DATA PROCESSING AGREEMENT INFOBRIC CONSTRUCTION

Appendix 3

(2023:1)

DATA PROCESSING AGREEMENT INFOBRIC CONSTRUCTION (2023:1)

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').

1.2 Sub-section 1.2 applies only when the Customer's operations that have given rise to the personal data processing are conducted in Sweden and is applicable to the use of the service Ease Construction. When the Customer, by supplying the Supplier's equipment to a workplace, requests a subcontractor to use the Supplier's equipment to fulfil its obligation to register in the staff register, the subcontractor is the controller for its Staff data in the Services. The Customer is the processor for the subcontractor's personal data processing, and a Data Processing Agreement must therefore be made by the subcontractor and the Customer, with content corresponding to this Data Processing Agreement. Similarly, if the Customer supplies equipment on behalf of a client, the Customer is the processor for the client's personal data processing and must make a Data Processing Agreement with the client. In relation to the subcontractor and the client, the Supplier has the role of sub-processor for the Customer. The Customer is liable to obtain instructions from the subcontractor and client for the Supplier's processing of personal data as the sub-processor, and the Customer must otherwise act as the point of contact for the performance of the Supplier's obligations to the subcontractor and client under the Applicable Legislation. The provisions in the Agreement on the role of the Supplier as processor will also apply to the role of sub-processor.

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 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 – Supplier Ease.

2.3 Notwithstanding the provisions in sub-section 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 Section 8 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 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 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 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 Section 8 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 Section 6 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 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 Data Processing Agreement with each Sub-processor. Such a 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 Section 17 of 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-section 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. If the Customer has requested a backup in accordance with sub-section 18.5 of the General Terms and Conditions – Supplier Ease, the Supplier must, however, store backups for the period specified there, subject to the provisions in this Agreement. When the time limit specified in sub-section 18.5 of the General Terms and Conditions – Supplier Ease has been reached, the Supplier must securely erase the backups unless agreed otherwise with the Customer.

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

This appendix is considered to be an integral part of the 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 AB. 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.

3. Retention of personal data

The Customer may decide the period for which personal data is stored in the Services. 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 Data Processing Agreement. See also Section 0 below for further information on the period for which personal data is retained within the framework of each sub-service.

4. A further description of the processing of personal data in the Services in relation to each sub-service

The processing of personal data that occurs in the Services in relation to each sub-service is described below.

A. EASE CONSTRUCTION

Sub-service/Purpose	Example of Personal data processing methods	Categories of data subjects	Categories of personal data	Retention of personal data
Workplace The sub-service Workplace includes HR management, access control, registration of attendance and skills management.	• Collection by registration when creating a user profile and using cards, for example card reading and checking in/out • Transfer of personal data from registration box, Controlbox, Machine Controller or other hardware and the App to the Application • Access for viewing and editing personal data via the Application • Access for the data subject to log data on the data subject in connection with their use of the Software • Disclosure of personal data to subcontractors, limited to personal data on the subcontractors' own employees, contracted staff, consultants or other staff that may be equated to employees • Preparation of reports for follow-up and documentation	• The Customer's employees and other staff contracted or otherwise engaged by the Customer • The Customer's subcontractors' employees and other staff contracted or otherwise engaged by the Customer's subcontractors • Any other person who visits a workplace in which the Software is used	• Identity data (for example name, employment number, applicable ID number[1], photograph and fingerprints (if the Customer connects such equipment to the Software and activates the function)) • Contact details (for example address, phone numbers (work, home, mobile), fax number, email address (work/personal)) • Organisation data (for example title, employer, workplace (where the person was added to the database), company for which the person works (if other than employer), access authorisation group) • Card details (for example card number, PIN and card reads) • Skills and certificate data (for example training and certificates based on HSE rules, certificate of tax liability) • Log data (for example records of entry and departure at workplaces)	Unless the Customer actively changes the instruction, the instruction to the Supplier is to retain data for three (3) years from registration.

[1] For *Sweden:* personal identity number, coordination number or equivalent foreign number. For *Norway:* HSE card number. For *Finland:* tax number. And for the *United Kingdom:* CSCS/IPAF number.

Sub-service/Purpose	Example of Personal data processing methods	Categories of data subjects	Categories of personal data	Retention of personal data
			• Location data (for example GPS position for records of entry and departure at workplaces via the App) • Data on contact in case of emergency (ICE) • Further categories of personal data as a result of the instructions provided by the Customer from time to time	
Staff Register/Team List The Staff Register/Team List sub-service includes management of the staff register and team list for workplaces.	• Disclosure of personal data via reports to authorised recipients (for example employer, safety officer and public authority) • Disclosure of personal data to subcontractors, limited to personal data on the subcontractors' own employees, contracted staff, consultants or other staff that may be equated to employees • Preparation of reports for follow-up	• The Customer's employees and other staff contracted or otherwise engaged by the Customer • The Customer's subcontractors' employees and other staff contracted or otherwise engaged by the Customer's subcontractors • Any other person who visits a workplace in which the Software is used •	• Identity data (for example name and applicable ID number[2]) • Demographic data (for example date of birth (in applicable countries)) • Organisation data (for example employer, workplace (where the person was added to the database), company for which the person works (if other than employer)) • Log data (for example start and finish times of shift or day on which the person works at the workplace) •	*Sweden:* The data is retained until the end of the current calendar year and for three (3) more years, calculated from the time of registration. *Norway:* The data is retained for six months after the construction site has been closed.

[2] For *Sweden:* personal identity number, coordination number or equivalent foreign number. For *Norway:* HSE card number. For *Finland:* tax number. And for the *United Kingdom:* CSCS/IPAF number.

