**Commissioned Data Processing Agreement**

between

COMPANY

ADDRESS AND STREET

ZIP CITY

as the controller (hereinafter referred to as 'Customer')

and

Next Matter GmbH

Gormannstr. 14

10119 Berlin

as the processor (hereinafter referred to as 'Next Matter')

# Recitals

Whereas, the Customer wishes to engage Next Matter to provide the services specified in Section 4. Part of the performance of the Agreement is the processing of personal data. In particular, Art. 28 GDPR sets forth specific requirements for such commissioned data processing. To comply with these requirements, the parties conclude the following Agreement the performance of which shall not be paid for separately, except if expressly agreed.

# Definitions

2.1 Controller as defined in Art. 4 (7) GDPR is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

2.2 Processor as defined in Art. 4 (8) GDPR means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

2.3 Personal data as defined in Art. 4 (1) GDPR means any information relating to an identified or identifiable natural person (hereafter: '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.

2.4 Personal data requiring special protection means personal data pursuant to Art. 9 GDPR that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of data subjects, personal data pursuant to Art. 10 GDPR relating to criminal convictions and offences or related security measures and genetic data pursuant to Art. 4 (13) GDPR, biometric data pursuant to Art. 4 (14) GDPR, data concerning health pursuant to Art. 4 (15) GDPR and data concerning a natural person’s sex life or sexual orientation.

2.5 Processing as defined in Art. 4 (2) GDPR means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.6 Supervisory authority as defined in Art. 4 (21) GDPR means an independent public authority which is established by a Member State pursuant to Art. 51 GDPR.

# Indication of the competent data protection supervisory authority

3.1 The supervisory authority competent for the Customer is the Berlin Data Protection Commissioner.

3.2 The supervisory authority competent for Next Matter is the Berlin Data Protection Commissioner.

3.3 The Customer and Next Matter and their representatives, if any, shall on request cooperate with the supervisory authority to fulfil its tasks.

# Subject-matter of the Agreement

4.1 Next Matter shall provide Software Services to the Customer on the basis of the Agreement dated March 26th, 2021 ('Main Agreement'). Doing this, Next Matter will have access to personal data and process these exclusively on behalf and in accordance with the instructions of the Customer. Scope and purpose of the data processing by Next Matter result from the Main Agreement (and the performance description belonging to it). It shall be the Customer's obligation to assess the admissibility of the data processing.

4.2 The parties conclude this present Agreement to specify in detail their mutual rights and obligations under data protection laws. In any case of doubt, the provisions of the present Agreement shall take priority over the provisions of the Main Agreement.

4.3 The provisions of this Agreement shall apply to all activities relating to the Main Agreement and in the performance of which Next Matter and its employees or any agent engaged by Next Matter come into contact with personal data stemming from the Customer or having been recorded on behalf of the Customer.

4.4 The term of this Agreement shall be based on the term of the Main Agreement, unless
further additional rights of termination or obligations result from the provisions set forth below.

# Right to issue instructions

5.1 Next Matter may collect, process or use data only within the scope of the Main Agreement and in accordance with the Customer's instructions. This shall apply in particular with respect to the transfer of personal data to a third country or an international organisation. Should Next Matter be obliged under European Union law or the law of a Member State to carry out further processing, it shall inform the Customer of these legal requirements prior to processing.

5.2 The Customer's instructions shall initially be defined by this Agreement and may thereafter be altered, supplemented or replaced by the Customer by individual instructions (individual instruction). The Customer may issue appropriate instructions at any time. This shall include instructions regarding the correction, erasure and blocking of data. The persons authorised to issue instructions are specified in Annex 5. Should any of the persons named be exchanged or be unable to carry out its duties for a longer time, the successor or stand-in shall be named to the contracting party in text form without delay.

5.3 All instructions issued shall be documented by both the Customer and Next Matter. Any instruction exceeding the services agreed in the Main Agreement shall be treated as a request to alter the extent of the services.

