt is made to identify personal data to a specific natural person. Except in cases of legal obligation or where sharing is essential for service delivery, BIT will never sell, rent, or otherwise share your personal data with third parties. BIT does not transfer your data to processors located outside the European Union. No automated decision-making is performed based on your data, nor is profiling of natural persons conducted.

3 Rights

You are the owner of your personal data. This means you also have rights concerning this data, even when it is processed by BIT. The rights you may exercise are outlined below. You can contact BIT to invoke any of these rights. The rights you may exercise include:

- Right of access: you may request access to the personal data processed by BIT about you. Most of your personal data can be viewed by you via BIT's portal. You will need an account for this portal to access your data.
- Right to rectification: you may request correction of personal data processed by BIT if it is inaccurate.
- Right to data portability: you may request the personal data processed by BIT in a machine-readable format, enabling you to transfer services provided by BIT to another provider.
- Right to erasure: you may request the deletion of personal data processed by BIT if you withdraw your consent and no other legal basis for processing remains.
- Right to object: you may object to the processing of your personal data by BIT. Based on your objection and BIT's interests, it will be assessed whether processing can be ceased or modified.
- Right to lodge a complaint: you may file a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) if you believe BIT is not handling your personal data appropriately. Complaints can be submitted via the AP's website.

4 Contact Information

If you wish to exercise one or more of the rights described in this statement, please contact BIT, the data controller:

BIT B.V.
Subject: processing personal data
PO Box 536
6710 BM Ede
The Netherlands
T: +31 318 648 688
E: info@bit.nl

If you have any questions about the processing of your data, this privacy statement, or if you wish to report a data breach, please contact the Data Protection Officer (DPO) of BIT. This officer is registered with the Dutch Data Protection Authority under AP DPO number FG002803. The contact details of the officer are:

BIT B.V.
Attn.: Data Protection Officer
PO Box 536
6710 BM Ede
The Netherlands
T: +31 318 648 688
E: dpo@bit.nl

5 Security

BIT has implemented the following general security measures to ensure the safety and availability of your data:

- **Flooding and water damage:** data is stored in data centers located at least 6 meters above sea level (NAP), equipped with water detection systems and water pumps connected to emergency power supplies.
- **Lightning strikes:** lightning protection systems installed and certified according to NEN standard 1014, class LP4, for data centers and offices.
- **Fire:** fire detection systems (checked monthly, fully tested annually in cooperation with maintenance partners), automatic alerts to the RAC, tailored emergency response plans with the fire department, gas extinguishing systems (checked monthly, fully tested annually) for each server room in the data centers, a sufficient number of emergency response officers (BHV), certified fire alarm system managers, and quarterly evacuation drills.
- **Power outage:** N+1 generators for the BIT-2A data center, N+1 generators for the BIT-2BCD data center, N generator for BIT-1, A and B-side UPS systems per server room, power redundancy extended to each rack, monthly load testing of all generators, and UPS support for office locations.
- **Burglary:** security zoning, electric fencing, intrusion detection and alarm systems at all premises, armed monitoring, video surveillance, two independent security services, certified according to VEB Security Class 4*.
- **Climate control:** three building management systems (BMS) – one for BIT-1, one for BIT-2A, and one for BIT-2BCD – maintain proper temperature and humidity in the server rooms, with cooling and humidification implemented at a minimum of N+1 redundancy.
- **Cabling (interference):** cabling in offices and server rooms is routed through cable ducts; in server rooms, cables run under the raised computer floors in two separate ducts: one for power and fiber-optic cables, and one for UTP network cables. Heavy connections (cooling and UPS systems) are routed through separate ducts in the server rooms.
- **Network redundancy:** network equipment is distributed across BIT-1 and BIT-2 locations, with redundancy in routers, switches, internal and external connections (multiple links to transit providers and major European Internet Exchanges), and geographically separated routes between BIT-1 and BIT-2, between BIT-1 and a PoP in Amsterdam, and between BIT-2 and another PoP in Amsterdam. The entire network is based on dynamic routing, allowing automatic rerouting of traffic in case of component failures.
- **Storage:** fully redundant storage, geographically separated data storage across BIT-1 and BIT-2, data encryption both in transit and at rest.
- **Backup:** fully redundant storage infrastructure. Backup storage runs on separate hardware from the production environment, with encryption in transit and at rest.
- **Load balancing:** many services are offered with standard load balancing. For most other services, load balancing is optionally available. Load balancers and servers for load-balanced services are geographically separated between BIT-1 and BIT-2.
- **Logical access:** enforced password policy, access control lists for IP-based access to BIT information systems, role-based access control (RBAC), VPN with multi-factor authentication, firewalls, centralized logging of BIT systems, and detection systems for certain unauthorized changes.
- **Organizational:** ISO 27001 and NEN 7510 certification across the entire range of services, confidentiality obligations for employees and third parties, certificate of conduct (VOG) requirement for all staff, designated security and privacy officers within the organization, security awareness training for all employees, and an encryption policy for sensitive information.

You can find a more detailed overview of the specific security measures taken for each type of data processing activity below.

6 Processing Register

The processing register specifies the processing activities for which BIT acts as the data controller. It includes:

- The purpose of the processing.
- The legal basis on which the processing is conducted.
- In the case of consent as the legal basis, the consequences of withdrawal of that consent.
- The type (category) of personal data being processed.
- The data subjects (owners) of that data.
- The recipients of the data and/or parties who may access it.
- The data retention period.
- The methods used to secure the data.

BIT processes more personal data than what is included in this register. However, for those processing activities, BIT acts solely as the data processor and not the data controller. For any questions regarding such processing activities, please contact the respective data controller.