Data Processing Agreement for Personal Data within the Meaning of Art. 28 GDPR

1 Introduction, scope, definitions

This agreement governs the rights and obligations of nooa and the customer (hereinafter referred to as the "parties") in the context of processing personal data on behalf of the customer.
This contract applies to all activities in which employees of nooa or subcontractors commissioned by nooa process personal data of the customer on behalf of the customer.
Terms used in this contract shall be understood according to their definition in the EU General Data Protection Regulation. In this sense, the customer as principal is the "controller", nooa as contractor is the "processor". Insofar as declarations are to be made "in writing" in the following, the written form according to Art. 126 BGB is meant. Otherwise, declarations may also be made in another form, provided that adequate verifiability is ensured.

The processing is based on the existing contract between the parties "**Subscription contract**" (hereinafter "Main contract").

The language available for the conclusion of this agreement is exclusively German. Translations of this Data Processing Agreement into other languages are for your information only. In the event of any differences between the language versions, the German text shall take precedence.

2 Scope and period of processing

The scope and period of processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects and the obligations and rights of the controller are set out in Annex 1 to this contract and in the service specification of the main contract.

3 Duties of nooa

(1) nooa processes personal data exclusively as contractually agreed or as instructed by the customer, unless nooa is legally obliged to a certain processing. If such obligations exist, nooa will inform the customer prior to the processing, unless the communication is prohibited by law. nooa will furthermore not use the data provided for processing for any other purposes, in particular not for its own purposes.
(2) nooa confirms that it is aware of the relevant general data protection regulations and observes the principles of proper data processing.
(3) nooa commits itself to strictly maintain confidentiality during processing.
(4) Persons who may obtain knowledge of the data processed on behalf of the customer shall undertake in writing to maintain confidentiality, insofar as they are not already subject to a relevant confidentiality obligation by law.
(5) nooa assures that the persons employed by them for processing have been familiarised with the relevant provisions of data protection and this contract prior to the start of processing. Corresponding training and awareness-raising measures shall be repeated on an appropriate regular basis. nooa shall ensure that persons employed for commissioned processing are appropriately instructed and monitored with regard to compliance with data protection requirements on an ongoing basis.
(6) In connection with the commissioned processing, nooa shall support the customer as far as necessary in the fulfilment of his obligations under data protection law, in particular in the creation and updating of the list of processing activities, in the performance of the data protection impact assessment and any necessary consultation with the supervisory authority. The required information and documentation shall be kept available and provided to the customer upon request without delay.
(7) If the customer is subject to inspection by supervisory authorities or other bodies or if data subjects assert rights against the customer, nooa undertakes to support the customer to the extent necessary insofar as the processing on behalf is concerned.
(8) Information to third parties or the person concerned may only be provided by nooa with the prior consent of the customer. Requests addressed directly to him will be forwarded to the customer without delay.
(9) To the extent required by law, nooa shall appoint a competent and reliable person as Data Protection Officer. It has to be ensured that there are no

conflicts of interest for the Data Protection Officer. In case of doubt, the customer may contact the Data Protection Officer directly. nooa will inform the customer immediately about the contact details of the Data Protection Officer or give reasons why no officer has been appointed. Changes in the person or the internal tasks of the Data Protection Officer will be communicated to the customer by nooa without delay.

(10) The order processing takes place exclusively within the EU or the EEA.

4 Processing safety

(1) The data security measures described in Appendix 2 are defined as binding. They define the minimum owed by nooa. The description of the measures must be made in such detail that a knowledgeable third party can at any time undoubtedly recognise what the minimum owed should be, solely on the basis of the description. A reference to information which cannot be taken directly from this agreement or its annexes is not permissible.

(2) The data security measures can be adapted according to the technical and organisational development as long as the level agreed upon here is not undercut. Changes required to maintain information security shall be implemented by nooa without delay. The customer has to be informed about changes without delay. Significant changes are to be agreed between the parties.

(3) Insofar as the security measures taken do not or no longer meet the requirements of the customer, nooa shall notify the customer immediately.

