DATA PROCESSING AGREEMENT GDPR

DATA PROCESSING AGREEMENT BIT B.V. – VERSION 2018-02-01

This processing agreement applies to all forms of processing of personal data that Processor performs on behalf of the Controller to whom it provides services.

Article 1: PURPOSE OF PROCESSING

1.1 Processor agrees to process personal data from Controller under the restrictions of this Processing Agreement. Processing will only take place within the framework of the purpose/purposes as described in Appendix 1, plus the purposes that are reasonably related thereto or that are determined with further consent.

1.2. The personal data that will be processed by Processor in the context of the activities as referred to in the previous paragraph and the categories of the data subjects that provide this data, are included in Appendix 1.

1.3. Processor will not process the personal data for any other purpose than established by the Controller. Controller will inform Processor of the processing purposes that are not included in this Processing Agreement.

1.4. The personal data processed on behalf of the Controller will remain the property of the Controller and/or the relevant parties involved.

Article 2: OBLIGATIONS OF PROCESSOR

2.1 With regard to the processing operations referred to in article 1, Processor will ensure compliance with relevant laws and regulations, including but not limited to the laws and regulations in the area of the protection of personal data, like the General Data Protection Regulation.

2.2. Processor will inform Controller, upon Controller's first request, of the measures taken in regard to the obligations in this Processing Agreement.

2.3. The obligations of the Processor arising from this Processing Agreement also apply to those processing the personal data on the authority of the Processor, including but not limited to employees, in the broadest sense of the word.

2.4. The Processor will immediately inform the Controller if, in his opinion, an instruction of the Controller is in conflict with the legislation referred to in subsection 1.

2.5. Processor will, if possible, provide reasonable assistance to Controller for performing data protection impact assessments (PIAs). The time spent on this will be charged to Controller by Processor.

Article 3: TRANSFER OF PERSONAL DATA

3.1 Processor can process personal data in countries within the European Union. Transfers to countries outside of the European Union are not permitted, unless the Controller gives permission to do otherwise.

3.2. Processor will report to Controller which country or countries it may concern.

Article 4: DISTRIBUTION OF RESPONSIBILITY

4.1 The authorised processing operations will be performed by employees of Processor within an automated environment.

4.2. Processor is merely responsible for the processing of the personal data included in this Processing Agreement, in accordance with the instructions of Controller and under the express (final) responsibility of Controller. Processor is expressly not responsible for other processing of personal data, including, but not limited to, the collection of personal data by Controller, processing for purposes not reported to Processor by Controller, processing by third parties and/or for other purposes.

4.3. Controller guarantees that content, use and instructions for processing of the personal data as referred to in this Processing Agreement are not illegal and do not infringe any right of third parties.

Article 5: ENGAGING THIRD PARTIES OR SUBCONTRACTORS

5.1. Processor may use third parties in the context of this Processing Agreement and will supply a list of third parties (sub-processors) to Controller upon request.

5.2. Processor will, in any case, ensure that these third parties take on, in writing, at least the same obligations as agreed upon between Controller and Processor.

5.3. Processor guarantees correct compliance with the obligations in this Processing Agreement by third parties and is responsible for all damages caused by these third parties as if it had caused the damage(s) itself.

Article 6: SECURITY

6.1 Processor will endeavour to undertake sufficient technical and organisational measures with regard to the processing of personal data against loss or any form of unlawful processing (such as unauthorised access, impairment, alteration or provision of the personal data).

6.2. Processor has taken the measures as included in the Security Protocol, which is included in Appendix 2 of this Processing Agreement. Processor may unilaterally alter the Security Protocol at any time. He will inform Controller of the alterations.

6.3. Processor does not guarantee that the security is effective under all circumstances. If an explicitly defined security measure is not included in the Processing Agreement, Processor will endeavour to provide security of a level that is, given the state of the technology, the sensitivity of the personal data and the cost of the security, not unreasonable.

6.4. Controller will only make personal data available to Processor for processing, if it has ensured that the required security measures have been taken. Controller is responsible for compliance with the measures agreed upon by Parties.

6.5. Processor works in accordance with ISO 27001/ISO 27002 and NEN 7510, which are considered to comply with the security requirements in light of the current state of technology.

