General Terms and Conditions

of INFORM Institut f. Operations Research und Management GmbH ("INFORM")

for

the product SYNCROSUPPLY in the Cloud

Last updated: July 2024

§ 1 Scope

(1) These General Terms and Conditions (hereinafter "Terms") as in force at the time of conclusion of the contract regulate the time-limited provision of the software product selected in the order (hereinafter the "Software") on the internet exclusively to companies (hereinafter the "Customer"; INFORM and the Customer together the "Parties"). These General Terms and Conditions, including their annexes, form the contract together with the individual information and ordering data of the Customer.

(2) The Customer can at the conclusion of the contract decide between different versions of the Software and optional add-on packages. The applicable parameters such as scope of support, amount of fee, period of storage of transaction data processed with the Software are notified to the Customer in the contract.

(3) The contract is the only binding document. There are no additional oral agreements between the parties. Terms and conditions of the Customer which are inconsistent or in conflict with the present General Terms and Conditions shall not apply; this applies even if INFORM does not expressly reject the terms and conditions of the Customer. In case Customer and INFORM agree upon individual contract terms and conditions such terms and conditions shall prevail with regards to these Terms and Conditions.

(4) Unilateral amendments to these Terms with effect on existing contracts may only be made to the extent that the equivalence ratio between performance and consideration is not unreasonably changed to the detriment of the Customer as a result. INFORM has the right to change these Terms in this context. New versions of the Terms shall be communicated to the Customer in writing or by e-mail, highlighting the changes. They shall take effect if the Customer does not object to the new version in writing within six weeks of receipt of the notification of change. The consequences of its inaction must be explicitly stated to the Customer in the notice of change. If the Customer rejects the revised Terms, the contractual relationship shall continue on the original Terms, but may be terminated by INFORM for good cause with a period of notice of three months.

§ 2 Conclusion of the Contract

(1) The description of the Software on the website is not a legally binding offer from INFORM, but only a non-binding invitation to the Customer to submit an offer for its part. With the conclusion of the order of the Customer by clicking the order button, the Customer makes a binding offer to conclude a contract. Before concluding the order, the Customer can on a separate page check its order and contract data again and if necessary make corrections (e.g. selecting another Software version).

(2) INFORM shall acknowledge the receipt of the electronic order of the Customer by sending an automatic confirmation of receipt by e-mail. This confirmation does not constitute a binding acceptance of the Customer's offer. It merely serves to inform the Customer of the arrival of its order. The contract is only concluded with the activation of Customer account. INFORM is free to not accept orders from the Customer; the decision is at the sole discretion of INFORM.

(3) After an electronic order from the Customer, the individual order and contract data of the Customer of INFORM are stored on the website of INFORM. INFORM is entitled to contact the Customer to prove his identity and clarify any questions about the order. The Customer can inspect and supplement order and contact data after activation of its Customer account with the role "Company Admin" through the user interface of the Software. In addition, each Customer is again sent after approval a summary of the order and contract data (together with the Terms included in the contract). The version of these General Terms and Conditions currently in force is also available and printable on the INFORM website at all times. Contracts via the website are concluded in German and/or English.

§ 3 Special Provisions During the Trial Period

(1) The contract period begins with a Trial Period during which the Software can be used free of charge. The term of this Trial Period is specified in the order and may be extended by INFORM upon Customer’s request in particular cases.

(2) During this Trial Period the Customer may use the unrestricted functionality of the selected Edition, build up the operational master data and test the workflow. The contract data needed for subsequent invoicing should be completed until the first turn of the month to ensure the smooth operation even in this process.

(3) The Customer will be made aware of the end of the cost-free Trial Period in due time by e-mail. Until the end of the Trial Period both Parties shall have the right to termination this contract for cause without notice. In deviation of the other provisions of this contract, for such termination during the Trial Period the textual form is sufficient, meaning that – for example - the consignment via e-mail to cloud-support@inform-software.com shall be valid and binding.

§ 4 Main Services; Functionality of the Software

(1) INFORM provides the Customer for the duration of the contract the Software in the currently released version within the agreed availability (see. SLA in Annex B) for use via the internet. There is no permanent release of the Software (purchase). In addition to the Software, the Customer is given electronic user documentation as online help in German.

