Data Processing Addendum

This Data Processing Addendum forms part of the YMSLITE Terms and Conditions, along with the Registration Form ("Agreement").

In respect of the Parties' rights and obligations under this DPA regarding personal data that INFORM processes on behalf of Customer in connection with Customer's use of the Services pursuant to the Agreement, Customer is the controller, and INFORM is the processor.

[As the controller, Customer (i) is solely responsible for determining the purposes and means of processing personal data; (ii) has all necessary authority, grounds, rights, and permissions to provide personal data to INFORM; and (iii) has provided, and will continue to provide, all notices and has obtained, and will continue to obtain, all consents and rights necessary under applicable law for INFORM to process personal data for the purposes described in this DPA and the Agreement.

Customer shall have sole responsibility for the accuracy, quality, and legality of the personal data and the means by which Customer acquired the personal data. Customer will comply with applicable laws, including with all obligations as a controller under applicable law, in respect of its processing of personal data and any processing instructions it issues to INFORM

Customer acknowledges that INFORM is not responsible for determining which laws or regulations are applicable to Customer's business. Customer is solely responsible for determining that the Services provided by INFORM and the terms of the Agreement and this DPA meet Customer's business, contractual, and legal obligations. Customer also will ensure that Customer's processing instructions to INFORM do not violate any applicable law.

Notwithstanding anything to the contrary in the Agreement, including this DPA, INFORM will not be liable for any claim made by a data subject arising from or related to INFORM's acts or omissions, to the extent that INFORM was acting in accordance with Customer's instructions. INFORM's liability under or in connection with this DPA is subject to the exclusions and limitations on liability contained in the Agreement.]

Standard contractual clauses ("DPA SCCs")

SECTION I

Clause 1

Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

b) The controller and processor have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.

c) These Clauses apply to the processing of personal data as specified in Annex II.

d) Annexes I to IV are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

Clause 2

Invariability of the Clauses

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub- processor to fulfil its contractual obligations.

e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

4) the obligations in Article 32 of Regulation (EU) 2016/679.d)

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

   1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   2) the likely consequences of the personal data breach;

   3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

   Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2. Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

   1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

   2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

   3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

Processor, contact person and Data Protection Officer

Processor:

Name: INFORM Institut fuer Operations Research und Management GmbH

Address: Pascalstrasse 35, 50276 Aachen, Germany

Eva Savelsberg

Email: eva.savelsberg@inform-software.com

Data Protection Officer: Dr. Oliver Meyer-van Raay, V-Formation GmbH, Stephanienstrasse 18, 76133 Karlsruhe, Germany

Tel.: +49 721 / 17029034

E-Mail: om@v-formation.gmbh

Signature and accession date: The Parties agree that execution of the Agreement by the Controller and the Processor shall constitute execution of these Clauses by both Parties as of the submission of the Registration Form.

Controller:

Name: Customer, as specified in the Agreement.

Address: As specified in the Agreement.

Contact person’s name, position and contact details: As specified in the Agreement.

Signature and accession date: The Parties agree that execution of the Agreement by the Controller and the Processor shall constitute execution of these Clauses by both Parties as of the submission of the Registration Form.

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed:

- Customer employees who use YMSlite as named users, including admins and operational users.
- External parties recorded for yard operations, as entered by the customer, for example drivers and additional details.
- Customer billing and finance contacts, if billing and subscription management applies.
- Customer details stored in CRM

Categories of personal data processed:

Account and user management

- Name, business email address, username, role, permissions.
- Authentication and session data, for example user ID, login timestamps, session identifiers, access tokens.
- Audit and activity logs linked to user actions, for example who created or changed a record and when.
- Contact identification data, for example first name, last name, job title, company, department.
- Contact details, for example business email address, business phone number.

Operational yard management data

- Contact data captured in operational records, for example driver name, phone number.
- Identifiers related to yard movements, for example vehicle license plate, trailer number, container number, booking reference, shipment reference.
- Operational timestamps and status information, for example appointment times, check in and check out times, dock assignment times, yard status milestones.
- Free text fields entered by users, to the extent the customer chooses to input personal data.

Technical and usage data

- Log data and device data required to provide and secure the service, for example IP address, user agent, time zone, event logs, error logs.
- Support and troubleshooting data, for example configuration data and relevant log extracts.