(4) nooa assures that the data processed on the basis of this agreement are strictly separated from other data.

(5) Copies or duplicates shall not be made without the knowledge of the customer. Technically necessary, temporary duplications are excepted, insofar as an impairment of the level of data protection agreed here is excluded.

(6) nooa shall provide regular evidence of the fulfilment of its obligations, in particular the complete implementation of the agreed technical and organisational measures as well as their effectiveness. The proof shall be provided to the customer unsolicited at the latest every 12 months and otherwise at any time upon request. The proof can be provided by approved rules of conduct or an approved certification procedure. Evidence shall be kept for at least three calendar years after the end of the commissioned processing and shall be provided to the customer at any time upon request.

5 Rules on the correction, deletion and blocking of data

(1) Data processed within the scope of the order will only be corrected, deleted or blocked by nooa according to the contractual agreement reached or according to the customer’s instructions.

(2) The corresponding instructions of the customer will be followed by nooa at any time and also beyond the termination of this contract.

6 Subcontracting relations

(1) The contractually agreed services or the partial services described below shall be performed with the involvement of the subcontractors named in Appendix 3. nooa is authorised to establish further subcontracting relationships with subcontractors ("subcontractor relationship") within the scope of its contractual obligations. nooa shall inform the customer of this without delay. nooa is obliged to carefully select subcontractors according to their suitability and reliability. When involving subcontractors, nooa has to oblige them according to the regulations of this agreement and ensure that the customer can also directly exercise his rights from this agreement (especially his inspection and control rights) against the subcontractors. If subcontractors in a third country are to be involved, nooa has to ensure that an adequate level of data protection is guaranteed by the respective subcontractor (e.g. by concluding an agreement based on the EU standard data protection clauses). nooa will prove the conclusion of the aforementioned agreements with its subcontractors to the client upon request.

(2) A subcontractor relationship within the meaning of these provisions does not exist if nooa commissions third parties with services which are to be considered as purely ancillary services. This includes e.g. postal, transport and shipping services, cleaning services, telecommunication services without concrete reference to services provided by nooa for the client and security services. Maintenance and testing services constitute subcontractor relationships subject to approval insofar as they are provided for IT systems

that are also used in connection with the provision of services for the customer.

7 Rights and obligations of the customer

(1) The customer alone is responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.
(2) nooa may only collect, process or use data within the framework of the main contract and in accordance with the customer's instructions; this applies in particular with regard to the transfer of personal data to a third country or to an international organisation.
(3) If nooa is obliged to carry out further processing by law of the European Union or the Member States to which it is subject, it shall inform the customer of these legal requirements prior to the processing.
(4) The customer shall issue all orders, partial orders or instructions in documented form. In urgent cases, instructions may be given verbally. The customer shall immediately confirm such instructions in a documented manner.
(5) The customer shall inform nooa immediately if he detects errors or irregularities in the examination of the order results.
(6) The customer is entitled to control the compliance with data protection regulations and contractual agreements at nooa to a reasonable extent himself or by third parties, in particular by obtaining information and inspecting the stored data and the data processing programs as well as other on-site controls. The persons entrusted with the controls have to be granted access and insight by nooa as far as necessary. nooa is obliged to provide the necessary information, to demonstrate processes and to provide evidence necessary for the control. nooa is entitled to refuse controls by third parties as far as they are in a competitive relationship with nooa or if there are similar weighty reasons.
(7) Inspections at nooa shall be carried out without avoidable disruption of its business operations. Unless otherwise indicated for urgent reasons to be documented by the customer, inspections shall take place after reasonable advance notice and during nooa's business hours, and not more frequently than every 12 months. As far as nooa provides evidence of the correct implementation of the agreed data protection obligations as provided for in chapter 4 (6) of this contract, any control shall be limited to spot checks.

