

## PRIVACY STATEMENT

### PRIVACY STATEMENT BIT B.V. – VERSION 2018-05-25

#### 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. 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](mailto: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](mailto: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.

Registration	Purpose	Legal base	Consequences withdrawing consent	Category data	Category involved parties	Category receivers	Retention period	Security
Tickets	- Recording client orders - Recording orders to suppliers	Contract		- name and address details - contact information - payment details - IP addresses - URI's - MAC-addresses	- clients - suppliers - prospects - employees - clients' relations	- employees - clients ( <i>own data</i> ) - suppliers ( <i>own data</i> )	No limitation <sup>3</sup>	- access list - locally hosted system - login required - messages to relations or internally classified - TLS only
Abuse registration	Registration and processing of complaints on abuse by clients	Contract		- name and address details - contact information - IP-addresses - URI's	clients	- employees - clients ( <i>own data</i> )	No limitation <sup>4</sup>	- locally hosted system - login required - role-based access - TLS only
CIOT registration	Legal provision of data	Legal obligation		- name and address details - IP addresses - date - time - duration - email addresses	clients	CIOT	None	- encrypted file - TLS only
Role based email	Mail communication on role-addresses of BIT	Contract		- name and address details - contact information - payment details - IP addresses - URI's - MAC addresses	- clients - suppliers - prospects - employees - clients' relations - third parties	- employees - clients ( <i>own data</i> ) - suppliers ( <i>own data</i> ) - third parties <sup>2</sup>	No limitation <sup>5</sup>	- access list - locally hosted system - login required - role-based access to mailboxes - TLS only
Mailbox employees	Personal/direct mail communication of BIT employees	Contract		- name and address details - contact information - payment details - IP addresses - URI's - MAC addresses	- clients - suppliers - prospects - employees - clients' relations - third parties	- employees - clients ( <i>own data</i> ) - suppliers ( <i>own data</i> ) - third parties <sup>2</sup>	No limitation <sup>5</sup>	- locally hosted system - login required - encryption for confidential information - TLS only
Relation management	Registration contact information	- Contract (for clients/suppliers) - Consent (for employees, prospects and relations)		- name and address details - contact information - payment details	- clients - suppliers - prospects - employees - clients' relations - suppliers' relations	- employees - clients ( <i>own data</i> ) - suppliers ( <i>own data</i> )	No limitation <sup>6</sup>	- access list - locally hosted system - login required - role-based access - TLS only
IP addresses	Registration use of IP addresses	Contract		- name and address details - IP addresses - MAC addresses	clients	- employees - RIPE	Duration of service	- access list - locally hosted system - login required - messages to relations or internally classified - TLS only

Camera images	Security of access	Legitimate interest, meaning security of the property and data of clients and BIT		Personal, external characteristics	Visitors BIT premises and grounds	employees	1 week	<ul style="list-style-type: none"> <li>- access list</li> <li>- internally hosted system</li> <li>- login required for viewing of images</li> </ul>
Biometric access	Security of access	Contract		Biometric data	visitors BIT premises with independent access	employees	Duration of service	<ul style="list-style-type: none"> <li>- access list</li> <li>- internally hosted system</li> <li>- login required</li> <li>- role-based access</li> </ul>
ANPR	Security of access	Consent ( <i>with identification of known number plates</i> ) Legitimate interest, meaning recognition of known number plates only possible by scanning all number plates	If there is no consent for processing the number plate, the user of the number plate cannot pass the gates on the grounds of BIT without access pass or use of the intercom.	<ul style="list-style-type: none"> <li>- pictures of cars</li> <li>- logging of number plate, time and location</li> <li>- identification of visitor based on known number plates</li> </ul>	visitors BIT grounds with car	employees	2 years	<ul style="list-style-type: none"> <li>- access list</li> <li>- internally hosted system</li> <li>- login required</li> <li>- role-based access</li> </ul>
Access control system	Security of access	Contract		<ul style="list-style-type: none"> <li>- logging of name, time and location</li> <li>- identification of persons based on access pass or biometric data</li> </ul>	visitors premises of BIT with independent access	employees	1 year	<ul style="list-style-type: none"> <li>- access list</li> <li>- internally hosted system</li> <li>- login required</li> <li>- role-based access</li> </ul>
Access registration	Security of access	Contract		<ul style="list-style-type: none"> <li>- name of registered person</li> <li>- number plate of registered person</li> <li>- proof of identification from registered person</li> <li>- company name</li> <li>- date, time, duration and location of registration</li> <li>- name of notifier</li> </ul>	visitors premises and grounds of BIT	<ul style="list-style-type: none"> <li>- employees</li> <li>- clients (<i>data about own company</i>)</li> </ul>	Current year plus previous year	<ul style="list-style-type: none"> <li>- access list</li> <li>- login required</li> <li>- locally hosted system</li> <li>- role-based access</li> <li>- TLS only</li> </ul>
Phone conversations	Registration communication	Legitimate interest, meaning providing the opportunity to resume and the opportunity to remove possible doubt about unclear orders		<ul style="list-style-type: none"> <li>- name</li> <li>- phone number</li> <li>- audio recording (<i>only outside office hours</i>)</li> <li>- date, time and duration of conversation</li> </ul>	<ul style="list-style-type: none"> <li>- people calling to BIT</li> <li>- people receiving calls from BIT</li> </ul>	employees	1 month	<ul style="list-style-type: none"> <li>- access list</li> <li>- login required</li> <li>- locally hosted system</li> <li>- role-based access</li> <li>- TLS only</li> </ul>