Billing and payment data, if applicable

- Billing contact data, for example name, email address.
- Payment related data processed via the payment provider, for example payment method tokens and transaction metadata.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

- The service is not designed to process special categories of personal data under Article 9 GDPR, or criminal convictions data under Article 10 GDPR.
- The controller must not upload special category data into free text fields or attachments.
- If the controller uploads such data, the processor will treat it as personal data and will apply the security measures defined in Annex III.

Nature of the processing:

- Collection, recording, organisation, structuring.
- Storage, adaptation, updating, retrieval, consultation, use.
- Disclosure by transmission within the service, for example API calls and user interface delivery.
- Alignment or combination of data within the tenant for operational workflows.
- Restriction, erasure, and destruction on instruction and at end of contract.

Purpose(s) for which the personal data is processed on behalf of the controller:

- Provide a yard management system for planning and executing yard operations, including appointment scheduling, gate processes, yard visibility, and dock assignment.
- Provide authentication, authorization, and access control for customer users.
- Provide audit trails and operational traceability.
- Maintain security, availability, monitoring, and incident response for the SaaS platform.
- Provide customer support, troubleshooting, and service improvement limited to what is necessary to deliver the service under the controller’s instructions.

Duration of the processing:

- For the term of the SaaS agreement.
- Upon termination, deletion or return of personal data as instructed by the controller in accordance with the YMSlite Terms and Conditions.
- Residual copies may remain in backups for a limited period required by the processor’s backup and disaster recovery procedures, then the processor deletes them according to the backup lifecycle.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing.

Amazon Web Services, Inc.

- Subject matter: Cloud infrastructure hosting for the SaaS platform.
- Nature: Storage, processing, and transmission of customer data within the hosted environment, including backups and logs required to operate the service
- Duration: For the term of the SaaS agreement, plus backup retention per the processor’s backup lifecycle.

Stripe, Inc. and Stripe Payments Europe, Ltd.

- Subject matter: Payment processing and subscription billing operations.
- Nature: Processing of billing contact data and payment transaction metadata, and tokenization of payment methods, as necessary to facilitate payments and fraud prevention.
- Duration: For the term of the billing relationship, plus retention required by applicable financial and tax laws and Stripe’s standard retention policies.

Keycloak, maintained by Red Hat, Inc.

- Subject matter: Identity and access management for user authentication and authorization.
- Nature: Processing of user identifiers, credentials handling, session management, and issuance of access tokens required for secure login and access control.
- Duration: For the term of the SaaS agreement. Session data is short lived. User account data persists until deleted by the controller or contract termination.

ANNEX III

Technical and Organizational Measures (TOM)

1 Confidentiality (Art. 32 para. 1 lit. b GDPR)

1.1 Access control to premises and facilities (physical access control)

Access control to premises and facilities **Unauthorized access to premises and facilities must be prevented, whereas the term is to be understood spatially.**	**existent** **yes**
Electronic access code card / access transponders	☒
Two-factor authentication data centers	☒
Central reception area	☒
Access authorization concept	☒
Video surveillance	☒
Alarm system	☒
Key management	☒
Security areas with different access authorizations	☒
Escorting of visitors‘ access by our own employees	☒
Securing off-hours by site security service	☒
Scaled security areas and controlled access	☒
Secured entrance for delivery and pickup	☒
Special glazing	☒
Storage of servers in access protected data centers	☒
Locked storage of data carriers or storage in locked rooms	☒
Data backups in access protected data centers	☒
Instruction for issuing code card / access transponders	☒
Obligation to visibly wear the access code cards (employee badges)	☒

1.2 Access Control to Systems (Hardware access control)

Access control to systems **The intrusion of unauthorized persons into the data processing systems or their unauthorized use must be prevented.**	**existent** **yes**
Data processing equipment is under lock	☒
Functional and/or time-limited assignment of user authorizations	☒
Use of individual passwords	☒
Automatic locking of user accounts after multiple incorrect password entries	☒
Automatic password-protected screen locking after inactivity (screen saver)	☒
Password policy with minimum requirements for password complexity:	
▪ Minimum of 10 characters / upper and lower case, special characters, numbers (of which at least 4 criteria)	☒
▪ Upper and lower case character, special character and number	☒
▪ Password history (no re-use of the last 10 passwords)	☒
▪ Prevention of trivial passwords	☒
▪ Change of password after 180 days max	☒
▪ Scanning of AD passwords for compromise	☒
Hashing of stored passwords	☒
Procedure for the assignment of authorizations with the entry of employees	☒
Procedure for revocation of authorizations due to department change of employees	☒
Procedure for revocation of authorizations due to exit of employees	☒
Obligation to confidentiality and data secrecy	☒
Certified destruction of data carriers	☒
Securing externally accessible services using two-factor authentication	☒
Storage of embodied personal data in lockable security cabinets	☒