(2) If INFORM, during the contract period, develops additional modules, language versions and/or new features of the Software, it may include them in its sole discretion in the standard Software and provide them to the Customer (e.g. as part of a regular update) without additional compensation or offer them separately to the Customer for a corresponding increase in the fee as part of new versions or chargeable additional packages. The Customer is not entitled to free provision of such newly developed modules, language versions or functionalities.

(3) INFORM provides the Customer during term of the contract with space in an external data centre to store its transaction data processed with the Software (hosting). The data is secured via the period applicable to the version of the Software chosen by the Customer on external servers that are operated on behalf of INFORM by third parties. The cost of storing the transaction data is covered by the uniform fee. The Customer is not entitled to allow a third party, for consideration or not, to use the space in whole or in part.

(4) INFORM is entitled to have the contracted services provided by third parties as subcontractors, and in particular INFORM uses the external data centre where it keeps the Software for use and the transaction data of the Customer is stored.

(5) In the context of the continuous improvement and development of the Software during the contract period, functions and services shall be added, altered or eliminated, unless this leads to a significant restriction of the contracted services, the purpose of the contract is threatened and as a result the adjustment is not reasonable for the Customer .

§ 5 Granting of Usage Rights

(1) The copyright and other intellectual property rights in the Software, including user documentation, are the exclusive property of INFORM in relation to the Customer. The Customer only receives the simple rights to use the Software described in more detail below.

(2) The Customer receives regarding the Software a non-exclusive, non-transferable, non-sublicensable and time-limited right to use the Software for the term of the contract and only for its own business purposes. All additional rights, especially the rights of reproduction, dissemination, including (further) leasing, processing and public access remain with INFORM. The Software may exclusively be used by the Customer for the purposes of the contract; the intended use of the Software is described in detail in the corresponding description of the applications on the INFORM website. Any deviation from the intended use of the Software is inadmissible.

(3) The Customer is not entitled to use the Software for business purposes of third parties or have it used by third parties for themselves or make it available to third parties. This does not apply to third parties which, in the written order of the Customer, are entrusted with activities in the context of the implementation of the transactions of the Customer.

(4) The transaction data belong to the Customer. He grants INFORM all the rights to the data transmitted by it necessary for fulfilling the contract, in particular for storing and processing its transaction data. Furthermore INFORM receives from the Customer the right to use transaction data processed with the Software for analysis and benchmarking purposes on an anonymous basis and merge it with other data, reproduce it and process it. INFORM thereby ensures that the Customer, on any publication of the results for third parties, is not (even indirectly) identifiable. Any other use of the transaction data by INFORM or transfer of non-anonymised transaction data to third parties is not permitted.

§ 6 Services

INFORM performs during the term of this contract the services described in detail in this § 6 and - unless otherwise stated below - covered by the single transaction fee:

(1) INFORM shall provide the Customer with the Software during the contract period under the agreed availability (see SLA in Annex B) in a form operational for use and shall service it. The Customer will be centrally provided during the contract period by INFORM with generally released updates of the Software.

(2) For questions about the application and use of the Software, the Customer shall during the term of its contract have access to online help in the Customer portal. In the event of faults and errors, which prevent the use of the Software in whole or in part, the Customer can contact the service e-mail address cloud-support@inform-software.com. If the Customer uses the Enterprise Edition of the Software, it also has access, on the occurrence of usage-preventing faults and errors, to a hotline. Details can be found in the latest available version of Annex B - Service Level Agreement (SLA).

(3) The Customer will describe occurring faults and errors in the Software in sufficient detail that they can be reproduced and understood by INFORM. Duly issued error messages will be resolved by INFORM within its maintenance responsibility as detailed in § 8 and the provisions of the SLA in Annex B.

(4) At the request of the Customer, INFORM shall provide optional advisory and support services for the introduction and application of the Software, such as configuration support, training of the Customer or commissioning support staff. This also includes the individual provision of all stored transaction data in a form specified by the customer. These services are provided by INFORM in line with the Customer's

requirements and in accordance with the applicable year's price list or the INFORM training conditions and charged separately according to cost.

§ 7 Responsibility and Cooperation of the Customer

(1) The Customer shall provide all cooperation services required for use of the Software, especially the services listed and described in this § 7, in § 10 and the Annexes in detail.

(2) The Customer is responsible for ensuring the satisfaction, as necessary for the contractual commissioning and use of the Software and as described by INFORM in Annex A, the technical minimum requirements of the hardware and software used and its internet connection. The Customer is itself responsible for procurement of a suitable internet browser, with which access to the Software is possible. The Customer may not use any software or other technical facilities that could jeopardize the functioning of the Software. In particular the Customer is not allowed to gain access with other technical means than those listed in Annex A to the Software and its transaction data.

