PRIVACY STATEMENT

PRIVACY STATEMENT BIT B.V. – VERSION 2021-06-15

Definitions
Legal base
The base on which data is processed. That can be consent, vital interests, legal obligation, execution of contract, general interest or legitimate interest.

Legitimate interest
Trade-off between the interest of BIT and the interests of the client whose data will be processed.

Principle
BIT respects your privacy. The privacy-by-design and the privacy-by-default principles are both enforced. As far as it is not vital for the services we provide for you, it will not be attempted to identify personal data to a specific individual. With the exception of legal obligations or in cases that require sharing for servicing purposes, BIT will never sell, rent or otherwise share your personal data with others. BIT does not share your data with processors outside the European Union. Except for orders placed for Untangle products. No automated decisions will be made and no profiling of individuals will be done based on your data.

Rights
You are the owner of your own personal data. This means that you also have rights over this data, even if they are processed by BIT. The rights that you can claim, are listed below. You can always contact BIT about these rights. The rights you can claim are:

* Right of access; you can request access to your personal data processed by BIT. In BIT's portal you can access (almost) all of your personal data. You need an account to access this portal and your data.
* Right of rectification: you can change the personal data processed by BIT if they are incorrect (or have them changed).
* Right of transfer: you can request the personal data processed by BIT in a 'machine-readable' format so you can transfer the services provided by BIT to another supplier.
* Right of removal: you can remove the personal data processed by BIT if you withdraw your consent for processing and when there is not other legal base for the processing of your data (or have them removed).
* Right of objection: you can object against the processing of your personal data by BIT. Based on your objection and the interest of BIT, there will be an assessment on whether the processing needs to be stopped or altered.
* Right to submit a complaint: you can file a complaint the Dutch Data Protection Authority (AP) if you feel that BIT is not handling your personal data correctly. You can file your complaint on the AP website.

Contact details
If you wish to exercise one or more of the rights described in this statement, you can 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 questions about the processing of your data, this privacy statement or if you want to report a data breach, please contact BIT's Data Protection Officer (FG). This officer is registered with the Dutch Data Protection Authority with AP FG number FG002803. The contact details of this official 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

Security
BIT has taken the following generic security measures to keep your data safe and available:
* Flooding and water damage: data storage in data centers that are at least 6 meters above NAP, water detection and water pumps connected to emergency power supplies.
* Lightning: lightning protection installation installed and certified in accordance with the NEN standard 1014 class LP4, for data centers and offices.
* Fire: fire detection systems (monthly checks, annual tests with maintenance party), reporting to the RAC, customised plan with fire brigade, gas extinguishing installation (monthly checks, annual tests with maintenance party) for the data centers per server room, a large number of in-house emergency officers, a large number of fire alarm system administrators and quarterly evacuation exercises.
* Power failure: generators N+1 for BIT-2A data center, generators N+1 for BIT-2BVD data center, generator N for BIT-1, UPS sets with A and B side per server room, power redundant to every rack, monthly loaded test of all generators and offices also equipped with UPS.
* Burglary: zoning, electric fence, burglary detection and alarm system on all premises, switch-on monitoring, camera surveillance, two independent surveillance services, VEB (security class 4*) certified.
* Climate: three building control systems ('GBS'), one for BIT-1, one for BIT-2A and one for BIT-2BCD which ensure the right temperature and humidity in the server rooms, minimum setup of N+1 cooling and N+1 humidification.
* Cables (interference): cables are located in cable ducts in the offices and server rooms, in the server room there are two ducts beneath the raised computer floor: one for power and fibre optic cables and one for UTP network cables, heavy connections (cooling and UPSs) in the server room in separate cable ducts.
* Network redundancy: network equipment is spread over locations BIT-1 and BIT-2, redundancy in the fields of routers, switches, internal and external connections (multiple connections to transit suppliers and all large European Internet Exchanges), 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 where different paths are automatically selected in case of failure in components in order to lead the traffic around the failing components.
* Storage: fully redundant storage. Storage runs on different software than the production storage.
* Backup: fully redundant storage. Storage runs on hardware other than the production storage.
* Load balancing: a large number of services are available with standard load balancing. For most other services, load balancing is optionally available. The load balancers and servers for the load balanced services are located in geographically separated buildings BIT-1 and BIT-2.
* Logical access: mandatory password policy, access lists for access of IP addresses to BIT's information systems, RBAC, VPN with 2 factor authentication, firewalls, central logging of BIT information systems and detection systems for certain unauthorised changes.
* Organisational: ISO 27001 and NEN 7510 certification on the entire range of services, confidentiality agreements for all employees and engaged third parties, obligation of police clearance certificate for all employees, a security officer within the organisation, security awareness trainings for all employees, encryption policy for sensitive information.

The overview below provides more specific information on the measures taken to protect your personal data per processing action.

Processing register
The following register lists the processing actions of personal data for which BIT is the data controller. It states:

– The purpose of the processing action.
– Which legal base is applicable to the processing action.
– In case of the legal base of consent: the consequences of withdrawing permission.
– The type (category) of personal data that is being processed.
– The involved party (owner) of the data.
– The receivers of the data and/or who can access the data.
– The retention period of the data.
– The way in which the data is protected.

BIT processes more personal data than mentioned in this register. However, BIT is not the data controller for those processing actions, merely the processor. Questions about these processing actions can be directed to the data controller.

In the event of conflict between the English version and the Dutch version of this document, the Dutch version prevails.