5.4 Should Next Matter believe that any instruction issued by the Customer breaches a data protection regulation, it shall inform the Customer of this without delay. Next Matter shall be entitled to suspend the implementation of any such instruction until the Customer confirms or changes it. Next Matter may refuse the implementation of any instruction which is obviously unlawful.

5.5 Should any instruction issued by the Customer cause additional expenditure or costs to Next Matter, Next Matter may claim an adjustment of the remuneration decided by the Customer and Next Matter together or reimbursement of the costs by the Customer.

# Nature of the data processed, group of data subjects

6.1 In connection with the performance of the Main Agreement, Next Matter will have access to the personal data specified in detail in Annex 1. These data include the special categories of personal data specified and identified as such in Annex 1.

6.2 The group of data subjects affected by the data processing is identified in Annex 2.

# Protection measures taken by Next Matter

7.1 Next Matter shall be obliged to observe the statutory regulations regarding data protection and to not disclose to a third party, or enable access by a third party to, the information obtained from the Customer's sphere. Documents and data shall be protected against disclosure to unauthorised persons, taking account of the state of the art.

7.2 Within its sphere of responsibility, Next Matter shall design its internal organisation in such a way that it satisfies the special requirements of data protection. Next Matter shall implement all technical and organisational measures necessary to appropriately protect the Customer' data as set forth in Art. 32 GDPR, in particular at least the following measures specified in Annex 3:

1. Confidentiality
2. Integrity
3. Availability
4. Other

Next Matter may alter the protection measures taken, ensuring, however, the contractually agreed level of security.

7.3 At Next Matter, the managing director Johannes Hugenroth is appointed as contact for data protection.

7.4 The persons employed for the purpose of data processing by Next Matter are prohibited from collecting, processing and/or using personal data without authorisation. Next Matter shall appropriately oblige (obligation of confidentiality, Art. 28 (3) (b) GDPR) all persons it entrusts with the processing and the performance of this Agreement (hereinafter referred to as 'Employees') and use due diligence to ensure observance of this obligation. These obligations shall be stipulated in such a way that they will continue in force also after termination of this Agreement or the employment relationship between the Employee and Next Matter. These obligations shall be proven to the Customer in a suitable way on request.

# Next Matter's obligations to provide information

8.1 In the event of a malfunction, suspicion of a breach of data protection or of a breach of contractual obligations of Next Matter, suspicion of incidents relevant to security or other irregularities during the processing of the personal data by Next Matter or any person employed by Next Matter in the context of the order or at a third party, Next Matter shall inform the Customer without delay in writing or text form. The same applies to audits of Next Matter by the data protection supervisory authority. A report of a breach of the protection of personal data shall include at least the following information:

a) A description of the nature of the breach of the protection of personal data, if possible stating the categories and number of data subjects, the categories affected and the number of data records affected

b) A description of the measures taken or proposed by Next Matter to remedy the breach and, possibly, measures for mitigating their possible detrimental effects

8.2 Next Matter shall without delay take the necessary measures to protect the data and to mitigate possible detrimental consequences for the data subjects, inform the Customer of this and ask for further instructions.

8.3 Moreover, Next Matter shall be obliged to provide information to the Customer at any time if its data are affected by a breach according to Section 1.

8.4 Should the Customer's data be jeopardised at Next Matter due to attachment or seizure, insolvency or composition proceedings or other events or measures by a third-party, Next Matter shall inform the Customer without delay, unless Next Matter is prohibited from doing this by any court or official order. In this connection, Next Matter shall without delay inform all competent bodies that only the Customer, as the controller pursuant to the GDPR, has the power of decision with respect to the data.

8.5 Next Matter shall without delay notify the Customer of any substantial change of the protection measures pursuant to Section 7.2.

8.6 The Customer shall be informed without delay of any change of the data protection officer.

8.7 Next Matter and, where applicable, its representative shall maintain a record of all categories of processing activities carried out on behalf of the Customer which shall contain all details specified in Art. 30 (2) GDPR. The record shall be provided to the Customer on request.

