Contract for the processing of personal data on behalf of third parties (data processing agreement) as an annex to the main contract

Between
Ninox Software GmbH
Monbijoustrasse 3A
10117, Berlin, Germany

- hereinafter referred to as the "**Processor**" -.

and

- hereinafter referred to as "**Controller**" -
- both hereinafter referred to as "**the contracting parties**" -

All terms are gender-neutral.

the following order processing agreement is concluded:

Preamble and scope of application

This annex specifies the obligations of the contracting parties regarding data protection, which arise from the order processing described in the main contract and in Annex 1 (order processing contract). It applies to activities related to the contract in which

employees of the contractor or persons commissioned by the contractor process personal data on behalf of the customer. The processing order does not apply if the GDPR is not applicable to the processing of personal data by the Controller (for example, in the case of exclusively personal or family activities in accordance with Art. 2 (2) lit. c. GDPR) and the Processor therefore does not act as a Processor within the meaning of Art. 4 No. 8 GDPR.

1. Terms and definitions

a. "Commissioned processing" - In accordance with Article 4 No. 8 of the GDPR, "commissioned processing" shall mean the processing of personal data pursuant to Article 4 No. 2 of the GDPR by the Processor on behalf of the controller, irrespective of the number of interposed Processors, in accordance with the subject matter of this processing contract.

b. "Main Contract" - The term "Main Contract" includes all types of ongoing business relationships between the Controller and the Processor under which the Processor processes Personal Data on behalf of and at the direction of the Controller in accordance with the subject matter of the Processing in this Processing Agreement. Insofar as the applicability of this Processing Agreement has been limited elsewhere (i.e. within this Agreement or outside, in other contracts or regulations) to certain types, kinds or specific business relationships, contracts, etc., these shall each be understood as a main contract. The term main contract also includes ongoing individual orders placed by the Controller with the Processor under the main contract (e.g. in the case of framework contracts).

c. "Controller" - "Controller" is the person who alone or jointly with others determines the purposes and means of processing (Art. 4 No. 7 GDPR).

d. "Personal data" - "Personal data" (hereinafter also referred to as "data" for short) means, in accordance with Art. 4 No. 1 GDPR, any information relating to an identified or identifiable natural person (data subject); an identifiable natural

person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

e. "Data subjects" - In accordance with Art. 4 No. 1 GDPR, data subjects are persons who are at least identifiable by means of personal data. The data subjects affected by this commissioned processing result from the object of the commissioned processing.

f. "Third party" - "Third party" means, in accordance with Art. 4 No. 10 GDPR, any natural or legal person, public authority, agency or other body, other than the data subject, the controller, the Processor and the persons authorized to process the personal data under the direct responsibility of the controller or the Processor;

g. "Sub-processing" - If a Processor is not directly contracted by the controller but by a Processor of the controller, there is "sub-processing" and the Processors following the first Processor are referred to as "sub-Processors".

h. "Electronic format" - Declarations shall be deemed to have been made in "electronic format" in accordance with Art. 28 (9) GDPR if the person making the declaration is identifiable and the electronic declaration format is suitable for proving the declaration. Electronic format" is understood to mean in particular the text form, an agreement stored on durable data carriers (e.g. e-mail), digital signing procedures or use of dedicated online functions (e.g. in user accounts).

2. Subject matter of the processing

a. The order processing takes place within the framework of the following legal relationship (main contract): This order processing contract is part of and subject to the terms and conditions of the contract between Ninox Software GmbH (Ninox General Terms and Conditions of Business and Use) and the customer.

b. Detailed information on the object of the processing carried out on behalf of the Controller, the personal data processed, the persons affected by the processing as well as the type, scope and purpose of the processing shall be governed by the specifications in the Annex "Object of the data processing".

3. Type of order processing

Insofar as the Controller acts as the person responsible for the commissioned processing, it shall be responsible within the scope of this commissioned processing agreement for compliance with the provisions of the data protection laws, in particular for the lawfulness of the data processing as well as for the lawfulness of the commissioning of the Processor. Insofar as the Controller itself acts as a Processor, it shall commission the Processor as a sub-Processor. The controller of the processing may directly invoke the rights to which the Controller is entitled against the sub-Processor on the basis of this processing contract.