8 Reporting obligations

(1) nooa shall notify the client immediately of any violations of the protection of personal data processed on behalf of the customer. Reasonable suspicion of such breaches shall also be notified. The notification has to be sent to an address named by the customer within 24 hours after nooa became aware of the relevant event. It must contain at least the following information:
    a. a description of the nature of the personal data breach, including, where possible, the categories and approximate number of individuals concerned, the categories concerned and the approximate number of personal data records concerned;
    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;
    d. a description of the measures taken or proposed to be taken by nooa to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.
(2) Significant disruptions in the execution of the order as well as violations of data protection regulations or the stipulations of this agreement by nooa or its employees must also be reported immediately.
(3) nooa shall inform the customer without delay of inspections or measures by supervisory authorities or other third parties, insofar as these relate to the commissioned processing.
(4) nooa assures to support the customer in his obligations according to Art. 33 and 34 of the General Data Protection Regulation to the necessary extent.

9 Directives

(1) The customer reserves a comprehensive right to issue instructions with regard to processing on their behalf. The customer may appoint persons authorised to issue instructions. Insofar as persons authorised to give instructions are to be named, they shall be named in the appendix. In the event that the

customer's authorised persons change, the customer shall inform nooa in writing.

(2) nooa may name the person(s) to the customer who are authorised to receive instructions from the customer. If persons authorised to receive instructions are to be named, they will be named in the annex. In case the persons authorised to receive instructions change, nooa will inform the customer in text form.

(3) In the event of a change or long-term prevention of the appointed persons, the other party shall be informed immediately of their successors or representatives.

(4) nooa will immediately inform the customer if, in their opinion, an instruction given by the customer violates legal regulations. nooa is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the person in charge at the customer.

(5) nooa shall document instructions given to them and their implementation.

10 Termination of contract

(1) If, at the end of the contractual relationship, data processed in the order or copies thereof are still in the power of disposal of nooa, nooa shall, at the customer's option, either destroy the data or hand it over to the customer. The customer has to make this choice within 2 weeks after request by nooa. The destruction has to be carried out in such a way that a recovery of even residual information is no longer possible with reasonable effort. Physical destruction shall be carried out in accordance with DIN 66399, with a minimum of protection class 3.

(2) nooa is obliged to cause the immediate destruction or return, also from subcontractors.

(3) nooa shall provide proof of proper destruction and submit it to the customer without delay.

(4) Documentation serving as proof of proper data processing shall be kept by nooa at least until the end of the third calendar year after the end of the contract. He may hand them over to the client for his discharge.

11 Compensation

The compensation of nooa is conclusively regulated in the main contract. There is no separate compensation or reimbursement of costs within the scope of this contract.

12 Liability

(1) For compensation of damages suffered by a data subject due to inadmissible or incorrect data processing or use within the scope of commissioned processing in accordance with the data protection laws, the customer alone is responsible to the data subject in the internal relationship with nooa.

(2) The parties shall each release themselves from liability if a party proves that it is not responsible in any respect for the circumstance by which the damage occurred to an affected party.

13 Obligation to maintain professional secrecy (Art. 203 StGB)

(1) Within the scope of this order, data is also processed that is subject to professional secrecy (in the sense of 203 StGB (German Criminal Code)). nooa undertakes to maintain secrecy about professional secrets and to obtain knowledge of such data only to the extent necessary to fulfill the tasks assigned to them.

(2) The customer points out to nooa that persons who participate in a professional activity subject to professional secrecy and unauthorizedly disclose a third party secret which has become known to them during the exercise or on the occasion of their activity, are liable to prosecution according to Art. 203 para. 4 p. 1 StGB. In addition, a cooperating person is liable to prosecution under Art. 203 (4) sentence 2 of the Criminal Code if he or she uses the services of another cooperating person who in turn discloses without authorization a third party secret that has become known to him or her in the course of or on the occasion of his or her work and has not ensured that this person has been obligated to maintain secrecy.