(3) The Customer agrees not to store content on the memory whose transmission, storage or use is prohibited by law or agreements with third parties (e.g. for secrecy). The Customer shall not manipulate the Software and store any data on the servers of INFORM that damages or jeopardises the Software, the servers, the other IT infrastructure or data of other customers. It shall also not use the data of other customer and not load the space provided with exceptionally large data volumes that are not required to process its transactions.

(4) The Customer bears the sole responsibility for compliance with all legal requirements for its transaction processing and the storage, custody and archiving of its transaction data. This includes compliance with the retention periods of general commercial and tax law as well as, if applicable, compliance with specific (e.g. industry-related) obligations and deadlines (e.g. for certain environmental data). The Customer shall take, within its duty to mitigate damages, reasonable measures in the event of data loss, especially by regular review of its own IT systems and the regular production of backup of its transaction data processed with the Software through the export function provided by INFORM for this purpose.

(5) Costs incurred by INFORM for the absent, delayed or improper intervention of the Customer, in particular through the use of antiquated or incorrect interfaces, mishandling of the Software, data which is incorrect, incomplete, inconsistent, outdated or not consistent with the requirements of INFORM or scheduling delays caused by the Customer shall be charged to the Customer separately at cost according to the valid price list of INFORM for the year. Further rights of INFORM remain unaffected.

§ 8 Warranty

(1) INFORM does not warrant the results and expenditure achieved with the Software, in particular their timeliness, correctness, quality and completeness, insofar as they are based on Customer input. The transaction data entered by the Customer is not checked or corrected either by INFORM or by the Software for accuracy.

(2) INFORM warrants that the Software meets the product description on the website www.inform-software.com and the user documentation and is free of third-party rights that prevent or restrict the contractual use of the Software. Claims may only be made by the Customer due to defects that are reproducible or can be intelligibly described by the Customer. A defect is in particular not functional limitations of the Software resulting from the hardware or software environment of the Customer, invalid data, improper use or other circumstances derived from the responsibility of the Customer. INFORM shall not accept liability for links of the Software not created by INFORM to the systems of the Customer.

(3) Properly alleged defects of the Software shall be removed by INFORM during the term of this contract within the scope of the maintenance and repair obligations covered by the fee, within a reasonable period and as detailed in the SLA in Annex B.

(4) The right of termination pursuant to § 543 para. 2 no. 1 BGB may only be asserted by the Customer if it has previously given INFORM an appropriate written period of at least two weeks for subsequent performance and the deadline has passed without result.

(5) Damages and compensation for wasted expenditure shall be paid by INFORM only within the limits of § 9.

§ 9 Liability

(1) If INFORM perform services for the Customer without the need for remuneration, e.g. the release of the Software during an unpaid test phase, INFORM shall only be liable for intentional or grossly negligent violation of duty.

(2) For defects in the Software that were already present at the conclusion of the contract, INFORM shall, contrary the statutory provision of § 536 BGB, be liable only if INFORM is responsible for such defects.

(3) Notwithstanding the above, Inform shall be liable for damages for any legal reason only in accordance with the following provisions:

a. Wilful misconduct and gross negligence

Unlimited liability for damages caused by the wilful misconduct or gross negligence of INFORM or its vicarious agents (“Erfüllungsgehilfen”) or legal representatives (“gesetzliche Vertreter”).

b. Personal injuries

In the event of damage resulting from injury to life, body or health, liability shall be unlimited, even in the event of a negligent breach of duty (“einfach fahrlässige Pflichtverletzung”) by INFORM or a legal representative or vicarious agent of INFORM.

c. Organisational fault (“Organisationsverschulden”) and guarantee

Liability is also unlimited in terms of amount for damages caused by serious organisational fault of INFORM and for damage caused by the absence of a guaranteed quality (“garantierte Beschaffenheit”), guaranteed performance (“garantierter Leistungserfolg”) or the assumption of a procurement risk (“Beschaffungsrisiko”).

d. Breach of essential contractual obligations (“wesentliche Vertragspflichten”)