4. Authority

a. The Processor may only process personal data within the framework of the main contract and the instructions of the Controller and only insofar as the processing is necessary within the framework of the main contract.
b. The instructions shall initially be laid down by the main contract or this processing contract and may thereafter be amended, supplemented or replaced by the Controller by means of instructions in writing or in an electronic format (text form, e.g. e-mail) to the Processor or the entity designated by the Processor.
c. Verbal instructions may be given if they are required due to the circumstances (e.g. urgency) and must be confirmed immediately in writing or in electronic form.
d. If the Processor is of the opinion, based on objective circumstances, that an instruction of the Controller violates applicable data protection law, the Processor shall notify the Controller thereof without undue delay and provide factual

reasons for the opinion. In this case, the Processor shall be entitled to suspend the execution of the instruction until the Controller has expressly confirmed the instruction and to reject instructions that are obviously unlawful.

e. The Processor may be obliged to carry out processing operations or to communicate information by Union or Member State law and by administrative and judicial measures to which the Processor is subject. In such a case, the Processor shall communicate the legal requirements of the overriding legal obligation to the Controller prior to the processing, unless the law or order in question prohibits such communication on grounds of important public interest; in the case of a prohibition of communication, the Processor shall take possible and reasonable measures to prevent or restrict the legally overriding processing.
f. The Processor shall document instructions given to it and their implementation.
g. The Processor shall designate the contact persons authorised to receive instructions and shall be obliged to immediately notify any changes to the contact persons or their contact information as well as representatives in the event of a non-temporary absence or prevention.

5. Technical and organisational measures

a. The Processor shall organise the internal organisation in its area of responsibility in accordance with the legal requirements and shall in particular take technical and organisational measures (hereinafter referred to as "TOMs") to adequately safeguard, in particular, the confidentiality, integrity and availability of data of the Controller, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of the Data Subjects, and shall ensure that they are maintained, in particular by regular evaluation at least once a year. With regard to the protection of personal data, the TOMs include, in particular, access control, access control, disclosure control,

input control, order control, integrity and availability control, segregation control and the safeguarding of data subjects' rights.

b. The TOMs notified by the Processor upon conclusion of the contract define the minimum level of security owed by the Processor. The TOMs may be further developed in accordance with technical and legal progress and replaced by adequate protective measures, provided that they do not fall below the security level of the specified measures and significant changes are communicated to the Controller. The description of the measures must be so detailed that a knowledgeable third party can at any time undoubtedly see from the description alone that the required legal level of data protection and the defined minimum level of security are not undercut.

c. The Processor shall ensure that the employees, agents and other persons working for the Processor who are involved in the processing of the Data are prohibited from processing the Personal Data outside the scope of the instruction. The Processor shall further ensure that the persons authorised to process the Controller's Data have been instructed in the data protection provisions of law and of this Data Processing Agreement and have been bound to confidentiality and secrecy or are subject to a corresponding and appropriate legal obligation of secrecy. The Processor shall ensure that persons deployed for the purpose of processing the order are appropriately instructed on an ongoing basis with regard to compliance with the data protection requirements.

d. The Processor shall ensure that its data controllers participate in recurrent training and awareness-raising activities with an appropriate frequency with regard to the protection of personal data and compliance with data protection law.

e. The processing of personal data outside the Processor's business premises (e.g. in the home or mobile office or in the case of remote access) is permissible,

provided that the necessary technical and organisational measures are taken and documented which adequately take into account the special features of these processing situations and, in particular, also enable sufficient control of the data processing (e.g. conclusion of an agreement on data protection in the home and mobile office with employees). The Processor shall provide the Controller with documentation of the implemented technical and organisational measures for such home, mobile or other remote processing upon request.

f. The processing of personal data on private devices of the employees of the Processor and agent is only permitted with the consent of the Controller.

g. If required by law, the Processor shall appoint a data protection officer who complies with the legal requirements. The Processor shall inform the Controller of the contact details of the Data Protection Officer and of any subsequent changes.

h. The Processing Processes carried out for the Controller shall be documented separately by the Processor to an appropriate extent, in a register of Processing Activities and provided to the Controller upon request.

i. The data provided within the scope of the order processing contract as well as data carriers and all copies made thereof shall remain the property or ownership of the Controller, shall be subject to the Controller's control, shall be carefully stored by the Processor, shall be protected against access by unauthorised third parties and may only be destroyed with the Controller's consent. The destruction shall be carried out in accordance with data protection and in such a way that a recovery of even residual information is no longer possible with reasonable effort and is not to be expected. Copies of data may only be made if they are necessary for the fulfilment of the main and secondary obligations of the Processor towards the Controller (e.g. backups) and the contractual and statutory level of data protection is guaranteed.