(3) nooa ensures that all employees and other persons working for nooa (e.g. subcontractors) involved in the processing of data of the client subject to professional secrecy have committed themselves in text form not to disclose

without authorization the professional secrets that have become known to them during the exercise or on the occasion of their activities and that they have been instructed about the possible criminal liability according to Art. 203 para. 4 StGB. The customer points out to nooa that a collaborating person is liable to prosecution according to Art. 203 para. 4 p. 2 StGB, if he or she uses another collaborating person, who in turn discloses without authorization a third party secret, which has become known to him or her during the exercise or on the occasion of his or her activity, and the collaborating person has not ensured that the other collaborating person has been obliged to maintain secrecy. nooa will carefully select any subcontractors and obligate them to maintain secrecy, as far as they could gain knowledge of third party secrets in the sense of this agreement in the course of their work. nooa will also obligate any subcontractors to obligate all persons employed by them and any further subcontractors, who come into contact with secrecy data for the intended purpose or where this cannot be excluded, to maintain secrecy according to the principles mentioned above and to inform them about the consequences of a breach of duty.

(4) Furthermore, subcontractors shall be informed of the existing right to remain silent pursuant to Art. 53a of the Code of Criminal Procedure (StPO) as well as the protection against seizure pursuant to Art. 97 of the Code of Criminal Procedure (StPO); this also includes the reference to the right of the professional secrecy holder to decide on this right and the associated obligation to immediately contact the customer regarding the exercise of these rights. This obligation applies to all further subcontracts.

(5) nooa is advised that data which it processes on behalf of a professional secrecy holder may be subject to the right of so-called cooperating persons to refuse to testify (Art. 53a Code of Criminal Procedure (StPO)). However, in accordance with Art. 53a of the Code of Criminal Procedure, the professional secrecy holder decides on the exercise of the right to remain silent. In the event of questioning, nooa will object to this with reference to Art. 53a StPO and immediately inform the customer, who will then decide whether to exercise the right to remain silent.

(6) nooa is advised that the confidentiality data in its custody is subject to the prohibition of seizure pursuant to Art. 97 (2) of the Code of Criminal Procedure. The data may not be released without the consent of the customer (professional secrecy holder). In the event of seizure, nooa will object to this and inform the customer immediately.

14 Special termination right

(3) The customer may terminate the main contract and this agreement at any time without notice ("extraordinary termination"), if there is a serious breach of data protection regulations or the provisions of this agreement by nooa, nooa is unable or unwilling to carry out a lawful instruction of the customer or nooa refuses control rights of the customer in breach of contract.

(4) A serious breach shall be deemed to have occurred in particular if nooa fails to fulfill or has failed to fulfill to a significant extent the obligations specified in this agreement, in particular the agreed technical and organizational measures.

(5) In case of insignificant violations, the customer shall set a reasonable deadline for nooa to remedy the situation. If the remedy is not provided in time, the customer is entitled to extraordinary termination as described in this section.

(6) nooa has to reimburse the customer for all costs incurred by the customer due to the premature termination of the main contract or this contract as a result of an extraordinary termination by the customer.

15 Other

(1) Should the customer's property be endangered by measures of third parties (e.g. seizure), by insolvency proceedings or by other events, nooa has to inform the customer immediately.

(2) Ancillary agreements must be made in writing and must expressly refer to this agreement.

(3) The defense of the right of retention within the meaning of Art. 273 BGB (German Civil Code) is excluded with regard to the data processed in the order and the associated data carriers.

(4) Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement.

(5) nooa may amend this agreement from time to time by posting the amended version on its website. If, in nooa's sole discretion, the proposed changes are material, nooa shall cause notice to be given to the customer at least twenty (20) days prior to the effective date of the changes made. By continuing to access or use the service after the published effective date of the changes to

this agreement, the customer agrees to the amended version of the agreement.

Annex 1: Description of the data processing

1. Customer data

1.1. Type and scope of the data collected

(A) Inventory data

- General account information: Name, type and address of organisation; Creation date and status of account; Name and email of account owner; Related association (optional)
- Billing information: Name and email address of the billing contact; Subscriptions; Payment method; Billing address; VAT ID (optional)

(B) Usage data

- Number, type, status of users and access codes; Number, type of connected organizations and users; Number, type, status of pinboards; Number of posts, comments and likes; Number, type, status of tasks; Number, type of messages and conversations; Number, type, status of invitations; Timestamps of user activity

1.2. Purpose and legal basis

nooa processes personal data to provide customers with access to the administration interface of the services and to process orders. The processing of this data is necessary for the fulfillment of the subscription contract according to Art. 6 para. 1 lit.b DSGVO. Personal data are processed, based on Art. 5 para. 1 DSGVO, exclusively on the basis of their self-declaration and to the extent necessary for the use of the service.