In the case of material and financial losses caused by the negligence of INFORM and its vicarious agents or legal representatives are liable for the violation of essential contractual obligations if none of the cases mentioned above in a. to c. and in f. is given, but the amount is limited to the damage foreseeable and typical (“vorhersehbare und vertragstypische Schäden”) for the contract at the time of conclusion of the contract but limited to the amount of the net amount of this contract (“Netto-Auftragssumme”); essential contractual obligations are those whose fulfilment characterizes the contract and on which the customer may rely.

e. Disclaimer of liability

Any further liability for damages, in particular liability without fault, is excluded.

f. Product Liability Act (“Produkthaftungsgesetz”)

Liability under the Product Liability Act remains unaffected.

g. Contributory negligence (“Mitverschulden”)

If damage is attributable both to fault on the part of INFORM and to fault on the part of customer, customer shall have his contributory negligence taken into account.

h. Data security

The customer is responsible for the regular backup of his data. In the event of data loss for which INFORM is responsible, INFORM shall therefore be liable exclusively for the costs of copying the data, the backups to be made and for the costs of restoring the data, which would also have been lost if the data had been properly backed up, unless a case mentioned in letters a. to c. and f. exists.

§ 10 Secrecy; Access Data; Data Protection; Data Security

(1) The Parties mutually agree to treat confidential information and documents of the other Party, which are either clearly to be regarded as confidential or are designated by the other Party as confidential, as business and commercial secrets. The Customer shall in particular treat all programs, documentation, and other documents made available by INFORM as business and commercial secrets of INFORM and not disclose them to unauthorised third parties.

(2) The Software may only be used by employees of the Customer as well as third parties commissioned in writing by the Customer which support the customer in the implementation of its workorder (in case of using SYNCROSUPPLY for example the logistics service providers or freight forwarders of the Customer). Such third parties must provide a secrecy commitment in writing before accessing the Software. Other third parties may not enable the Customer to use the Software and gain access to the cloud interface either directly or indirectly.

(3) The Customer may not pass on its personal login data regarding the Customer account or to the cloud interface of the Software to any unauthorised third party. All access data must be stored and protected in such a way that others cannot access it. The Customer shall notify INFORM promptly if there is a suspicion that unauthorised third parties might have gained knowledge of them. In the event of suspicion of unauthorised access to the data by third parties, INFORM is authorised temporarily to block access of the Customer to its Customer account or to the cloud interface of the Software.

(4) INFORM uses an external data centre or data centre operator to perform its contractual obligations. The Customer has no right to the involvement and use of a specific data centre operator. INFORM shall, however, always make sure that the data centres used are within the EU and that - according to the information of the computer centre operator - a transfer of Customer data to countries outside the EU does not take place. The browser connection to the data centre shall be SSL encrypted. The relevant security procedures in the external data centre include, in particular, physical security, logical security, operational security and data protection.

(5) The Customer processes and stores with the hardware and Software provided only its own operational transaction data. If the data provided to INFORM by the Customer have a personal reference, the Customer is responsible as the responsible entity for compliance with data protection regulations. The Customer shall ensure that the relevant legal requirements for processing and transmission by INFORM are met. In order to ensure self-disclosure by the enduser in accordance with the European General Data Protection Regulation GDPR it has to be urgently ensure that input fields must be filled out purposefully and free text fields (e.g. remark fields) are not filled with any personal data, e.g. UserID, name, telephone number, email addresses, etc. The customer accepts the Data Processessing Agreement (DPA), attached in Annex C. INFORM is entitled to pass on the data provided to the operator of the external computer centre commissioned for the purpose of fulfilling the contract.

(6) Sensitive customer data and personal data are processed as part of the customer project. Not only for aspects of the software but also for the processing of the data the compliance with a security level based on ISO/IEC 27001 is aimed at. INFORM classifies information within customer projects as confidential, which includes appropriate measures for secure communication and data exchange between the customer and INFORM , including the use of state-of-the-art secure transport encryption on both sides. In order to ensure this security, the Customer undertakes to report any breaches of information security and data protection (security incidents) affecting INFORM to INFORM immediately. The report must be made to the relevant INFORM contacts and via email to Security-Incident@inform-software.com. If the incident involves personal data of INFORM, this must be reported to Privacy@inform-software.com in addition to the provisions in the DPA (Annex C). Security incidents affecting the respective customer at INFORM are also reported vice versa.

§ 11 Term and Termination

(1) The contract has an initial term until 31.12. of the calendar year following the conclusion of the contract. It is then extended in each case by another calendar year if it is not terminated by either Party with notice of three (3) months before the expiry of each period.