j. The Processor shall be obliged to bring about the return or deletion of the data and data carriers without undue delay, also in the case of sub-Processors, in accordance with this Processing Agreement.

k. The Processor shall keep proof of the destruction or deletion of data and files duly carried out within the scope of this Contract and make it available to the Controller upon request.

l. The defence of a right of retention is excluded with regard to the data processed in the order and the associated data carriers.

m. The Processor shall provide regular evidence of the fulfilment of its obligations, in particular the full implementation of the agreed technical and organisational measures as well as their effectiveness (e.g. by means of regular checks, audits, etc.) to an appropriate extent. The proof shall be provided to the Controller upon request. The proof can be provided by approved rules of conduct or an approved certification procedure.

n. Insofar as the security measures taken do not or no longer meet the requirements of the Processor or the statutory requirements, the Processor shall notify the Controller without delay.

o. The technical and organisational measures already in place at the time of the conclusion of this Order Processing Agreement are listed by the Processor in the Annex "Technical and Organisational Measures" and accepted by the Controller.

6. Information and cooperation obligations of the Processor

a. The Processor may only provide information to third parties or the Data Subject with the prior consent of the Controller or in the case of mandatory legal obligations, judicial or statutory information. If a data subject approaches the Processor and asserts his or her data subject rights (in particular rights to information or correction, or deletion of personal data), the Processor shall refer the data subject to the Controller, provided that an assignment to the Controller

is possible according to the data subject's information. The Processor shall forward the Data Subject's request to the Controller without undue delay and shall assist the Controller to the extent reasonable and possible. The Processor shall not be liable if the request of the Data Subject is not answered by the Controller, is not answered correctly or is not answered in a timely manner, insofar as this is not the fault of the Processor.

b. The Processor shall immediately and fully inform the Controller if the Processor becomes aware of any errors or irregularities with regard to the processing of the Personal Data in complying with the provisions of this Processing Agreement and/or relevant data protection regulations. The Processor shall take the necessary measures to secure the Personal Data and to mitigate any possible adverse consequences for the Data Subjects and shall consult with the Controller without undue delay.

c. The Processor shall inform the Controller without undue delay if a supervisory authority takes action against the Processor and its activity may affect the data processed for the Controller. The Processor shall support the Controller in the performance of its obligations (in particular to provide information and to tolerate inspections) towards supervisory authorities.

d. If the security of the Controller's personal data is endangered by measures taken by third parties (e.g. creditors, authorities, courts, etc.) (attachment, seizure, insolvency proceedings, etc.), the Processor shall immediately inform the third parties that sovereignty and ownership of the data lie exclusively with the Controller and, after consultation with the Controller, take appropriate protective measures if necessary (e.g. file objections, applications, etc.).

e. The Processor shall provide the Controller with information concerning the processing of data under this Processing Agreement that is necessary for the fulfilment of the Controller's legal obligations (which may include, in particular,

requests from data subjects or public authorities and compliance with its accountability obligations of a data protection impact assessment).

f. The information obligations of the Processor initially extend to information available to the Processor, its employees and agents. The information does not have to be obtained from third party sources if the procurement could be carried out by the Controller within reasonable limits and no other agreement has been made.

7. Measures in the event of a threat to or breach of data protection

a. In the event that the Processor discovers facts that give reason to believe that the protection of personal data processed for the Controller could be violated within the meaning of Article 4 No. 12 of the GDPR, the Processor shall inform the Controller without undue delay and in full, take any necessary protective measures without undue delay, and assist in the fulfilment of the obligations incumbent on the Controller, in particular in connection with the notification of competent authorities or data subjects.

b. Information about a (possible) personal data breach must be provided without delay.

c. In accordance with Art. 33 (3) of the GDPR, the notification of the Processor must contain at least the following information:

    a. Description of the nature of the personal data breach, including, to the extent possible, the categories of data involved and the approximate number of individuals and personal data sets involved;

    b. the name and contact details of the data protection officer or other contact point for further information;

    c. a description of the likely consequences of the personal data breach (e.g. providing further details: identity theft, financial loss, etc.);

ninox

d. A description of the measures taken or proposed by the Processor to address the personal data breach and, where applicable, measures to mitigate its possible adverse effects

d. Significant disruptions in the execution of the order as well as violations of data protection provisions or the stipulations made in this order processing contract by the Processor or the persons employed by the Processor or the persons commissioned by the Processor shall also be notified without delay.