1.3. Deletion period

The data will be archived after cancellation of the customer account after the legally required data storage for business processing:

- Contract data 6 years after the end of the contract
- Invoices 10 years

2. User data

2.1. Type and scope of the data collected

(A) Inventory data
- Auto-generated, non-personal data: nooa ID; User account creation date
- Personal data, entered by organization or User: Name; Nickname; Function; Organisation; Role; Password; Status; Email address (optional, obligatory when Admin); Avatar (optional); Birth date (optional); Short biography (optional); Name and date of connection with external contacts; Personal settings for usage of app (e.g. language, sounds)

(B) Usage data
- Auto-generated non-personal data: Account access code for self-activation (if applicable); Account access code expiry date; ""Asset hash" – a unique, random string to generate cloud URLs for media
- Devices and log data: Incoming network request parameters; App version; Device and OS version; Browser type and version; Log information

(C) Content data
- Pinboards: Name; Shared/internal; Members; Header image (optional); Description (optional)
- Direct messages, Posts, Comments, Likes, Tasks, if applicable: Type; Sender ID; Recipient ID; Date of creation; Date of editing; Title; Content incl. text or media; Status flags

All content data can only be viewed by logged in and authorized users.

2.2. Purpose and legal basis

nooa processes personal data to provide the services according to instructions of the main contract.

2.3. Deletion period

All data of users are archived after cancellation of the customer or user account and deleted after 3 months.

Annex 2: Technical and organizational measures

The following specifies the order-related technical and organizational measures to ensure data protection and data security that nooa must at least establish and maintain on an ongoing basis.

The aim is to guarantee in particular the confidentiality, integrity and availability of the information processed on behalf.

Overview of measures and legal basis	**Measures**
Pseudonymization (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)	Measures for pseudonymization are intended to exclude the identification of the data subject or to make it significantly more difficult: 1. The storage and consolidation of personal customer and user data takes place in such a way that an unauthorized third party cannot access this data.
Encryption (Art. 32 Abs. 1 lit. a DSGVO)	Encryption measures have the purpose of preventing the use and misuse of the data by unauthorized third parties: 1. Communication between servers and connected clients is encrypted using industry standard transport level encryption: HTTPS, SSL, TLS. 2. Stored customer data is encrypted with AES-256 or similar grade symmetric and/or asymmetric encryption algorithms. 3. User passwords are not saved. Instead, a secure procedure based on cryptographic hash functions is used ("Salted Cryptographic Hash"). 4. The nooa Web App is accessed over secure transport: HTTPS, SSL, TLS. 5. The mobile end devices communicate with the endpoint in encrypted form.

