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 Main 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. INFOBRIC SITE

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	• 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	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
	• Preparation of reports for follow-up and documentation		HSE rules, certificate of tax liability) • Log data (for example records of entry and departure at workplaces) • 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	• 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	• 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	*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
	• Preparation of reports for follow-up	which the Software is used •	shift or day on which the person works at the workplace) •	
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	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
			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	
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.

Sub-service/Purpose	Example of Personal data processing methods	Categories of data subjects	Categories of personal data	Retention of personal data
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.
Manage inquiries and support	• Communication in connection with inquiries or support • Troubleshooting and error handling	• Customer's employees • Customer's hired or otherwise engaged personnel • System users	• Identity data • Contact data • Organizational data • Communication	Technical data Personal data is retained for as long as the Customer uses the Service, however for a maximum period of two (2) years from the time the case was closed.

A. INFOBRIC 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
Organizational 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.

INFOBRIC SITE

Identity	Processing location	Service
Sigma Nordic Software AB, , 559492-6692, Lindholmspiren 9, S-417 56 Göteborg	Sweden and Ukraine	Support and development
Axians AB, 556590-7069 Råsundavägen 4, S-169 67 Solna	Sweden	IT operations
Microsoft	EU	Storage of documentation
Intercom R&D Unlimited Company Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Republic of Ireland	Ireland	Support

INFOBRIC FIELD

Identity	Processing location	Service
Amazon Web Services 38 John F. KennedyL-1855 Luxembourg	EU	Hosting/infrastructure

Comstream Sweden AB Östra Vittusgatan 36, S-371 14 Karlskrona	EU	Development and quality assurance
Mixpanel Inc 1 Front St., Suite 2800, San Francisco, CA 94111, United States	USA	Product analysis
Branchmetrics Inc 1400 Seaport Blvd, Building B, 2nd Floor, Redwood City, CA 94063, United States	USA	Link distribution
OneSignal Inc 2194 Esperanca Avenue Santa Clara, CA 95054 United States	EU	Push notice distribution
StartDeliver AB Kungsgatan 33, 111 51 Stockholm, Sweden	Sweden	Account Maintenance
Intercom R&D Unlimited Company Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Republic of Ireland	Ireland	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.