8. Reviews and inspections

a. The Controller shall have the right to monitor the Processor's compliance with the statutory requirements and the provisions of this Order Processing Agreement, in particular the TOMs, at any time to the extent necessary itself or through third parties and to carry out the necessary checks, including inspections.

b. The Processor shall support the Controller in the controls and inspections to the extent necessary (e.g. by providing personnel and granting access and access rights).

c. On-site inspections shall take place within normal business hours and shall be notified by the Controller with a reasonable period of notice (at least 14 days). In emergencies, i.e. if waiting would endanger the rights of the data subjects and/or the Controller to an unreasonable extent, a reasonably shorter period may be chosen. Conversely, a longer period may be necessary (e.g. if extensive preparations have to be made or during holiday periods). The deviations from the time limit shall be justified by the contracting party making use of them.

d. The controls shall be limited to the necessary scope and must take into account the Processor's trade and business secrets as well as the protection of personal data of third parties (e.g. other customers or employees of the Processor). Avoidable operational disruptions shall be avoided. Insofar as sufficient for the

reason and purpose of the inspection, inspections shall be limited to random samples.

e. Only competent persons who can legitimise themselves and who are bound to confidentiality and secrecy with regard to the Processor's business and trade secrets as well as internal processes and personal data shall be permitted to carry out the inspection. The Processor may request proof of a corresponding obligation. If the auditor engaged by the Controller is in a competitive relationship with the Processor or if there are otherwise reasonable grounds for its rejection, the Processor shall have a right of objection against it.

f. Instead of the inspections and on-site inspections, the Processor may refer the Controller to an equivalent inspection by independent third parties (e.g. neutral data protection auditors), compliance with approved codes of conduct (Art. 40 GDPR) or suitable data protection or IT security certifications pursuant to Art. 42 GDPR. This shall only apply if the reference is reasonable for the Controller and the type and scope of the audit and references correspond to the type and scope of the Controller's justified control project. The Processor undertakes to inform the Controller without undue delay of the exclusion of approved codes of conduct pursuant to Art. 41 (4) GDPR, the revocation of a certification pursuant to Art. 42 (7) and any other form of revocation or material change of the aforementioned evidence.

g. In principle, the Controller shall not exercise its right of inspection more frequently than every 12 months, unless a specific reason (in particular a breach of data protection, a security incident or the result of an audit) makes inspections necessary before the end of this period.

9. Subcontracting

a. Without prejudice to any restrictions imposed by the main contract, the Controller expressly agrees that the Processor may use sub-Processors within the scope of

the processing. The Processor shall inform the Controller of any new sub-Processors with reasonable advance notice, which shall normally be 14 working days, and shall give the Controller the opportunity to reasonably review the sub-Processors prior to their use and, if it has a legitimate interest, to object to the use of the sub-Processors. If the contracting authority does not object within the time limit, the sub-Processor may be used. The Controller shall only exercise its right to object with regard to the changes in compliance with the principles of good faith, reasonableness and fairness.

b. If the Processor uses the services of a sub-Processor (e.g. a sub-contractor) to carry out certain processing activities on behalf of the Controller, the Processor must impose on the sub-Processor, by way of a contract or other legal instrument permitted by law, the same data protection obligations to which the Processor has committed itself in this processing contract (in particular with regard to following instructions, complying with TOMs, providing information and tolerating checks).
c. The Processor shall carefully select the Sub-Processor with particular regard to the suitability and reliability to comply with the obligations under this Processing Agreement and the suitability of the TOMs taken by the Sub-Processor.
d. The Processor shall regularly verify compliance with the obligations of the sub-Processors, in particular the TOMs, to an appropriate extent. The audit and its result shall be documented in such a way that they are comprehensible to a competent third party. The documentation shall be presented to the contracting authority upon request. Instead of its own review, the Processor may refer to a review by independent third parties (e.g. neutral data protection auditors), compliance with approved codes of conduct (Art. 40 GDPR) or suitable data protection or IT security certifications pursuant to Art. 42 GDPR.

e. It must also be possible to effectively exercise the rights of the Controller vis-à-vis the sub-Processors. In particular, the Controller must be entitled to carry out checks at any time on sub-Processors or to have them carried out by third parties to the extent stipulated in this contract.