8.8 Next Matter shall reasonably support the Customer with the creation of the record of processing activities. Next Matter shall provide the Customer with the information required in each case in a suitable way.

# Customer's rights of control

9.1 The Customer shall convince itself of the technical and organisational measures taken by Next Matter prior to the start of the data processing and thereafter at regular intervals. To do this, the Customer may obtain information from Next Matter, request the submission of existing attestations issued by experts, certificates or internal audits or examine itself in person or have examined by an expert third party, that must not be a competitor of Next Matter, the technical and organisational measures taken by Next Matter after timely coordination at the normal business hours. The Customer shall carry out controls only to the extent necessary and during them not unreasonably disturb Next Matter's operational procedures.

9.2 Next Matter undertakes to provide to the Customer, at its verbal or written request and within reasonable time, all information and evidence that is necessary to carry out a control of the technical and organisational measures taken by Next Matter.

9.3 The Customer shall document the result of the control and communicate it to Next Matter. If any fault or irregularity is detected, in particular during the examination of order results, the Customer shall inform Next Matter without delay. If any fact is found during a control that requires a change of the procedure to avoid its reoccurrence in the future, the Customer shall without delay inform Next Matter of the necessary changes of procedure.

9.4 Next Matter shall on request provide to the Customer a comprehensive and up-to-date data protection and security concept for the commissioned data processing and regarding the persons that have access authorisation.

9.5 Next Matter shall on request prove to the Customer the obligation of the Employees pursuant to Section 7.4.

# Use of subcontractors

* 1. The contractually agreed services or the partial services described below shall be provided by using the subcontractors named in Annex 4. Within the scope of its contractual obligations, Next Matter shall be entitled to establish additional subcontractor relationships with subcontractors ('Subcontractor Relationship'), provided that Next Matter informs the Customer thereof at least 30 days in advance in written or text form . The Controller is entitled in individual cases to object to the commissioning of a further potential processor in written or text form. Next Matter shall be obliged to select subcontractors carefully based on their qualification and reliability. When involving subcontractors, Next Matter shall oblige them in accordance with the provisions of this Agreement and ensure that the Customer will be able to exercise its rights under this Agreement (in particular, its rights of inspection and control) also directly against the subcontractor. Where a subcontractor in a third country is to be involved, Next Matter shall ensure that an adequate level of protection of personal data will be guaranteed at the respective subcontractor (e.g., by concluding an agreement based on the EU Standard Data Protection Clauses). Next Matter shall on request prove to the Customer that it has concluded the abovementioned agreement with its subcontractors and disclose the technical and organizational measures taken by its subcontractors. Further outsourcing by the subcontractor requires the express consent of the main client/ customer (at least in text form).

10.2 For the purposes of this provision, a Subcontractor Relationship shall not exist where Next Matter engages a third party to provide services that are to be regarded as pure ancillary services. This shall include services such as mail, transport and shipping services, cleaning services, telecommunication services without specific connection with services that Next Matter provides to the Customer and guard services. Maintenance and inspection services shall be Subcontractor Relationships requiring approval if they are provided for IT systems that are used also in connection with the provision of services for the Customer.

# Requests and rights of data subjects

11.1 If feasible, Next Matter shall, by means of suitable technical and organisational measures, support the Customer to enable it to comply with its obligations pursuant to Art. 12-22, 32 and 36 GDPR.

11.2 If a data subject exercises a right, such as the right of access, correction, or erasure with respect to its data, directly against Next Matter, Next Matter shall not respond to this itself but refer the data subject to the Customer without delay and wait for the Customer's instructions.

# Liability

12.1 In the internal relationship with Next Matter, only the Customer shall be responsible towards the data subject with respect to compensation for damage suffered by the data subject because of any data processing or use in the context of commissioned data processing which is inadmissible or incorrect pursuant to data protection laws.

12.2 A party shall indemnify the other from liability if the other party demonstrates that it is in no way responsible for the circumstance that led to the damage suffered by the data subject.

