infobric

Data Processing Agreement

1. GENERAL

1.1 The Customer is the controller for all personal data processing using the Software, unless specified otherwise in this Agreement. Within the framework of the Services, the Supplier will process personal data on behalf of the Customer as the processor. The object of the processing, the duration, nature and purpose of the processing, the type of personal data and categories of data subject affected by the processing are described in further detail in the Appendix – Description of the processing of personal data in the Services. The Customer is liable to ensure that all such personal data processing takes place in compliance with the personal data legislation in force from time to time, including the General Data Protection Regulation (EU 2016/679) ('Applicable Legislation').

2. GENERAL OBLIGATIONS OF THE SUPPLIER

2.1 In its role as processor, the Supplier must only process personal data in accordance with written instructions from the Customer under this Agreement, and any other documented instructions given by the Customer from time to time. Other instructions may be given to the Supplier by email or on a separate form. Instructions should contain information equivalent to that in the appendix to this Personal Data Processing Agreement.

2.2 If the Supplier lacks instructions which the Supplier considers essential to carry out its assignment, the Supplier must inform the Customer without delay and await further instructions. If the Supplier finds that instructions contravene the Applicable Legislation, the Supplier must inform the Customer without undue delay. If, in such case, the Customer fails to provide further instructions to the Supplier, the Supplier must ignore the instructions and notify the Customer that it has done so. If the Customer maintains the unlawful instructions, the Supplier is entitled to terminate the Agreement prematurely as specified in the General Terms and Conditions

2.3 Notwithstanding the provisions in sub-clause 2.1 above, the Supplier is entitled to process personal data to the extent necessary to permit the Supplier to perform the obligations incumbent on the Supplier under the Applicable Legislation in force from time to time, for example to comply with orders by public authorities. However, before any such processing takes place, the Supplier must inform the Customer of the legal obligation unless mandatory legislation prevents the Supplier from providing such information.

2.4 If anyone requests information from the Supplier concerning the Customer's processing of personal data, the Supplier must refer the request to the Customer by notifying the Customer's System Administrator by email. The Supplier must not disclose personal data or other information on the processing of personal data without written instructions from the Customer. The Supplier is not entitled to represent the Customer or act on the Customer's behalf in relation to any third party, including the supervisory authority.

3. TECHNICAL AND ORGANISATIONAL MEASURES

3.1 The Supplier must take the technical and organisational measures necessary under the Applicable Legislation to protect the personal data processed in the Services and at least the technical and organisational measures specified in the security appendix to this Agreement. The Customer's prior consent is required if the Supplier wishes to make changes to the technical and organisational measures that would entail a lower level of security. The Parties agree that the technical and organisational measures taken must be subject to regular follow-up to ensure that they are appropriate to the risks associated with the processing of personal data.

3.2 At the request of the Customer, the Supplier must assist the Customer with information that the Supplier needs so that, where appropriate, the Customer is able to perform its obligations to carry out an impact assessment and prior consultation with the supervisory authorities concerned in respect of the processing that the Supplier performs on behalf of the Customer within the framework of the Services. The Supplier has prepared an impact assessment for the processing of personal data that the Supplier performs on behalf of the Customer and the Customer may receive a copy on request.

3.3 Where possible, the Supplier must assist the Customer by taking appropriate technical and organisational measures to permit the Customer to perform its obligation to respond to a request from a data subject to exercise their right under the Applicable Legislation. The Software has been designed to assist the Customer in this respect. Using special functionality, the Customer is able to manage requests from data subjects to exercise their rights under the Applicable Legislation itself.

3.4 The Supplier must ensure that access to personal data is limited only to the Supplier's staff who need access so that the Supplier is able to meet its obligations to the Customer. Moreover, the Supplier must ensure that such authorised staff observe confidentiality as specified in Clause 7.2 below through individual non-disclosure agreements.

4. PERSONAL DATA BREACHES

4.1 If a personal data breach (as defined in the Applicable Legislation) occurs, the Supplier must notify the Customer in writing via the Customer's System Administrator without undue delay after the Supplier has learned of the breach and no later than within twenty-four (24) hours in accordance with the Supplier's procedures from time to time. The notice must include information about the nature of the breach, the categories and number of data subjects and personal data items affected, the probable consequences of the breach and a description of the measures the Supplier has taken (where appropriate) to limit any negative effects of the breach to make it possible for the Customer to meet any obligation to notify the relevant supervisory authority of the personal data breach. If it is not possible, it is not necessary for all information to be provided at the same time. However, the Supplier must provide the Customer with the information as soon as it is available to

the Supplier.