f. If the sub-Processor fails to comply with its data protection obligations, the Processor shall be liable for this vis-à-vis the Controller.

g. Processing of personal data which is not directly related to the provision of the main service under the main contract and where the Processor uses the services of third parties as a purely ancillary service in order to carry out its business activities (e.g. cleaning, security, maintenance, telecommunications or transport services) does not constitute sub-processing within the meaning of the above provisions of this Processing Agreement. Nevertheless, the Processor must ensure, e.g. by means of contractual agreements or notices and instructions, that the security of the data is not jeopardised and that the requirements of this processing agreement and the data protection regulations are complied with.

h. Subcontracting relationships notified to the Controller upon conclusion of this Order Processing Agreement shall be deemed approved to the notified extent subject to the provisions of this Order Processing Agreement on subcontracting relationships.

i. The subcontracting relationships already existing at the time of the conclusion of this Processing Agreement shall be listed by the Processor in the Annex "Subcontracting Relationships" and updated by the Processor.

10. Geographical area of the processing

a. Personal data is processed within the framework of commissioned processing in a member state of the European Union (EU) or in another contracting state of the Agreement on the European Economic Area (EEA).

b. Processing may take place in third countries provided that the special requirements of Art. 44 et seq. GDPR are met, i.e. in particular the EU Commission has determined an adequate level of data protection; b) on the basis of effective standard contractual clauses (SCC); or c) on the basis of recognised binding internal data protection regulations.

c. The approval of subcontracting relationships by the Controller within the scope of this commissioned processing agreement shall also extend to the spatial area of the commissioned processing.

11. Obligations of the Controller

a. The Controller shall inform the Processor immediately and in full if it discovers errors or irregularities in the order results, instructions or processing procedures with regard to data protection provisions.

b. The Controller shall designate the contact persons authorised to receive instructions and shall be obliged to notify any changes to the contact persons or their contact information as well as representatives without delay in the event of a non-temporary absence or prevention.

c. In the event of a claim being made against the Processor by data subjects, third companies, bodies or authorities with regard to any claims based on the processing of personal data within the scope of this Processing Agreement, the Customer undertakes to support the Processor in defending the claim within the scope of its possibilities and taking into account the degree of fault of the contracting parties.

12. Liability

The statutory liability regulations apply, in particular Art. 82 DSGVO and, in the case of the use of a subcontracted Processor, Art. 28 para. 4. p. 2 DSGVO.

13. Term, continuation after the end of the contract and data deletion

a. This Order Processing Agreement shall become effective upon its signature or conclusion in an electronic format.
b. The term and end of this order processing contract shall be based on the term and end of the main contract.
c. The right to extraordinary termination is reserved for the contracting parties, in particular in the event of a serious breach of the obligations and specifications of this order processing contract and the applicable data protection law. A serious breach shall be deemed to have occurred in particular if the Processor fails to fulfil or has failed to fulfil to a significant extent the obligations specified in the Processing Agreement and the agreed technical and organisational measures.
d. In the case of insignificant breaches of duty, the extraordinary termination shall be preceded by a warning of the breaches with a reasonable period of time to remedy the breach, whereby the warning shall not be required if it is not to be expected that the breaches complained of will be remedied or if they are so serious that the terminating contracting party cannot reasonably be expected to adhere to the order processing contract.
e. The termination of this order processing contract as well as the cancellation of this formal clause must at least be made in electronic format.
f. Upon completion of the provision of the Processing Services under this Processing Agreement, the Processor shall, at the option of the Controller, either destroy or return all Personal Data and copies thereof (as well as all documents, processing and usage results and data files that have come into its possession in connection with the contractual relationship), unless there is a legal obligation to store the Personal Data, in which case the Processor shall inform the Controller of the obligation and its scope, unless knowledge of the obligation on the part of the Controller can be expected. The destruction or deletion shall be carried out in

accordance with data protection law and in such a way that it is no longer possible or to be expected to restore even residual information with reasonable effort. The defence of a right of retention is excluded with regard to the processed data and the associated data carriers. With regard to deletion or return, the Controller's rights to information, proof and control shall apply in accordance with this order processing agreement.

g. The obligations to protect confidential information arising from the processing contract shall continue to apply after the end of the processing contract, provided that the Processor continues to process the personal data covered by the processing contract and compliance with the obligations is reasonable for the Processor even after the end of the contract.