1.3 Access control to data (software access control)

Access control to data **Unauthorized activities in data processing systems outside of assigned authorizations must be prevented.**	**existent** **yes**
Definition of access authorization - authorization concepts	☒
Definition of authorizations to enter, modify or delete data	☒
Separation of authorization approval (organizational) and authorization assignment (technical)	☒
Procedure for the recovery of data from backups (who, when, on whose request)	☒

Restriction of free and uncontrolled database queries	☒
Time limitation of access possibilities	☒
Partial access options to databases and functions (Read, Write, Execute)	☒
Use of appropriate security systems (software/hardware)?	
▪ Extended Detection and Response Solution (XDR)	☒
▪ Virus scanner	☒
▪ Firewalls	☒
▪ SPAM-Filter	☒
▪ Intrusion prevention (IPS)	☒
▪ Intrusion detection (IDS)	☒
Encrypted storage of data	
▪ Encryption algorithms used:	
▫ AES (128/256 bit)	☒
▫ RSA (2048 bit minimum)	☒
▪ Hash function used:	
▫ SHA2 (256, 384, 512 bit)	☒
▫ SHA3	☒
▫ bcrypt	☒

1.4 Contractor Control

Contractor Control When personal data is processed "on behalf", it must be ensured that it is only processed in accordance with the instructions of the customer.	**existent** **yes**
Drafting of contracts in accordance with legal requirements (Art. 28 GDPR)	☒
Central recording of existing service providers (uniform contract management)	☒
Prior checks at the contractor before the start of the contract	☒
Regular checks at the contractor after the start of the contract (for the duration of the contract)	☒
Review of the data security concept at the contractor's premises (if provided)	☒
Inspection of existing IT security certificates of the contractors (if provided)	☒
Issuing instructions to the contractor to improve data protection	☒
Established reporting process in the event of serious operational disruptions and suspected data protection violations	☒

1.5 Separation Control

Separation control **Data collected for different purposes must also be processed separately.**	**existent** **yes**
Separation of customer data (multi-client capability of systems)	☒
Data separation in databases	☒
Logical data separation (e.g. based on customer or client IDs)	☒
Processing of the data of different customers by different employees of the contractor	☒
Authorization concept that takes into account a separate processing of data of different customers	☒
Separation of functions	☒
Separation of development, test and production system	☒

2 Integrity (Art. 32 para. 1 lit. b GDPR)

2.1 Control of transmission

Control of transmission **Aspects of the transfer (transmission) of personal data are to be regulated: electronic transfer, data transport as well as their control.**	**existent** **yes**
What is the mode of transmission of data between Controller and third parties?	
▪ Terminal server connection (min. 128 bit encrypted)	☒
▪ VPN connection (IP-Sec)	☒
▪ Email with encrypted ZIP file attached	☒
▪ Data exchange via https connection	☒
Encryption protocol used:	
▫ min. TLS 1.2	☒
Secured entrance for supply and delivery	☒
Documented management of data carriers, inventory control	☒
Encryption of data carriers with confidential data	☒
Encryption of laptop hard disks	☒
Encryption of mobile data carrier	☒
Data carrier disposal – Secure deletion of data carriers:	
▪ Physical destruction (e.g. shredder with particle cut - 1000 mm² max.)	☒
Paper disposal: Secure destruction of paper documents:	

▪ Closed metal containers (German so-called “Datenschutztonnen”), disposal by service provider	☒
▪ Shredder according to DIN 66399	☒

2.2 Entry control

Entry control **Traceability and documentation of data administration and maintenance must be guaranteed.**	**existent** **yes**
Definition of user authorizations (profiles)	☒
Read, modify, delete	☒
Partial access to data or functions	☒
Field access in databases	☒
Organizational definition of input responsibilities	☒
Logging of entries / deletions	☒
Obligation to confidentiality / data secrecy	☒
Regulations on retention periods for auditing/verification purposes	☒

3 Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

3.1 Availability control

Availability control **The data must be protected against accidental destruction or loss.**	**existent** **yes**
Data protection and backup concept	☒
Carrying out data protection and backup concept.	☒
Restriction of access to server rooms to authorized personnel	☒
Fire alarm systems in server rooms	☒
Smoke detectors in server rooms	☒
Waterless firefighting systems in server rooms	☒
Air-conditioned server rooms	☒
Lightning / overvoltage protection	☒
Water sensors in server rooms	☒
Server rooms in separate fire compartments	☒
Housing backup systems in separate rooms and fire compartment	☒