(2) An upgrade to a higher version and/or an entry of additional packages is possible at any time with an implementation period of usually one to three business days. The initial contract period is unaffected. A downgrade to a lower version is available at the end of each contract period and must be notified by the Customer at the latest one working week before the end of each contract period. With the entry into effect of the conversion, the level of remuneration for the following transactions is adjusted accordingly.

(3) The right of both Parties to a termination for cause remains unaffected. Such cause exists for INFORM especially if the Customer is in default of payment with a significant portion of the fee or in any other way breaches its material obligations arising from the contract. At its choice, INFORM, in the event of such a cause, can first temporarily block the Customer's access to the cloud interface of the Software as well as the Customer's access to its transaction data and invite the Customer with a reasonable deadline to remedy the breach of duty or fulfil the contract. Further rights of INFORM remain unaffected.

(4) INFORM may also terminate the contract for cause at any time with immediate effect if the Customer has not performed any transaction requiring payment with the Software over a period of at least 12 months.

(5) The Parties shall comply with all applicable export and import control regulations and shall observe all national and foreign trade restrictions. If one Party is unable to perform its obligations under the Agreement due to such restrictions, it shall have the right to terminate the Agreement without notice period. In this case, claims for damages are excluded for both Parties.

(6) Any termination shall be invalid unless made in writing.

(7) INFORM is not obliged to save the data of the Customer beyond the date of termination of this contract, archive it and/or reserve it for access by the Customer.

§ 12 Remuneration and Terms of Payment

(1) The remuneration for the contractual services takes the form of a base fee plus a transaction-dependent usage fee (togeteher hereinafter “fee”). The transaction-dependent usage fee may be designed for usage fee per single transaction or staggered according to transaction blocks. The amount of the fee is based on the Software version chosen by the Customer on the conclusion of the contract, the selected additional packages and secondly the number of transactions/transaction blocks (in the sense of truck approach in SYNCROSUPPLY) which the Customer processes with the Software (pay-per-use model). The number of transactions shall be recorded and stored automatically and transparently by the system; the Customer can view the current number of its transactions at any time through its Customer account.

(2) The fee shall be charged by INFORM monthly at the beginning of a calendar month for the previous month. If the invoice amount falls below the minimum amount of € 300, INFORM reserves the right to postpone the settlement of this amount into the subsequent billing cycle. The invoice shall be sent to the Customer as a pdf document by email to the email address entered by it in its Customer account.

(3) INFORM has the right to adjust the base fee as well as the usage fee per transaction/transaction block by written or e-mail notice with a period of notice of six weeks to the end of the calendar year in accordance with the general price trend (taking into account the development of the German Consumer Price Index, see. www.destatis.de). This adjustment must not exceed the fee of the preceding calendar year by more than 10%. If an increase in the fee by more than 5% occurs, the Customer can cancel the contract with written notice of four weeks to the end of the calendar year.

(4) Services that the Customer has to pay for separately at cost, shall be invoiced on a monthly basis at the beginning of the following month. Unless otherwise agreed in individual cases, the hourly rates of the latest annual price list of INFORM will apply. Travel times with on-site operations of employees of INFORM shall be recorded as working hours, summarised separately and invoiced to the Customer at cost. Travel costs and travel expenses shall be invoiced for the actual amount incurred.

(5) All fee components are exclusive of the applicable VAT. Payments shall be made by the Customer within 30 calendar days from the invoice date. Objections to the invoice by the Customer must be submitted within 14 calendar days in writing from invoice date with a statement of reasons.

(6) If the Customer defaults on the payment of the fee, INFORM is entitled, after notice and a reasonable grace period (with a threat of blockage), to block access of the Customer to the cloud interface of the Software and the Customer's access to its transaction data until the complete settlement of all outstanding and payable invoices. Further rights of INFORM due to late payment (specifically an extraordinary termination of the contract) remain unaffected.

§ 13 Final provisions

(1) If the Customer agrees to be named as a reference client, INFORM is entitled to publish logos, brands and names of the Customer in reference lists and technical articles (in print and online format), possibly in conjunction with comments agreed in content (e.g. press releases). This approval may at any time be revoked in writing or by email to cloud-support@inform-software.com.

(2) Changes and additions to the contract shall be effective only in writing. The repeal of this written form requirement must also be in writing. The written form requirement under this contract is met by transmission by fax (but not by email, unless otherwise specified in this contract).