Confidentiality (Art. 32 Abs. 1 lit. b DSGVO)	Authorization control: 1. The IT infrastructure used is provided by Amazon Web Services (AWS) at the Frankfurt location. 2. Access control to the highly secure AWS data centers is carried out through the use of electronic monitoring measures, multi-level access control systems, staffing of the data centers around the clock with trained security personnel and granting of access strictly according to the principle of least rights and exclusively for the purpose of system administration.
	Access control: 3. The access authorizations for IT systems are assigned according to a defined and documented process according to the four-eyes principle and the principle of the least amount of rights (“need-to-know principle”), therefore employees only receive those accesses that are necessary for the fulfillment their duties, are necessary and regularly reviewed. 4. A password manager with a security model based on the zero knowledge principle and SSL / TSL encryption in combination with integrated dark web monitoring is used for access to IT systems. 5. Work devices are equipped with security software such as firewalls, antivirus software and malware detection. There are written regulations on handling mobile devices and data carriers, applying a screen lock and aligning the screens, securely deleting data, destroying data carriers and working remotely (home office). Unattended devices are automatically locked. 6. In the application, customer and user accounts are secured against unauthorized access when they are created using appropriate authentication and authorization mechanisms such as the use of reCAPTCHA and randomly generated activation and access codes in conjunction with two-factor authentication. 7. The login information for customer and user accounts is pseudonymized by using the nooa ID and protected by the implementation of secure, state-of-the-art password specifications (password length, complexity, period of validity, etc.). 8. The access authorizations for the application can be assigned by administrators of the customer according to the principle of the least amount of rights (“need-to-know principle”), hence users only receive those accesses that are necessary for the fulfillment of their tasks. 9. All accesses and attempts to access IT systems and the application are logged and documented.
	Access control: 1. The access rights for IT systems are defined and documented as part of a role / authorization concept, are assigned to the respective roles according to the task-related requirements and are regularly checked and withdrawn as soon as the business need for access no longer exists. Critical combinations of administrative rights are monitored (“separation of duty principle”). 2. The access rights for the application can be defined and documented by the customer's administrators as part of a role / authorization concept and assigned to the respective roles according to the task-related requirements. 3. Access to the application is limited in time. 4. All access to IT systems and the application is logged and documented.
	Separation control: 1. The application and IT systems are multi-tenant.

	2. Customer and user data are logically and technically separated from one another and encrypted on the basis of their own customer and user accounts. 3. Data that are collected for different purposes are processed separately. 4. Production, demo and test systems are marked as such and strictly separated from each other.
Integrity (Art. 32 Abs. 1 lit. b DSGVO)	Transfer control: 1. Data between nooa's servers and the Internet is always transmitted in encrypted form.
	Input control: 1. The creation, change and deletion of data as well as changes to the settings of the IT systems and the application are logged as far as possible. 2. The role / authorization concept within the application allows the customer to define who is authorized to enter, change and delete personal data
Availability and resilience (Art. 32 Abs. 1 lit. b DSGVO)	Availability control: 1. The computer systems are located in air-conditioned rooms and are protected against overvoltage peaks, floods and electromagnetic fields with overvoltage protection. Fire protection measures, measures to ensure a trouble-free and continuous power supply as well as against vibrations and vandalism and theft are carried out. 2. AWS monitors and maintains the electrical and mechanical devices preventively to ensure the uninterrupted operation of the systems in the AWS data centers. Equipment maintenance is carried out by qualified personnel in accordance with a documented maintenance schedule. 3. AWS reviews infrastructure usage and requirements at least once a month using a capacity planning model. This model can also be used to forecast future
	demand. It also includes considerations for information processing, telecommunications, and the storage of audit logs. 4. Critical system components are backed up in several isolated locations (called Availability Zones). Each Availability Zone is designed to operate independently with high reliability. The Availability Zones are networked. This enables the use of applications for which an automatic, uninterrupted failover between the Availability Zones is set up. 5. The commissioning of the provided productive systems, their configuration and the importing of changes are carried out in a comprehensible and transparent manner.
	Resilience control (Ability of the systems to deal with risk-related changes and display a tolerance and ability to compensate for disruptions): 1. AWS monitors electrical and mechanical systems and equipment so that problems can be identified immediately. For this purpose, audit tools and information from the building management and electrical monitoring systems are continuously evaluated. Preventive maintenance is carried out to ensure continuous functionality of the systems. The operating staff offers a continuous staffing around the clock, seven days a week and 365 days a year in order to recognize incidents and to manage their effects and rectification. 2. The data centers are designed to anticipate and tolerate functional failures while maintaining service levels. In the event of a functional failure, the data traffic is diverted from the area affected by the failure to another. An N + 1 standard applies to important applications. If there is a functional failure in a data