4.2 If it is probable that a personal data breach entails a risk to the privacy of the data subjects, the Supplier must, to the extent possible, take appropriate remedial action to prevent or limit any negative effects of the personal data breach immediately after the Supplier became aware of the personal data breach.

5. ACCESS TO INFORMATION, ETC.

5.1 The Supplier must continually document the measures taken by the Supplier to meet its obligations under this Personal Data Processing Agreement. The Customer is entitled to receive the latest version of such documentation on request. For information on the processing of personal data within the framework of the Services, see the appendix to this Personal Data Processing Agreement.

5.2 Moreover, the Supplier must enable and help the Customer or a third party appointed by the Customer to carry out an audit, including an inspection, of the technical and organisational measures taken by the Supplier to perform its obligations under this Personal Data Processing Agreement. The Supplier must be given at least thirty (30) days' notice of any such audit. All costs of the audit must be borne by the Customer, including any costs for the Supplier's participation in the audit. The Customer must ensure that any third party that conducts the audit on behalf of the Customer observes confidentiality that is no less restrictive than that specified in Clause 7.2 below. Corresponding provisions apply to the Customer's request for an audit of a Sub-processor engaged by the Supplier in connection with the Services. See Clause 5.1 below.

6. ENGAGING SUB-PROCESSORS

6.1 The Customer hereby accepts that the subcontractors engaged by the Supplier that are specified on the website indicated by the Supplier from time to time may process personal data on behalf of the Customer in connection with the Services ('Sub-processors'). The sub-processors engaged by the Supplier at the time at which this Agreement is made are also specified in the appendix to this Personal Data Processing Agreement. The Customer also grants the Supplier general prior acceptance to engage new Sub-processors, provided that the Supplier ensures that the Sub-processors provide adequate guarantees that they will take appropriate technical and organisational measures to ensure that the processing meets the requirements of the Applicable Legislation.

6.2 The Supplier must make a personal data processing agreement with each Sub-processor. Such a personal data processing agreement must contain provisions equivalent to those in this agreement and the Applicable Legislation.

6.3 If the Supplier intends to engage a new Sub-processor, the Supplier must notify the Customer of this intention by email to the Customer's Contracts Officer. Such notice must include the Sub-processor's identity (including the full company name, corporate identity number and address), the (geographical) location at which the Sub-processor will process personal data, the type of service the Sub-processor performs and the safeguards that will be applied by the Sub-processor to protect the personal data processed. The Customer is entitled, within two (2) weeks from the date of the notice, to object to the Supplier engaging the Sub-processor to process personal data on behalf of the Customer, in which case the Supplier and the Customer must jointly attempt to reach consensus. If they are unable to do so, the Agreement may be terminated prematurely as specified in the General Terms and Conditions.

7. TRANSFER OF PERSONAL DATA OUTSIDE THE EU/EEA AND PROCESSING OUTSIDE THE EU/EEA

7.1 The Customer hereby accepts that the Supplier may, where appropriate, transfer the Customer's personal data outside the EU/EEA. However, any such transfer is permissible only if (i) the country has an adequate level of protection for personal data in accordance with a decision announced by the EU Commission that covers the processing of personal data, (ii) the Supplier ensures that there are appropriate safeguards in place such as standard data protection clauses, as adopted by the EU Commission, in light of the recipient country's legislation or (iii) any other exemption in the Applicable Legislation permits the transfer.

7.2 If the Supplier transfers personal data outside the EU/EEA on the basis of standard data protection clauses, the Customer hereby grants the Supplier power of attorney to agree such standard clauses on behalf of the controller.

8. CONFIDENTIALITY

8.1 The following will also apply without any impact on the undertaking of confidentiality in the Agreement.

8.2 The Supplier must observe strict confidentiality about the personal data processed on behalf of the Customer. Consequently, the Supplier may not, directly or indirectly, disclose any personal data to any third party unless the Customer has approved this in writing, except where the Supplier is under a statutory obligation to disclose personal data or this is necessary for the performance of the Agreement. The Supplier accepts that this undertaking of confidentiality will continue to apply after the termination of the Agreement.

8.3 The Customer undertakes to observe strict confidentiality about all information that the Customer receives concerning the Supplier's safeguards, procedures and IT systems or that is otherwise of a confidential nature, and also undertakes not to disclose to any third party any confidential information that originates from the Supplier or its Sub-processors. However, the Customer is entitled to disclose information that the Customer has an obligation to disclose by law or under the Agreement. The Customer accepts that this undertaking of confidentiality will continue to apply after the termination of the Agreement.