Staff files	Staff administration	Legal obligation		<ul style="list-style-type: none"> <li>- name and address details</li> <li>- salary data</li> <li>- assessments</li> <li>- copy ID</li> <li>- police clearance certificate</li> <li>- labour agreement</li> <li>- copy diplomas</li> </ul>	employees	<ul style="list-style-type: none"> <li>- employees administration</li> <li>- accountant (<i>salary data</i>)</li> <li>- management</li> <li>- tax authority (<i>salary data</i>)</li> </ul>	<ul style="list-style-type: none"> <li>- duration labour agreement, plus 3 months</li> <li>- information relevant for wage tax 7 years</li> </ul>	<ul style="list-style-type: none"> <li>- closed cabinet in secured room</li> <li>- login required for software</li> <li>- locally hosted system</li> <li>- TLS only</li> </ul>
Job applications	Recruitment	Consent	If there is no consent for the processing of personal data, the application cannot be accepted.	<ul style="list-style-type: none"> <li>- NAW</li> <li>- job history</li> <li>- education</li> <li>- several personal data</li> </ul>	Job applicants	Management	6 months	<ul style="list-style-type: none"> <li>- locally hosted system (<i>via email</i>)</li> <li>- login required (<i>via email</i>)</li> <li>- encryption for confidential information (<i>via email</i>)</li> <li>- TLS only (<i>via email</i>)</li> </ul>
Billing	Billing	Legal obligation		<ul style="list-style-type: none"> <li>- name and address details</li> <li>- payment details</li> <li>- specification products and services</li> </ul>	Clients	<ul style="list-style-type: none"> <li>- employees</li> <li>- clients</li> <li>- debt collection agency</li> <li>- accountant</li> </ul>	7 years	<ul style="list-style-type: none"> <li>- TLS preferred mailing</li> <li>- sent in closed envelopes (to <i>customers</i>)</li> <li>- to debt collection agency via webportal with TLS</li> <li>- locally hosted system with access list, login required, role-based access, TLS only</li> </ul>
Mechanics registration	<ul style="list-style-type: none"> <li>- Security of access</li> <li>- Recording awareness BIT house rules</li> </ul>	Consent	If there is no consent for the processing of personal data, no work can be done at BIT.	<ul style="list-style-type: none"> <li>- name</li> <li>- company name</li> <li>- contact information</li> <li>- ID number</li> <li>- if relevant: enforced sanctions</li> </ul>	Employees of suppliers	Employees	No limitation <sup>7</sup>	Cabinet in secured room
Websites	<ul style="list-style-type: none"> <li>- Securing personal data (<i>at BIT websites behind a login</i>)</li> <li>- Collecting visitor statistics (<i>all BIT websites</i>)</li> </ul>	Consent ( <i>for websites behind login</i> ) Legitimate interest, meaning guaranteeing proper functioning of the service	If there is no consent for the processing of the login credentials, the personal data cannot be accessed.	<ul style="list-style-type: none"> <li>- IP address</li> <li>- referrer</li> <li>- browser details</li> <li>- login credentials</li> </ul>	Visitors	<ul style="list-style-type: none"> <li>- employees</li> <li>- clients (<i>own login credentials</i>)</li> </ul>	<ul style="list-style-type: none"> <li>- 7 days (<i>logs</i>)</li> <li>- no limitation (<i>gathered statistics</i>)</li> </ul>	<ul style="list-style-type: none"> <li>- access list</li> <li>- locally hosted system</li> <li>- login required</li> <li>- role-based access</li> <li>- TLS only</li> </ul>
Mailing services	<ul style="list-style-type: none"> <li>- Securing personal data (<i>with access to mailing services</i>)</li> <li>- Collecting logging for problem solving</li> </ul>	Contract ( <i>with login mailing service</i> ) Legitimate interest, meaning guaranteeing proper functioning of the service		<ul style="list-style-type: none"> <li>- IP addresses of sender, addressee and reader</li> <li>- email addresses of sender and receiver</li> <li>- login credentials</li> </ul>	<ul style="list-style-type: none"> <li>- users of the mailing service</li> <li>- third parties</li> </ul>	<ul style="list-style-type: none"> <li>- employees</li> <li>- clients (<i>own login credentials</i>)</li> </ul>	7 days	<ul style="list-style-type: none"> <li>- access list</li> <li>- locally hosted system</li> <li>- login required</li> <li>- role-based access</li> <li>- TLS only</li> </ul>