Sub-service/Purpose	Example of Personal data processing methods	Categories of data subjects	Categories of personal data	Retention of personal data
Company The Company sub-service includes company management for the companies registered in the Software, management of staff registers and management of advance notification of staffing to workplaces.	• Collection through registration of data • Transfer of personal data from registration box, Controlbox, Machine Controller or other hardware and the App to the Application • Access for viewing and editing personal data via the Application • Transfer of personal data to ensure that the collected data is up-to-date and accurate • Access for the data subject to data on the data subject in connection with their use of the Software • Preparation of reports for follow-up and documentation	• The Customer's employees and other staff contracted or otherwise engaged by the Customer • Users of the App	• Identity data (for example name, employment number, applicable ID number[3] and photograph) • Contact details (for example address, phone numbers (work, home, mobile), fax number, email address (work/personal)) • Organisation data (for example title, employer, workplace (where the person was added to the database), company for which the person works (if other than employer), access authorisation group) • Card data (for example card number, card reads and PIN) • Skills and certificate data (for example training and certificates based on HSE rules, certificate of tax liability) • Data on contact in case of emergency (ICE) • Other categories of personal data arising out of the instructions given by the Controller from time to time	Unless the Customer actively changes the instruction, the instruction to the Supplier is to retain data for three (3) years from the most recent action.

[3] For *Sweden:* personal identity number, coordination number or equivalent foreign number. For *Norway:* HSE card number. For *Finland:* tax number. And for the *United Kingdom:* CSCS/IPAF number.

Sub-service/Purpose	Example of Personal data processing methods	Categories of data subjects	Categories of personal data	Retention of personal data
System Administration The System Administration sub-service includes user management and administration of services.	• Access for viewing and editing user accounts • Access for viewing and editing system authorisation • Management of GDPR cases	• System users • System administrators • Contract signatories • Users of the App	• Identity data (for example user name) • Contact data (for example phone number and email address) • Organisation data (for example employer) • User account data (for example accessibility (public or not), system authorisation, language settings, reminder settings) • Other categories of personal data arising out of the instructions given by the Controller from time to time	Personal data linked to user accounts is retained for as long as the user accounts are active and for a period of three (3) months after user accounts are closed.
Analysis The Analysis sub-service includes supplier follow-up and preparation of reports.	• Collection of credit information from credit rating agencies • Analysis of collected data and presentation of results in the Software • Retention of data to permit follow-up over time • Preparation of reports for follow-up	• Deputies (for example Board members and deputy Board members) for suppliers active at the Customer's workplace • Owners	• Identity data (for example name and personal identity number) • Contact data (for example address) • Organisation data (for example position) • Demographic data (for example marital status) • Data on financial status and risk (for example income data, credit commitments and records of non-payment) • Other categories of personal data arising out of the instructions given by the Controller from time to time	Credit information is retained for a period of three months from the time of collection. Status data is retained for a period of twelve months from the time at which follow-up took place to permit follow-up over time. Manual status is retained until further notice or until the time at which new follow-up is carried out. Status data is also retained for a period of twelve months from the time of collection to permit follow-up over time.

A. FIELD

Subservice/Purpose	Example of Personal data processing methods	Categories of data subjects	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.

The table below provides further information on the categories of personal data processed by the Supplier as described above.

Category of personal data	Examples of information
Employment information	Type of employment and length of employment
Photo	Identification photo
Health information	Information regarding health status
Identity	Name, username, personal identification number or similar
Incident data	Descriptive information of incidents that you are a subject to
Communication	Content of messages
Competence data	Information on professional certificates and certificates of various kinds
Contact details	E-mail address, phone number
Location data	Location information from a mobile device
Organisational information	Employer/client, title, role in project, responsibility
Performance data	Information on implemented measures, status of task
Status data	Active/Inactive
Technical data	IP address, UID, language settings
Nationality information	Citizenship

5. Sub-processors engaged

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

EASE CONSTRUCTION

Identity	Processing location	Service
Sigma Sweden Software AB, 559120-5561, Lindholmspiren 9, 417 56 Göteborg	Sweden and Ukraine	Support and development
Axians AB, 556590-7069 Råsundavägen 4, 169 67 Solna	Sweden	IT operations
Microsoft	EU	Storage of documentation
Freshdesks Inc, 2950 S. Delaware Street, Suite 201, San Mateo, CA 94403, USA	EU	Support

FIELD

Identity	Processing location	Service
Amazon Web Services 38 John F. KennedyL-1855 Luxembourg	EU	Hosting/infrastructure
Komstrim OOD 11 Prof. Aleksandar Tanev str. Mladost 4 Distr., Fl. 4, Office 14 Sofia, 1715 Bulgaria	EU	Internal development and quality assurance
Mixpanel Inc 1 Front St., Suite 2800, San Francisco, CA 94111, United States	USA	Produkt analysis
Branchmetrics Inc 1400 Seaport Blvd, Building B,	USA	Länkdistribution

2nd Floor, Redwood City, CA 94063, United States		
OneSignal Inc 2194 Esperanca Avenue Santa Clara, CA 95054 United States	USA	Pushnotis-distribution
StartDeliver AB Kungsgatan 33, 111 51 Stockholm, Sweden	Sweden	Account Maintenance
Freshdesks Inc, 2950 S. Delaware Street, Suite 201, San Mateo, CA 94403, USA	EU	Support

6. Changes to these instructions

The parties agree that these instructions may be updated from time to time to reflect the processing of personal data that the Supplier (and its Sub-Processors) conduct on behalf of the Customer in connection with the supply of the Services.

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 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 security measures are carried out regularly.