14. Final provisions

a. The applicable law is determined by the main contract.
b. The place of jurisdiction is determined by the main contract.
c. This order processing contract represents the complete agreement reached between the contracting parties. There are no ancillary agreements.
d. With the conclusion of this commissioned processing contract, all possible previous contracts concluded between the contracting parties to this contract and which regulate the processing of personal data on behalf, if and insofar as these concern the same subject of the commissioned processing and if and insofar as nothing else has been expressly agreed in writing between the contracting parties, shall be cancelled.
e. Amendments and supplements to this order processing agreement as well as the cancellation of this formal clause must be made at least in electronic format.
f. In the event of any contradictions, the provisions of this data protection order processing agreement shall take precedence over the provisions of the main agreement.

g. Should one or more provisions of this order processing agreement be invalid or unenforceable, this shall not affect the validity of the remaining provisions. Instead, the invalid provisions shall be replaced by way of supplementary interpretation by a provision that comes as close as possible to the economic purpose that the contracting parties were recognizably pursuing with the invalid provision(s). If the aforementioned supplementary interpretation is not possible due to mandatory legal requirements, the contracting parties shall agree on a corresponding provision.

Annex 1: Subject of the order processing

Purposes of order processing

Personal data of the Controller shall be processed on the basis of this Order Processing Agreement for the following purposes:

An essential component of the software is the creation, administration and maintenance of databases. Among other things, users can create databases, enter and evaluate data, export them to other formats and save them on their end device. The service description is defined in the main contract (Ninox General Terms and Conditions of Business and Use).

Types and categories of data

The types and categories of personal data processed on the basis of this data processing agreement include:

a. Inventory data.
b. Contact details.
c. Contract data.
d. Payment data and billing data,
e. Protocol data.
f. Database contents (e.g. end customer data - if contained in the Controller's databases).

Categories of data subjects

The categories of persons affected by the processing of personal data on the basis of this commissioned processing agreement include:

a. Software users.
b. Consumers.
c. Business customers.
d. Employees/ workers.

Sources of the processed data

The data processed on the basis of this order processing agreement are collected or otherwise received from the sources mentioned below or within the framework of the procedures mentioned:

Inputs or information from the Controller.

Annex 2: Technical-organisational measures (TOMs)

A level of protection appropriate to the risk to the rights and freedoms of the natural persons concerned by the processing shall be ensured for the specific commissioned processing and the personal data processed in the context thereof. In particular, the protection objectives of confidentiality, integrity and availability of the systems and services as well as their resilience in relation to the nature, scope, circumstances and purposes of the processing operations shall be taken into account in such a way that the risk is permanently mitigated by appropriate technical and organisational measures.

Organisational measures

Organisational measures have been taken to ensure an adequate level of data protection and its maintenance.

a. The Processor has implemented an appropriate data protection management system or a data protection concept and ensures its implementation.
b. A suitable organisational structure for data security and data protection is in place and information security is integrated into company-wide processes and procedures
c. Internal safety guidelines are defined and communicated internally to employees as binding rules.
d. System and security tests, such as code scans and penetration tests, are carried out regularly and also on an ad hoc basis.
e. The development of the state of the art and as well as the developments, threats and security measures are continuously monitored and derived in an appropriate manner to the own security concept.
f. A concept is in place to ensure the protection of data subjects' rights by the Controller (in particular with regard to access, rectification, erasure or restriction of processing, data transfer, revocations & objections). The concept includes

informing employees about the information obligations vis-à-vis the Controller, setting up implementation procedures and appointing responsible persons as well as regular monitoring and evaluation of the measures taken.

g. A concept is in place to ensure a prompt response to threats and breaches of personal data protection in accordance with legal requirements. The concept includes informing employees about the information obligations vis-à-vis the Controller, setting up implementation procedures and appointing responsible persons as well as regular monitoring and evaluation of the measures taken.
h. Security incidents are consistently documented, even if they do not lead to an external report (e.g. to the supervisory authority, affected persons) (so-called "security reporting").
i. Sufficient professional qualification of the data protection officer for security-relevant issues and opportunities for further training in this specialist area.
j. Service providers used to perform ancillary tasks (maintenance, security, transport and cleaning services, freelancers, etc.) are carefully selected and it is ensured that they observe the protection of personal data. If the service providers gain access to personal data of the Controller in the course of their activities or if there is otherwise a risk of access to the personal data, they are specifically obliged to maintain secrecy and confidentiality.
k. The protection of personal data shall be taken into account, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons associated with the processing, already during the development or selection of hardware, software and procedures, in accordance with the principle of data protection by design and by default settings.