Webhosting	<ul style="list-style-type: none"> <li>- Securing personal data (with access to hosting service)</li> <li>- Collecting logging for problem solving</li> <li>- Collecting visitor statistics</li> </ul>	Contract (with login hosting service) Legitimate interest, meaning guaranteeing proper functioning of the service		<ul style="list-style-type: none"> <li>- IP address</li> <li>- referrer</li> <li>- browser details</li> <li>- login credentials</li> </ul>	visitors	<ul style="list-style-type: none"> <li>- employees</li> <li>- clients (own login credentials and logging own websites)</li> </ul>	<ul style="list-style-type: none"> <li>- 7 days (logs)</li> <li>- no limitation (gathered statistics)</li> </ul>	<ul style="list-style-type: none"> <li>- access list</li> <li>- locally hosted system</li> <li>- login required</li> <li>- role-based access</li> <li>- TLS only</li> </ul>
VOIP	<ul style="list-style-type: none"> <li>- Billing</li> <li>- Insight calling history</li> </ul>	Legal obligation		<ul style="list-style-type: none"> <li>- phone number</li> <li>- date, time and duration of call</li> </ul>	<ul style="list-style-type: none"> <li>- people calling a client</li> <li>- people receiving a call from a client</li> </ul>	<ul style="list-style-type: none"> <li>- employees</li> <li>- clients (own data)</li> <li>- VOIP supplier</li> </ul>	1 year	<ul style="list-style-type: none"> <li>- access list</li> <li>- locally hosted system</li> <li>- login required</li> <li>- role-based access</li> <li>- TLS only</li> </ul>
Internet access on client location	Providing service	Contract		<ul style="list-style-type: none"> <li>- name and address details</li> <li>- contact information</li> <li>- VLAN number</li> <li>- client number (for mobile internet)</li> <li>- login credentials</li> </ul>	Clients	<ul style="list-style-type: none"> <li>- employees</li> <li>- provider infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>- duration of service</li> <li>- no limitation <sup>7</sup></li> </ul>	<ul style="list-style-type: none"> <li>- access list</li> <li>- locally hosted system</li> <li>- login required</li> <li>- role-based access</li> <li>- TLS only</li> <li>- TLS preferred email (for mobile internet)</li> </ul>
Software distribution	Providing service	Contract		<ul style="list-style-type: none"> <li>- name and address details</li> <li>- contact information</li> <li>- license information</li> </ul>	<ul style="list-style-type: none"> <li>- clients</li> <li>- resellers</li> </ul>	<ul style="list-style-type: none"> <li>- employees</li> <li>- clients</li> <li>- vendors</li> <li>- resellers</li> </ul>	No limitation <sup>7</sup>	<ul style="list-style-type: none"> <li>- access list</li> <li>- locally hosted system</li> <li>- login required</li> <li>- role-based access</li> <li>- TLS only</li> <li>- TLS preferred email (to vendors and resellers)</li> </ul>
SSL certificates	Providing service	Contract		<ul style="list-style-type: none"> <li>- name and address details</li> <li>- contact information</li> <li>- private key</li> <li>- host names</li> </ul>	Clients	<ul style="list-style-type: none"> <li>- employees</li> <li>- clients (own data)</li> <li>- certificate authorities</li> <li>- reseller CA</li> </ul>	No limitation <sup>7</sup>	<ul style="list-style-type: none"> <li>- access list</li> <li>- locally hosted system</li> <li>- login required</li> <li>- role-based access</li> <li>- TLS only</li> </ul>

1. This column describes the consequence of not giving permission to process the personal data.
2. Third parties have access to this data if the client has requested for them to be added to email communication as receivers.
3. BIT does not (yet) have the proper classification on tickets that can discern between tickets that need to be stored for legal reasons or in the interest of the client and tickets that do not have such reasons. Additionally, in some cases the data of multiple relations is placed in one ticket (which can only be accessed by BIT employees) instead of the ticket being linked to a specific relation.
4. IP addresses change user and abuse history of an IP address is of importance for certain uses. It is therefore in the interest of a potential new user of the IP address to know the history of the IP address.
5. BIT does not (yet) have the proper classification on emails that can discern between emails that need to be stored for legal reasons or in the interest of the client and emails that do not have such reasons. Additionally, individual emails are not systematically linked to a specific relation. In some cases, the data of multiple relations is placed in one email (which can only be accessed by BIT employees).
6. Personal data of individuals with clients that we are no longer servicing, are removed after the termination of all contracts.
7. This personal data is stored in tickets and emails. See notes 3 and 5 for the lack of limitation in the retention period for this data.