(3) If any provision of this contract is or becomes invalid or unenforceable, the validity of the remaining provisions shall not be affected. The invalid or unenforceable provision must be replaced by the Parties by mutual agreement with a commercially equivalent provision so far as possible. The same applies to contractual loopholes.

(4) The Customer may only transfer rights and obligations under this contract to a third party with prior written consent of INFORM.

(5) INFORM complies with the minimum wage law and commits itself to ensure that its subcontractors do the same.

(6) This contract shall be governed exclusively by the law of the Federal Republic of Germany, to the exclusion of the UN Sales Convention. The legal venue for all disputes arising out of this contractual relationship is Aachen.

Annex A - Technical Requirements

The following technical requirements for the use of the Software must be observed by the Customer or established and maintained during the contractual lifetime:

1. **Supported browsers**
   For access to the user interface of the Software, we recommend using the following browsers:
   - Mozilla Firefox,
   - Google Chrome,
   - Microsoft Internet Explorer,
   - Microsoft Edge oder
   - Apple Safari

   in the latest version. Browser versions whose support by the respective manufacturer has expired are generally not supported.

   JavaScript execution and fading in of pop-up windows must be allowed and Compatibility Mode must be deactivated when using the Internet Explorer.

2. **Monitor resolution**
   The user interface of the Software requires a minimum monitor resolution of 1920 x 1080 pixel (HD-Format). At lower resolutions, full operation, for example, because of non-display of controls, cannot be warranted.

3. **Internet connection**
   A sufficient working speed is influenced by many factors. In addition to the infrastructure used (landline/mobile) to access the internet, the transmitted data volume in each case and the complexity of the Software, e.g. the simultaneous access of different system users, are also influential parameters. A general minimum bandwidth requirement for the internet connection cannot therefore really be defined.
   As a rule of thumb for the bandwidth of the network, it can be said that for trouble-free operation of the software by up to 10 users accessing simultaneously from the same network, the minimum requirement for the download speed actually available via the Internet is 1 Mbit/s for 100 truck arrivals per day. For 1000 truck arrivals, the requirement increases to 4 Mbit/s. The upload rate requirement is 10% of the download rate.

4. **Password policy**
   For security reasons, each user of the Software must choose a password which meets the usual security criteria. Appropriate rules and regulations when setting the password are predetermined by the Software. The conscious use of personal security-relevant information is the responsibility of each user.
   Multiple unsuccessful access attempts with the password shall result in the suspension of the user account.

Annex B - Service Level Agreement (SLA)

This SLA regulates the availability and fault processing of the Software.

A. Service Hours

The service hours are Monday to Friday 8:30 to 16:30, excluding german public or company holidays, as well as 24. and 31. December.

In the Enterprise Edition, the service hours can be expanded by adding a corresponding additional package up to a 24/7 service (24 hours, 7 days a week). Information about the reserved version and the reserved additional packages can be found in the order confirmation and on the user interface of the Software, such that contract information can only be seen by the user role "Company Admin".

B. Availability

INFORM warrants availability of the Software (including access to the transaction data stored by the Customer) at the output of the data centre authorised by INFORM of 99% on the calendar year average. Unavailability is assumed if the Software is not available to the Customer due to circumstances that are the responsibility of INFORM. Unavailability is in particular not to be assumed if due to

- incorrect operation or noncontractual use by the Customer,
- planned and announced maintenance,
- technical problems beyond the control of INFORM or
- force majeure

the Software is not available.

INFORM shall implement planned maintenance so far as possible outside the service hours and complete them by schedule and notify the Customer by email in such a way that they inconvenience the Customer as little as possible. Overall, the duration of scheduled maintenance work may not exceed 10 hours a month.

INFORM may limit the Customer's access temporarily if the security of network operations, maintenance of network integrity, the prevention of server network problems, the software, and/or data stored by the Customer so require. INFORM shall take such a decision in the legitimate interests of the clients with adequate consideration, inform the Customer of the measures taken immediately and take all reasonable steps as soon as possible to remove the access restriction again.

C. Troubleshooting

Communication

All communication on fault processing is carried out between the Customer administrator (user role "Admin") or his representative (as *Single Point Of Contact* on the part of the Customer) and the support team of INFORM, accessible via the service e-mail cloud-support@inform-software.com.

In the Enterprise Edition, the Customer administrator also has the telephone service hotline. The service hotline has the same service hours and service levels as for the email service.