Article 7: REPORTING

7.1. Controller is responsible for reporting a security and/or data leak (meaning: a breach in the security of personal data that leads to a chance for negative consequences, or has negative consequences for the protection of personal data) to the supervisor and/or parties involved at all times. To enable Controller to comply with this statutory obligation, Processor will inform Controller of the security and/or data leak within 48 hours of finding out about the leak.

7.2. Every incident must be reported, but only if the event actually occurred.

7.3. The reporting obligation includes the notification of leaks. It also includes:

- The nature of the breach in relation to personal data, where possible with reference to the categories of the affected parties and personal data registers in question and, by approach, the number of affected parties and personal data registers in questions;
- The name and contact details of the data protection officer or another contact point where more information can be obtained;
- The likely impact of the breach in relation to personal data;
- The measures that Processor proposed or took to handle the breach in relation to personal data, including, where appropriate, the measures to mitigate any adverse effects.

Article 8: HANDLING REQUESTS FROM DATA SUBJECTS

8.1 In case a data subject submits a request to execute his/her legal rights to Processor, Processor will forward the request to Controller, who will handle the request from there. Processor may inform the data subject of this.

Article 9: CONFIDENTIALITY AND PRIVACY

9.1. All personal data received by Processor from Controller and/or is collected by Processor in the framework of this Processing Agreement, is subject to a confidentiality obligation towards third parties. Processor will not use this information for any purpose other than that for which it was obtained, even if it is in such form that it cannot be traced back to the parties involved.

9.2. This confidentiality obligation is not applicable if the Controller has given express permission to provide the information to third parties, if the provision of the information to third parties is logically necessary considering the given assignment and the execution of this Processing Agreement, or if there is a legal obligation to provide the information to a third party.

Article 10: AUDIT

10.1 Processor hereby gives Controller the right to have an independent third party who is bound to confidentiality perform an audit in order to check compliance with the provisions in this Processing Agreement or Processor shall provide Controller with a third party account notification that proves that Processor is acting in compliance with the provisions in this Processing Agreement.

10.2. This audit may be performed once a year as well as in case of a concrete suspicion for abuse of personal data.

10.3. Processor will cooperate with the audit and will make all reasonably relevant information, including supporting data such as system logs, and employees available as quickly as possible.

10.4. The findings resulting from the performed audit will be assessed by Processor and may be implemented by Processor, at the discretion of Processor and in the manner that Processor sees most fit.

10.5. The cost of an audit will always be for Controller.

Article 11: LIABILITY

11.1. The liability of Processor for damage as a result of attributable shortcoming in the fulfilment of the Processing Agreement, in tort or otherwise, is limited per event (a series of consecutive incidents will be considered one event) to the compensation of direct damages, up to the amount of payment received by Processor from Controller for activities under the Processing Agreement in the month prior to the event that caused the damage.

11.2. Direct damage is exclusively understood to mean all damages consisting of:

- Damage caused directly to property (“property damage”);
- Reasonable and demonstrable costs to urge Processor to properly comply with the Processing Agreement (again);
- Reasonable costs to determine the cause and extent of the damage insofar that it relates to the direct damage as referred to here;
- Reasonable and demonstrable costs that Controller made to prevent or limit the direct damage as referred to in this article.

11.3. The liability of Processor for indirect damage is excluded. Indirect damage is understood to mean all damage that is not direct damage, including, but not limited to, consequential losses, lost profit,

missed savings, reduced goodwill, loss due to business stagnation, damage due to non-determination of marketing objectives, damage related to the use of data or data files prescribed by Controller, or loss, mutilation or destruction of data or data files.

11.4. The exclusions and limitation referred to in this article will be cancelled if and in so far as the loss sustained is the result of intent or deliberate recklessness on the part of the management of Processor.

11.5. Unless compliance by Processor becomes permanently impossible, the liability of Processor due to imputable shortcoming in the fulfilment of the Agreement arises only if Controller immediately informs the Processor in writing of the shortcoming, where a reasonable period for the rectification of the shortcoming is determined, and Processor remains attributable to the fulfilment of its obligations after the set period. The notice of default must contain a complete and detailed description, insofar that is possible, of the shortcoming, so that Processor is given the opportunity to respond adequately.