l. Software and hardware used is always kept up to date and software updates are carried out without delay within a reasonable period of time in view of the degree of risk and any need for testing. No software and hardware is used that is no longer updated by the providers with regard to data protection and data security concerns (e.g. expired operating systems).

m. Standard software and corresponding updates are only obtained from trustworthy sources.

n. Documents in paper format shall only be retained if there is no digital copy adequate with regard to the commissioned processing, its purpose and the interests of the persons affected by the contents of the documents, or if retention has been agreed with the Controller or is required by law.

o. A deletion and disposal concept is in place that complies with the data protection requirements of commissioned processing and the state of the art. The physical destruction of documents and data carriers is carried out in compliance with data protection requirements and in accordance with legal requirements, industry standards and state-of-the-art industrial standards (e.g. in accordance with DIN 66399). Employees were informed about legal requirements, deletion deadlines and, if responsible, about specifications for data destruction or device destruction by service providers.

p. The processing of the Controller's data that has not been deleted in accordance with the agreements of this order processing contract (e.g. as a result of statutory archiving obligations) shall be restricted to the necessary extent by blocking notices and/or segregation.

Data protection at employee level

Measures have been taken to ensure that the employees involved in the processing of personal data have the necessary expertise and reliability required by data protection law.

a. Employees are bound to confidentiality.
b. Employees are sensitised and instructed with regard to data protection in accordance with the requirements of their function. Training and awareness-raising shall be repeated at appropriate intervals or when circumstances require.
c. Relevant policies, e.g. on email/internet use, are kept up to date and are easy to find (e.g. on the intranet).
d. If employees work outside the company's internal premises (home and mobile office), employees are informed about the special security requirements and protection obligations in these constellations and are obliged to comply with them, subject to control and access rights.
e. Keys, access cards or codes issued to employees, as well as authorisations granted with regard to the processing of personal data, shall be withdrawn or revoked after their departure from the services of the Processor or change of responsibilities.
f. Employees are required to leave their working environment tidy and thus in particular prevent access to documents or data carriers containing personal data (Clean Desk Policy).

Access control

Physical access control measures are in place to prevent unauthorised persons from physically approaching the systems, data processing equipment or procedures by which personal data are processed.

a. With the exception of the workstation computers and mobile devices, no data processing systems are maintained on the Controller's own business premises. The Controller's data is stored with external server providers in compliance with the specifications for order processing.
b. The visitors are logged.
c. Visitors are not allowed to move freely, but only when accompanied by staff.

d. Access is secured by a manual locking system with security locks.
e. The issue and return of keys and/or access cards is logged.
f. Employees are required to lock devices or secure them specially when they leave their work environment or the devices.
g. Records (files, documents, etc.) are stored securely, e.g. in filing cabinets or other appropriately secured containers and adequately protected from access by unauthorised persons.
h. Data carriers are stored securely and appropriately protected from access by unauthorised persons.

Access control

Electronic access control measures are in place to ensure that access (i.e. already the possibility of use, use or observation) by unauthorised persons to systems, data processing equipment or procedures is prevented.

a. A password concept, specifies that passwords must have a minimum length and complexity corresponding to the state of the art and the requirements for security.
b. All data processing systems are password protected.
c. Passwords are generally not stored in plain text and are only transmitted hashed or encrypted.
d. Access data shall be deleted or deactivated when their users have left the Processor's company or organisation.
e. Anti-virus software that is kept up to date is used.
f. Use of software firewall(s).
g. Backups are stored in encrypted form.

Internal access control and input control (permissions for user rights to access and change data)

Access control measures have been taken to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing. Furthermore, input control measures have been taken to ensure that it is possible to subsequently verify and establish whether and by whom personal data have been entered into data processing systems, altered, removed or otherwise processed.

a. A rights and roles concept (authorisation concept) ensures that access to personal data is only possible for a group of persons selected according to necessity and only to the extent required.
b. The rights and roles concept (authorisation concept) is evaluated regularly, within an appropriate time frequency as well as when an occasion requires it (e.g. violations of the access restrictions), and updated if necessary.
c. The entry, modification and deletion of individual data of the Controller is logged.
d. The activities of the administrators are appropriately monitored and logged within the scope of legally permissible possibilities and within the scope of technically justifiable expenditure.
e. It is ensured that it is comprehensible which employees or authorized representatives had access to which data and when (e.g. by logging the software use or drawing conclusions from the access times and the authorization concept).