Ensure technical readability of backup storage media for the future	☒
Storage of archive storage media under necessary storage conditions (air conditioning, protection requirements, etc.)	☒
CO^{2} fire extinguishers in the immediate vicinity of the server rooms	☒
UPS system (uninterruptible power supply)	☒

4 Measures to ensure resilience

4.1 Resistance and reliability control

Resistance and reliability control **Systems must be able to cope with risk-related changes and must be tolerant and able to compensate disruptions.**	**existent** **yes**
Redundant power supply	☒
Redundant data connection	☒
Redundant air conditioning	☒
Redundant fire fighting	☒
Hard disk mirroring	☒
Use of a high-availability SAN solution	☒
Load balancer	☒
Data storage on RAID systems (RAID 1 and higher)	☒
Delimitation of critical components	☒
Separation of the internal network from public networks by means of demilitarized zones (DMZ)	☒
Performance of penetration tests (for application and development systems and infrastructure)	☒
Monitoring of critical systems by a Security Operating Center (SOC)	☒
System hardening (deactivation of non-required components)	☒
Immediate and regular activation of available software and firmware updates	
▪ Identification of the different devices that make up the network and identification of their hardware version as well as their current software and firmware versions.	☒
▪ Communication channel with manufacturers to stay up-to-date on any new updates and patches released for the devices owned.	☒
▪ Definition of time periods in which the updates shall be implemented (e.g. periods of lower operations, maintenance times, etc.)	☒
▪ Use of redundant systems to maintain operations while main devices are being updated.	☒
▪ Deployment of updates / patches	☒
▪ Specify a testing period to verify the correct implementation of the update and ensure that operations continue to run smoothly with the new updates.	☒

Security is included as a main consideration during the design phase of the systems.	
▪ Definition of security measures to protect and validate communication between system components.	☒
▪ Limitation of authorizations on a need-to-know basis.	☒
▪ Revocation of temporary privileges as soon as they are no longer required	☒
▪ External contractors (service providers) and maintenance personnel must have a specific access, which must only be active during the intervention and remain disabled the rest of the time.	☒
▪ Interoperability will be included in the definition of network communication technologies and architecture	☒
▪ Identification of systems, infrastructures and environments that require communication with other systems (internal or external) or that will require such communication in the near future (taking into account the life cycle of the equipment involved)	☒
▪ Selection of communication protocols compatible with the identified systems and the systems of other organizations or environments.	☒
▪ Collaborative environments that enable the exchange of information between different parties	☒
▪ Identification of potential main attack vectors	☒
Periodic security training and awareness campaign within the organization	
▪ Awareness campaigns to inform users of the security concepts of specific systems and traditional IT systems	☒
▪ Specific security training to teach how to apply security measures and behaviors on the daily processes with the least impact possible.	☒
▪ Occasion-based warning of threats and risks	☒

5 Procedures for a regular testing, assessing and evaluating (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

5.1 Control procedures

Control procedures **A procedure is to be implemented for regularly testing, assessing and evaluating the effectiveness of the data security measures.**	**existent** **yes**
Records of processing activities are reviewed regularly/occasion-based.	☒
Notification of new/changed data processing procedures to the Data Protection Officer.	☒
Notification of new/changed data processing procedures to the Chief Information Security Officer (CISO).	☒
Privacy-friendly settings are selected.	☒
Security measures are subject to regular internal audits	☒

In the event of a negative outcome of the above-mentioned review, the security measures are adjusted, renewed and implemented in line with the risks involved.	☒

ANNEX IV

List of sub-processors

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1). The controller has authorised the use of the following sub-processors:

1. Name: **Amazon Web Services, Inc.**

   Address: 410 Terry Avenue North, Seattle, WA 98109, USA

   AWS Data Protection Team

   Email: aws-privacy@amazon.com

   Website: https://aws.amazon.com/privacy/

   AWS provides infrastructure and cloud-hosting services, including the storage, processing, and transmission of data required for operating the SaaS platform. AWS acts solely as an infrastructure sub-processor and does not access customer data except where technically necessary to deliver the services.