9. LIABILITY

9.1 If the Supplier suffers any loss or receives a claim as a consequence of the Supplier's processing of personal data in accordance with the Customer's instructions or as a consequence of the Customer having been in breach of sub-clause 1.2, the Customer must indemnify the Supplier for any loss arising as a consequence of this. However, the Supplier is liable for performance of a Sub-processor's obligations to the Customer if a Sub-processor fails to perform its obligations. No limitation of liability under this Agreement will be applied to the Customer's liability under this appendix.

9.2 If the Customer's further documented instructions for the processing of personal data are not supported by the Services or do not match the Supplier's undertakings under the rest of the Agreement and the Supplier could not reasonably have expected them, and these requirements cause the Supplier to incur additional expenses, the Supplier is entitled to choose between terminating the Agreement with immediate effect or receiving compensation from the Customer for these expenses.

10. TERMINATION OF THE AGREEMENT

10.1 On termination of the Agreement, the Supplier must, at the Customer's discretion, either return or erase all personal data that the Supplier has processed on behalf of the Customer. If the Customer does not make any such request within fourteen (14) days after the end of processing, the Supplier must securely erase the personal data

Appendix – Description of the processing of personal data in the Services

This appendix is considered to be an integral part of the Personal Data Processing Agreement.

1. Purpose of the processing

Personal data is processed for the following purposes:

- To provide the Services and support the Services, and
- To carry out any further documented instructions provided from time to time by the Customer or the Customer's subcontractors

2. Locations at which personal data will be processed

The personal data is processed by the Supplier in Sweden. For information on the sub-processors engaged by the Supplier and where they process the Customer's personal data, see the website indicated by the Supplier from time to time. See also Clause 5 below for further information on the Sub-Processors we are employing to deliver the Service at the commencement of the Agreement.

3. Retention of personal data

If the Agreement is terminated, the data is retained until the Supplier has returned or erased the Customer's personal data in accordance with the provisions in the Personal Data Processing Agreement. See also Clause 5 below for further information on the period for which personal data is retained within the framework of each sub-service.

4. Sub-Processors engaged

The following Sub-processors are engaged by the Supplier to provide the Services at the time of commencement of the Agreement.

Identity	**Address**	**Processing location**	**Service**
BuildSafe Tech	Griboyedov Canal Embankment, St., 99 b., A liter, 07, 08 of., Saint Petersbourg	RU	Internal service development
Amazon Web Services	38 John F. KennedyL-1855 Luxembourg	EU/US	Hosting/infrastructure
Mixpanel Inc	1 Front St., Suite 2800, San Francisco, CA 94111	US	Product analysis
Branchmetrics Inc	1400 Seaport Blvd, Building B, 2nd Floor, Redwood City, CA 94063	US	Link distribution
OneSignal Inc	2194 Esperanca Avenue Santa Clara, CA 95054 United States	US	Push-notice distribution

StartDeliver AB	Kungsgatan 33, 111 51 Stockholm, Sweden	SE	Account service
Freshworks GmbH	*Neue Grünstraße 17, 10179 Berlin, Germany*	DE	Customer Support
Wootric Inc	220 27th St, San Francisco, California, 94131, United States	US	NPS-surveys

5. Detailed description of the processing of personal data in the Service

Nedan beskrivs den behandling av personuppgifter som förekommer i Tjänsten i förhållande till respektive deltjänst.

Subservice	Example of processing	Categories of registereds	Categories of personal data	Retention period
Managing introductions	• Communicating invitations to the service • Registering information at introduction • Compilation of information • Storing of registered information	• Employees of the Customer • Consultants, partners or otherwise employed by the Customer • Next-of-kin to the above • External participants • Visitors	• Picture • Identity • Competencies • Contact details • Organisational information • Status information • Citizenship (where applicable)	Personal data is retained during the construction project where the user is registered and for a period of two (2) years after the end of the project for traceability. Information about next-of-kin are retained for the same period.
Managing inspections	• Registering inspections • Scheduling inspections • Registering responsibility for actions • Documenting inspections • Compiling actions	• Employees of the Customer • Consultants, partners or otherwise employed by the Customer • External participants • Visitors	• Identity • Contact details • Organisational information	Personal data is retained during the construction project where the user is registered and for a period of two (2) years after the end of the project for traceability.
Conducting ad-hoc reporting	• Registerings reports of observations, near misses and accidents • Presenting overviews of reports	• Employees of the Customer • Consultants, partners or otherwise employed by the Customer • External participants • Visitors	• Picture • Employment status • Identity • Contact details • Organisational information • Location details • Health information	Personal data is retained during the construction project where the user is registered and for a period of two (2) years after the end of the project for traceability. Personal data registered regarding accidents are retained for a period of ten (10) years after the report of the accident for legal purposes.
Action management	• Assigning actions • Registering actions • Communicating actions • Presenting overviews of actions	• Employees of the Customer • Consultants, partners or otherwise employed by the Customer • External participants • Visitors	• Identity • Contact details • Organisational information • Performance data	Personal data is retained during the construction project where the user is registered and for a period of two (2) years after the end of the project for traceability.