Transfer control

Transfer control measures are in place to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or while being transported or stored on data carriers, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

a. When accessing in-house systems from outside (e.g. for remote maintenance), encrypted transmission technologies are used (e.g. VPN).
b. Emails are encrypted during transmission, which means that on the way from the sender to the recipient, the emails are protected from being read by anyone who has access to the networks through which the email is sent.
c. The transmission and processing of the Controller's personal data via online offers (websites, apps, etc.) is protected by means of TLS/SSL or equivalent secure encryption.

Order control, purpose limitation and segregation control

Job control measures have been taken to ensure that personal data processed on behalf of the Controller are only processed in accordance with the Controller's instructions. The measures ensure that personal data of the Controller collected for different purposes are processed separately and that no mixing, blending or other joint processing of these data contrary to the mandate takes place.

a. The processing operations carried out for the Controller shall be documented separately, to an appropriate extent, in a register of processing activities.
b. Careful selection of sub-Processors and other service providers.
c. Employees and agents shall be informed in a comprehensible and clear manner about the Controller's instructions and the permissible processing framework and instructed accordingly. Separate information and instruction are not necessary if compliance with the permissible framework can be reliably expected anyway, e.g. due to other agreements or company practice.
d. Compliance with the Controller's instructions and the permissible framework for the processing of personal data by employees and agents shall be reviewed at appropriate intervals.

e. The deletion periods applicable to the processing of the Controller's personal data shall be documented within the deletion concept of the Processor, separately if necessary.
f. The Controller's personal data shall be processed in a logically separate manner from data of other processing operations of the Processor and shall be protected from unauthorised access or combination or intersection with other data (e.g. in different databases or by appropriate attributes).

Ensuring the integrity and availability of data and the resilience of processing systems

Measures have been taken to ensure that personal data is protected against accidental destruction or loss and can be recovered quickly in an emergency.

a. Fail-safe server systems and services are used, which are designed to be double or multiple.
b. Personal data is stored with external hosting providers. The hosting providers are carefully selected and comply with the state of the art in terms of protection against damage caused by fire, moisture, power failures, disasters, unauthorised access, data backup and patch management, as well as building security.
c. Personal data is processed on data processing systems that are subject to regular and documented patch management, i.e. in particular regularly updated.
d. The server systems used for processing have an uninterruptible power supply (UPS) that is adequately secured against failures and ensures a controlled shutdown in emergencies without loss of data.
e. The server systems used for processing have adequate fire protection (fire and smoke detection systems as well as appropriate fire extinguishing devices or fire extinguishing equipment).
f. Server systems are used that have protection against moisture damage (e.g. moisture detector).

g. The Controller's data records are protected by the system against accidental modification or deletion (e.g. through access restrictions, security queries and backups).
h. Server systems and services are used that have an appropriate, reliable and controlled backup & recovery concept.

Annex 3: Sub-Processors

The Processor shall use the following sub-Processors in the course of processing data for the Controller:

System	Service provider	Processed data categories	Third country
The following service providers are used for hosting the Ninox platform:			
Public Cloud:			
Hetzner	Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Customer data depending on the application created on the Ninox platform	No third country
Private Cloud (here is a choice of service provider):			
Amazon Web Services EMEA SARL (AWS)	Amazon Web Services EMEA SARL, 5 Rue Plaetis, L-2338 Luxembourg, Luxemburg	Customer data depending on the application created on the Ninox platform	No third country
Hetzner	Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Customer data depending on the application created on the Ninox platform	No third country
Backup (Private and Public Cloud):			
Amazon Web Services EMEA SARL (AWS)	Amazon Web Services EMEA SARL, 5 Rue Plaetis, L-2338 Luxembourg, Luxemburg	Customer data depending on the application created on the Ninox platform, encrypted	No third country
Support services:			
SendGrid: E-Mail-Marketing platform	SendGrid, Inc. 1801 California Street, Suite 500 Denver, Colorado 80202, USA	Email address, name, email communication (when using the	USA

		email function in the Ninox platform).	
Carbone: document creation	CarboneIO SAS 130 La Sauvagère, 85170 Bellevigny, Frankreich	Contents of documents (when using dynamic printing in the Ninox platform)	No third country