11.6. Any claim for compensation by Controller against Processor that has not been specified and explicitly reported, shall expire in twelve (12) months after the claim arose.

Article 12: DURATION AND TERMINATION

12.1. This Processing Agreement is concluded by signing of both Parties and starts on the date of the last signature.

12.2. This Processing Agreement has been entered into for the duration as determined in the main agreement between Parties and, in the absence thereof, at least for the duration of the cooperation.

12.3. As soon as the Processing Agreement has been terminated, for what ever reason and in whatever way, the Processor will – by choice of Controller – return all original personal data and its copies to Controller, and/or delete and/or destroy all this personal data and possible copies. Aforementioned with exception of the personal data that Processor must retain in order to fulfil the statutory (storage) obligations.

12.4. Processor is entitled to revise this agreement from time to time. He will notify the Controller of all changes at least two months in advance. Controller may terminate the agreement at the end of this two month notice if they do not agree with the changes. Otherwise, the changes are considered to be approved by Controller.

Article 13: APPLICABLE LAW AND DISPUTE RESOLUTION

13.1. The Processing Agreement and its implementation are governed by Dutch law.

13.2. All disputes that may arise between the Parties in relation to the Processing Agreement shall be submitted to a competent court for the district in which the Processor is established.

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

Appendix 1: Specification of personal data, data subjects and purpose of processing

In the context of the Agreement, Processor will process the following (special) personal data on behalf of Controller:

01. _____

02. _____

03. _____

04. _____

05. _____

06. _____

07. _____

08. _____

09. _____

10. _____

It concerns the following categories of data subjects:

01. _____

02. _____

03. _____

04. _____

05. _____

It concerns processing with the purpose(s) of:

01. _____

02. _____

03. _____

04. _____

05. _____

Controller guarantees that the personal data, categories of data subjects and processing purposes described in this Appendix 1 are complete and correct and indemnifies Processor for any defects and claims that result from an incorrect representation by Controller.

Appendix 2: Security Measures

Processor has taken the following security measures:

- Flood and water damage: 6, 9 or 12 meters above Amsterdam Ordnance Datum, water detection, water pumps connected to emergency power.
- Lightning: lightning conductor installation installed and certified according to the NEN standard 1014 class LP4, for data centers and offices.
- Fire: fire detection systems (checked on a monthly basis, fully tested with maintenance party every year), reporting to the RAC, customised plan with fire brigade, gas extinguishing installation (checked on a monthly basis, fully tested with maintenance party every year) for the data centers per server room, a large number of ER officers, a large number of fire alarm system administrators, quarterly evacuation exercises.
- Power failure: generators N+1 for BIT-2A data center, generators N+1 for BIT-2BCD data center, generator N for BIT-1, UPS sets with A and B side per server room, redundant power to each rack, monthly load test of all generators, UPS in offices.
- Burglary: zoning, electric fence, intrusion detection and alarm system on all premises, switch-on monitoring, 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, these ensure the right temperature and humidity in the server rooms, at least N+1 cooling, N+1 humidification.
- Cabling (interference): cables are located in cable ducts in the office and in server rooms, in the server rooms under the raised computer floor in two ducts: one for power and fibre optic cables and one for UTP network cabling, large connections (cooling and UPSs) in separate ducts in the server room.
- Network redundancy: network equipment is spread over locations BIT-1 and BIT-2, there is redundancy in 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, and between BIT-1 and a PoP in Amsterdam and BIT-2 and another PoP in Amsterdam. The network is based on dynamic routing where the failure of components will automatically lead to another path to route the traffic around the failed components.
- Storage: full redundant storage for production and backup, geographically separated storage of data in BIT-1 and BIT-2, backup storage runs on different hardware than production storage.
- Load balancing: a large number of services is automatically load balanced, for most other services load balancing is optionally available, load balanced services have the load balancers and servers geographically separated in BIT-1 and BIT-2.
- Logical access: forced password policy, access lists for access to IP addresses on information systems of BIT, RBAC, VPN with 2-factor authentication, firewalls, central logging of BIT information system and detection systems for certain unauthorised changes.
- Organisational: ISO 27001 and NEN 7510 certification on all services, confidentiality obligation of employees and hired third parties, criminal records obligation for all employees, security officer in the organisation, security awareness training for all employees.