Service Level

Each reported fault associate shall be associated with a service level. This is defined by the severity and urgency of the effects. An individual and non-automated response to a fault notice shall be made within the service time.

Fault class	Target solution after reaction	Description
1	8 hours (within the service time)	Total failure Non-availability
2	2 INFORM business days	Failure of partial functions e.g. requests for time slot bookings are not answered by the Software
3	1 business week	Limited operability e.g. master data cannot be maintained
4	After the notice	Slightly restricted usability e.g. wrong colouring or marking

If the fault notice of Customer arrives outside the service hours, the counting of the response and resolution times commences with the start of the service time of the next working day. If the fault report of the Customer arrives within the service hours, any residual reaction or solution time which has not expired at the end of the service time of that day continues from the start of the service time of the next business day.

Faults may only be reported to INFORM by the appropriately authorised contact of the Customer (Admin or representative); he acts with respect to INFORM as the *Single Point Of Contact*. The contact of the Customer must be qualified and familiar with the handling of the Software.

The Parties shall allocate properly reported faults by agreement to the fault class is described. In the event that the Parties cannot agree on the fault class, the binding classification is performed by INFORM, taking due account of the interests of the Customer.

The desired solution times do not begin until proper and complete notification of the fault (see above) by the Customer and the release of all the necessary and useful documents, information and data to INFORM, which are related to the fault and enable INFORM to analyse and reproduce the reported fault. Periods in which INFORM, for reasons not related to its own area of responsibility, is prevented from providing support services and/or in which INFORM is waiting for the provision of necessary cooperation services (see above) or the necessary decisions to be taken by the Customer, are disregarded when calculating the desired solution times.

Full Fault Notice

A fault notice must be complete. The following is the required information to be transmitted on availability and relevance.
In the subject line of the email:

- proposed fault class
- customer name and location
- tags of the fault.

In the body of the email there must be a short, concise description of the problem with the following details:

- A screenshot of the entire screen content. Important points should be highlighted.
- Exact date of occurrence of the fault, or the multiple or prolonged occurrence
    - First occurrence of the fault or
    - Frequency of the fault
- Course of the fault
    - Step by step description
    - Expected (normal) behaviour
- Examples with associated identifications. e.g.UserID, order number, etc.

Duty to Cooperate

To minimise the effects of faults, the Customer has the following duties:

- The Customer creates and maintains emergency plans for different interference scenarios.
- The Customer maintains master data and configurations. It makes sure that they are complete and correct and do not contain any logical inconsistencies.
- The Customer shall ensure that all entries in the applications are complete and correct and do not contain any logical inconsistencies.
- The Customer reports occurring faults immediately to the service email address.
- The Customer supports INFORM for troubleshooting and analysis to a reasonable extent.

Annex C – Data Processing Agreement (DPA)

Preamble

The following standard contractual clauses for commissioned processing (hereinafter "DPA") were issued by the EU Commission on the basis of Article 28 Para. 7 GDPR and apply to INFORM (hereinafter referred to as "Processor") and the Customer (hereinafter "Controller"), but not directly to the Customer's employees or other third parties that the Customer involves in the use of the Software.

In case of contradictions between this DPA and other provisions of the GTC, the DPA shall prevail.

Standard contractual clauses

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 controllers and processors listed in Annex I 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

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 four weeks 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.

a) 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.

b) 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.

c) 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.

d) 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
List of parties

Controller:

Customer

Processor:

INFORM Institut für Operations Research und Management GmbH
Pascalstraße 35, 52076 Aachen, Germany

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

ANNEX II
Description of the processing

Categories of data subjects whose personal data is processed:

Employees, temporary workers, trainees, support staff, customers, service providers

Categories of personal data processed

User: General personal data (name, first name, language)
Identification number (User Code, password)
Organizational data (organization, role)
Contact data (phone)
Driver: General personal data (name, language)
Identification number (license plate truck, license plate trailer)
Organization data (organization)
Contact data (telephone)
Online data (GPS location data)

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.

No sensitive data, according to GDPR, will be processed.

Nature of the processing

Permanent processing of the data and operation of the software in a data center. Planned and unplanned maintenance in the event of errors and software maintenance or support of the Controller specify the type of data processing in detail per individual case.

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

Provision of software functionality via the Internet, planned and unplanned maintenance in the event of errors, software maintenance, support of the Controller.