	center, sufficient capacity is available so that the data traffic can be distributed to the remaining locations. 3. The AWS business continuity plan includes measures to prevent and reduce disruptions caused by environmental influences. It contains operational details of the actions to be taken before, during and after a relevant event. The business continuity plan is supported by tests that also include simulations of various scenarios. During and after these tests, AWS documents the performance of its employees and processes, corrective measures and the experience gained for continuous improvement. 4. AWS also takes into account pandemic response policies and procedures in its disaster recovery planning so that it can respond quickly to an infectious disease outbreak. Remedial measures include alternative staffing models that outsource critical processes to resources in other regions, as well as activating a crisis management plan designed to support critical operational operations. The pandemic plans contain information on international health authorities and regulations, including contact details for international authorities.
Recoverability (Art. 32 Abs. 1 lit. c DSGVO)	1. The architecture is protected against data loss per se by internal replication mechanisms within the AWS platform. 2. The use of Availability Zones and data replication allows extremely short recovery periods and recovery point targets. 3. The data stocks are regularly backed up in the form of backup copies within the AWS platform. The backup concept is documented and is regularly checked and updated. Backup media are protected against unauthorized access.

Procedures for periodic review, assessment and evaluation (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)	Data protection management: 1. The principle applies that data protection and security are the responsibility of the entire company. 2. All employees are instructed in the handling of confidential data and are obliged in writing to maintain confidentiality. There are written rules for viewing and disclosing sensitive data, for the transfer and disclosure of data and for regulations on data protection and security in accordance with the current state of the art. Disciplinary measures exist in the event of a breach of confidentiality obligations. 3. All employees are regularly made aware of the dangers and risks and are trained to ensure compliance with the provisions of the GDPR and compliance with instructions. Follow-up training takes place regularly. 4. A Data Protection Officer and Data Protection Coordinator are defined and instructed to accompany changes in the internal work processes from a data protection point of view, to point out data protection aspects and to coordinate them with the Data Protection Officer. Employees are instructed to report immediately recognized violations of data protection regulations, suspected violations and other incidents related to information security. 5. Product development and design are based on the principles of “Data Privacy by Design”, “Data Privacy by Default”, “Zero Knowledge”, data economy and the “OWASP”. 6. The procedures used are regularly subject to a documented data protection impact assessment,

	consisting of a protection requirement assessment, risk analysis and security concept. 7. There are regular data protection audits by internal and external Data Protection Officers. 8. Security checks (e.g. penetration tests) by external parties are actively supported.
	Incident-Response-Management: 1. Procedures for handling and reporting malfunctions including the detection and reaction to possible security incidents are defined.
	Privacy-friendly defaults: 1. The basic setting of the application is designed in such a way that the customer and user data are protected as well as possible. 2. Customers and users can make settings on the application that deviate from this recommended basic setting. This is always marked as a deviation and provided with warning notices.
	Order control: 1. The processing of personal data takes place exclusively in accordance with the instructions of the client. 2. Instructions from customers and activities carried out in the context of order processing are documented in relation to the customer.

Annex 3: Approved subcontractors

Nr.	Subcontractor	Categories of data processed	Purpose of subcontracted processing
1	**Amazon Web Services EMEA SARL (AWS Europe)** 38 avenue John F. Kennedy, L-1855 Luxembourg	Customer and user data	Storage and processing of order data
2	**HubSpot Inc.** 2nd Floor, 25 First Street, Cambridge MA 02141, USA	Customer data	Storage and processing of contract data
3	**Stripe Payments Europe, Ltd.** C/O A&L Goodbody, 25-28 North Wall Quay, Dublin 1, Ireland	Customer data	Billing and invoicing
4	**Twilio Ireland Limited** 25-28 North Wall Quay Dublin 1, Ireland	Customer and user data	Provision of infrastructure for voice calling, video calling and messaging
5	**OpenAI, L.L.C.** 3180 18th St, San Francisco, CA 94110	User data	Storage and processing of content data

Annex 4: Data Protection Officer, address for reporting data protection breaches

The contact details of the internal Data Protection Officer and for reporting personal data breaches:

Data Protection Officer
nooa GmbH
Rheinkaistraße 1
68159 Mannheim
privacy@nooa.app