2. Name: **Stripe, Inc.**

   Address: 354 Oyster Point Boulevard, South San Francisco, CA 94080, USA

   Name: **Stripe Payments Europe, Ltd.**

   The One Building, 1 Grand Canal Street Lower, Dublin 2, Ireland

   Stripe Data Protection Officer

   Email: dpo@stripe.com

   Stripe provides payment processing and related financial infrastructure services, including the secure transmission, tokenization, and storage of payment information. Stripe acts as a payment services sub-processor and processes personal data solely as necessary to facilitate transactions, prevent fraud, and support payment-related operations.

3. Name: **Keycloak (Open Source Identity and Access Management Software) Maintained by Red Hat, Inc.**

   Address: **Red Hat, Inc.** 100 East Davie Street, Raleigh, NC 27601, USA

   Red Hat Privacy Team

   Email: privacy@redhat.com

Keycloak provides identity and access management functionality, including user authentication, authorization, session management, and identity federation. Keycloak processes personal data such as user identifiers, credentials, and access tokens solely for the purpose of enabling secure login and access control within the SaaS platform. Keycloak does not access or process customer data beyond what is required for authentication workflows.

4. Name: **Microsoft Corporation**
Address: One Microsoft Way, Redmond, WA 98052, USA
Name: **Microsoft Ireland Operations Limited**
Address: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland

Microsoft Privacy Team / Data Protection Officer

Email: privacy@microsoft.com

Microsoft provides cloud-based customer relationship management (CRM) services through Microsoft Dynamics 365. This includes the storage, processing, and management of customer and user data required for CRM functionality, such as contact information, communication history, and activity tracking. Microsoft acts as a cloud application sub-processor and processes personal data only as necessary to deliver and maintain the Dynamics 365 services.

ANNEX V

Transfer SCCs

This Annex V applies only to international transfers from INFORM (acting as data processor/data exporter) to a Customer (data controller) established in a non-EU/EEA country that is not on the EU Commissions list of countries providing adequate protection, and accordingly applies where Customer has transferred personal data to INFORM, and such personal data is transferred back to Customer established in a non-EU/EEA country ("Restricted Transfer"). For all Restricted Transfers, the Parties shall (i) cooperate to ensure compliance with applicable law; and (ii) implement Restricted Transfers in compliance with the requirements of applicable law and this DPA at all times.

"Transfer SCCs" means Module 4 (Processor-to-Controller) of the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, adopted by the European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021, as amended, superseded, or replaced from time to time, as currently available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. To the extent applicable, the Transfer SCCs are incorporated in and executed as part of the Agreement. By accepting this DPA, INFORM and Customer agree that the Transfer SCCs apply to any Restricted Transfer and are hereby incorporated and completed as follows:

- The "data exporter" is INFORM and the "data importer" is Customer;
- The optional docking clause in Clause 7 is implemented;
- The optional redress clause in Clause 11(a) is struck;
- The governing law in Clause 17 is the law of Germany;
- The courts in Clause 18(b) are the Courts of Germany; and
- Annex I.A and I.B to the Transfer SCCs are completed with the information in DPA SCCs Annex I and Annex II, respectively.

ANNEX VI

CCPA Addendum

This CCPA Addendum applies only where the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations ("CCPA") apply to Customer.

For purposes of this CCPA Addendum, the terms "Business," "Business Purpose," "Commercial Purpose," "Personal Information," "Sell," and "Share" shall have the meanings ascribed to them in the CCPA.

INFORM will process Customer Personal Information for the specific purposes identified in the DPA SCCs Annex II. INFORM will not (i) retain, use, or disclose Customer Personal Information for any purpose, including any Commercial Purpose, except for the limited Business Purpose as permitted under the Agreement or under the CCPA; (ii) retain, use, or disclose Customer Personal Information outside of the direct business relationship between Customer and INFORM, including by not combining any Customer Personal Information collected or received from another party, except as otherwise permitted by the CCPA; or (iii) Sell or Share Customer Personal Information. INFORM will comply with all applicable sections of the CCPA, including by providing the same level of privacy protection as required of Businesses by the CCPA. INFORM will notify Customer if, in INFORM's opinion, INFORM is unable to meet its obligations under the CCPA, unless such notice is prohibited by applicable law. Upon notice, Customer has the right to take reasonable and appropriate steps to ensure that INFORM uses the Customer Personal Information in a manner consistent with its obligations under the CCPA and may take reasonable and appropriate steps to mitigate and remediate any unauthorized use of Customer Personal Information. Customer will inform INFORM of any consumer request made pursuant to the CCPA that INFORM must comply with and provide the information necessary for INFORM to comply with the request.