Duration of the processing

The processing of the data and the operation of the software in the data center ends with the end of the contract. In the event of error messages or software maintenance to be carried out, the software system installed at the hosting service provider (subcontracted processor) is accessed via remote service. In this case, the data files, including the personal data of the users and drivers, are visible to the specially sensitized and trained INFORM employee. The duration of the processing depends on the duration of the error correction.

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

Cf. to this extent Annex IV.

ANNEX III

Technical and organisational measures including technical and organisational measures to ensure the security of the data

EXPLANATORY NOTE:
The technical and organisational measures need to be described concretely and not in a generic manner.
Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:
Measures of pseudonymisation and encryption of personal data
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
Measures for user identification and authorisation Measures for the protection of data during transmission
Measures for the protection of data during storage
Measures for ensuring physical security of locations at which personal data are processed Measures for ensuring events logging
Measures for ensuring system configuration, including default configuration Measures for internal IT and IT security governance and management Measures for certification/assurance of processes and products
Measures for ensuring data minimisation Measures for ensuring data quality Measures for ensuring limited data retention Measures for ensuring accountability
Measures for allowing data portability and ensuring erasure]
For transfers to (sub-) processors, alsodescribe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller
Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

In addition to the details of the processor, the security certifications and technical and organizational security measures of the sub-processors used from Annex IV shall apply.

Safety certificates of INFORM, Manufacturing Logistics Division

ISO 27001 was certified by TÜV Rheinland.
The result is available at
https://www.certipedia.com/quality_marks/9000021449

The current audit report is valid until 2025, May 16th.

The assessment result is exclusively available
via the ENX portal at
https://portal.enx.com/en-US/TISAX/tisaxassessmentresults/

The current report is valid until 2025, May 13th.

The Cloud Vendor Assessment ISA/CVA, supervised by the
Deutsche Cyber-Sicherheitsorganisation GmbH,
was successfully passed.

The current report is valid until 2026, March 2nd.

Technical and Organisational Measures of INFORM (v7, dated September 2023)

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	☒
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	☒
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	☒

1.2 Access Control to Systems (Hardware access control)

Access control to systems The intrusion of unauthorised 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)	☒
▪ Prevention of trivial passwords	☒

▪ Password history (no re-use of the last 10 passwords)	☒
▪ Other: Change of password after 180 days max.	☒
▪ Scanning of AD passwords for compromise	☒
Hashing of stored passwords	☒
Procedure for the assignment of authorisations with the entry of employees	☒
Procedure for revocation of authorisations due to department change of employees	☒
Procedure for revocation of authorisations due to exit of employees	☒
Obligation to confidentiality / 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 Unauthorised activities in data processing systems outside of assigned authorisations must be prevented.	**existent** yes
Definition of access authorization, authorization concept	☒
Definition of the authority 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 query options for databases	☒
Time limitation of access possibilities	☒
Access to data stocks and functions (Read, Write, Execute)	☒
Use of appropriate security systems (software/hardware)?	
▪ Virus scanner	☒
▪ Firewalls	☒
▪ SPAM-Filter	☒
▪ Intrusion prevention (IPS)	☒
▪ Intrusion detection (IDS)	☒
Encrypted storage of data	
▪ Encryption algorithms used:	
▫ AES (128/256 bit), 3 DES, RSA (1024/2048 bit)	☒
▫ 3DES	☒
▫ RSA (1024/2048 bit)	☒
▪ 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:	
▪ 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 authorisations (profiles)	☒
Read, modify, delete	☒
Partial access to data or functions	☒
Field access in databases	☒
Organisational 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 authorised 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	☒
Keep 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)	☒

3.2 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	☒
Loadbalancer	☒
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	☒

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 /	☒
▪ 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 organisations 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 organisation	
▪ 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 behaviours on the daily processes with the least impact possible.	☒
▪ Occasion-based warning of threats and risks	☒

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

4.1 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 IT 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

The Parties acknowledge the use of the following sub-processors upon entering into this Agreement:

1. Name: *Microsoft Ireland Operations Ltd*
   Address: *Microsoft Plc,*
   Leopardstown South County Business Park Dublin 18
   D18 P521 Ireland

   Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

   INFORM-internal Communicationplatform MS Office 365 E5,
   a.o. with Teams incl. Telefone, Outlook, Sharepoint and OneDrive.

2. Name: *Amazon Web Services EMEA SARL*
   Address: *38 avenue John F. Kennedy*
   L-1855 Luxemburg

   Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

   Provision and operation of the data center for
   the software SYNCROSUPPLY