Subservice	Example of processing	Categories of registereds	Categories of personal data	Retention period
Incident management	• Registering information about incidents • Generating reports	• Employees of the Customer • Consultants, partners or otherwise employed by the Customer • External participants • Visitors	• Picture • Employment status • Identity • Contact details • Organisational information • Location details • Health information	Personal data is retained during the construction project where the user is registered and for a period of two (2) years after the end of the project for traceability. Personal data registered regarding accidents are retained for a period of ten (10) years after the report of the accident for legal purposes.
Insights	• Analysing data on an aggregated level • Evaluation of KPI:s connected to risk management and accidents	• Employees of the Customer • Consultants, partners or otherwise employed by the Customer • External participants • Visitors	• Identity • Contact details • Organisational information • Performance data	Personal data is retained for the same periods as the relevant subservices as listed above. Reports that do not contain personal data are retained for the full duration of the relationship between the Supplier and the Customer or until it is erased by the Customer.
Administration av Tjänsten	• Registrering av användarkonton • Registrering av behörigheter/åtkomst	• Employees of the Customer • Consultants, partners or otherwise employed by the Customer	• Identity • Contact details • Organisational information • Technical information	Personal data is retained for this purpose during the period that the user is considered active and for a period of 2 years thereafter. A user account is considered active if the user has been logged in in the last two years.
Managing customer support	• Communication in our support channels • Managing technical flaws	• Employees of the Customer • Consultants, partners or otherwise employed by the Customer	• Identity • Contact details • Organisational information • Technical information	Personal data is retained for this purpose for as long as your user account is active. Personal data in logs is retained in order to fulfil our legitimate interest of troubleshooting and incident management for a period of two (2) years from the log entry time.

Subservice	Example of processing	Categories of registereds	Categories of personal data	Retention period
Developing and improving the Service	• Storing information in test environments • Using user data to conduct tests • Anonymising user data	• Employees of the Customer • Consultants, partners or otherwise employed by the Customer • External participants • Visitors	• Technical information	Personal data is retained for the period necessary to anonymize the information, test the functionality and verifying corrections, however never for a period longer than six (6) months from the log entry time.
Ensuring necessary technical functionality and security	• Back-ups • Analysis • Incident management	All the categories above	All the categories above	Personal data is retained for the same periods as the relevant subservices as listed above.

I tabellen nedan anges närmare information om de kategorier av personuppgifter som Leverantören behandlar inom ramen för Tjänsten.

Category of personal data	Examples of information
Employment information	Type of employment and length of employment
Picture	Identification photo
Health information	Information regarding your health status
Identity	Name, username, personal identification number or similar
Incident data	Descriptive information of incidents that you are a subject to

Category of personal data	Examples of information
Communication	Contents of messages
Campetencies	Records of trainings or other similar competencies
Contact details	Email, phone number
Location details	GPS position or place of work
Organisational information	Information about your employer, title, role in project or responsibilities
Performance data	Information about performance in the Service
Status	Active/inactive
Technical information	IP-adress, UID, Device ID, Language settings
Citizenship	Citizenship connected to work status

Appendix – Technical and organisational safeguards

The Supplier and Sub-processors take the following technical and organisational measures to protect the Personal Data subject to this Personal Data Processing Agreement:

- Measures for access control, for example procedures for password management and authentication (via two-factor authentication), logging, user rights management and access to operating premises.
- Measures to ensure confidentiality, for example encryption of data for transfer.
- Measures to ensure accessibility, for example backups, firewalls, antivirus systems, logging and uninterruptible power supply (UPS).

The Supplier also has procedures for managing security breaches. The staff are subject to non-disclosure agreements, and penetration tests are carried out regularly.