# Right of termination without notice

The Customer may terminate the Main Agreement in whole or in part without notice if Next Matter fails to fulfil its obligations under this Agreement, wilfully or grossly negligently breaches a provision of the GDPR or cannot, or does not want to, carry out an instruction issued by the Customer. In the event of a simple, i.e., neither wilful nor grossly negligent, breach, the Customer shall set a reasonable time limit for Next Matter within which to remedy the breach.

# Termination of the Main Agreement

14.1 When the Main Agreement ends, or at any time at the Customer's request, Next Matter shall return to the Customer all documents, data and data carriers handed over to it or, if desired by the Customer, delete them, unless an obligation applies under Union law or the law of the Federal Republic of Germany to store the personal data. This shall also apply to any data backups existing at Next Matter. Next Matter shall furnish documented evidence of the proper deletion of any still existing data. Documents to be disposed of shall be destroyed using a document shredder according to DIN 32757-1. Data carriers to be disposed of shall be destroyed according to DIN 66399.

14.2 The Customer shall have the right check in a suitable manner the complete return or deletion in accordance with the Agreement of the data existing at Next Matter.

14.3 Next Matter shall be obliged to treat as confidential also after the end of the Main Agreement the data disclosed to it in connection with the Main Agreement. This present Agreement shall remain in force after the end of the Main Agreement while Next Matter still holds personal data that have been transferred to it by the Customer or that it has collected on behalf of the Customer.

# Final provisions

15.1 Furthermore, the parties are agreed that the defence of the right of retention by Next Matter pursuant to Section 273 of the German Civil Code (BGB) with respect to the data to be processed and the associated data carriers shall be excluded.

15.2 Any amendment or supplement to this Agreement shall only be valid if made in writing. This shall also apply to any waiver of this written form requirement. This shall not affect the precedence of individual contractual agreements.

15.3 Should any individual provision of this Agreement be or become legally invalid or unenforceable, in whole or in part, this shall not affect the validity of the remaining provisions.

15.4 This Agreement shall be governed by German law. References to foreign state law shall not apply. The exclusive place of jurisdiction shall be Berlin.

# Annexes

Annex 1 – Description of the data/categories of data requiring special protection

Annex 2 – Description of the data subjects/groups of data subjects

Annex 3 – Technical and organisational measures taken by Next Matter

Annex 4 – Approved subcontractors

Annex 5 – Persons authorised to issue instructions

Berlin, this \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_, this \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Next Matter Customer

Annex 1 – Description of the data/categories of data requiring special protection

* **[PLACEHOLDER TO FILL OUT BY CUSTOMER]**
* -

Annex 2 – Description of the data subjects/groups of data subjects

* **[PLACEHOLDER TO FILL OUT BY CUSTOMER]**

Annex 3 – Technical and organisational measures taken by Next Matter

1. **Confidentiality - (Art 32(1)(b) GDPR)**

Confidentiality meaning that personal data, data used, systems, and services must be protected from unauthorised and/or unlawful access or processing.

* 1. **Access Control - Physical**

The following measures shall ensure that unauthorised persons are denied access to sensitive locations where equipment is stored or used with which personal data is processed or used:

* + 1. As a remote first company, there is no sensitive data on Next Matter premises.
		2. Most data is stored on third party server locations which are sufficiently secured.
		3. Each employee has access to their own personal devices which they have to secure when not in use.
		4. Employees are to store their devices and sensitive materials in locked cabinets.
		5. Cabinets used for storing any kind of company data in the Next Matter office are locked.

* 1. **Access Control - System Authorization**

The following measures shall prevent data processing systems, equipment or procedures from being used by unauthorised persons:

* + 1. Access to stored data is limited to authorized users only.
		2. All successful and rejected access attempts are logged (user ID, Computer, IP address) and archived in audit-compliant form for 3 months.
		3. Inactive User IDs are to be deactivated after an extended period without login.
		4. Users are to be assigned unique accounts with no possibility for shared accounts.
		5. Random sampling and analysis of log files are to be executed to detect anomalies.

* 1. **Access Control - Data Authorization**

The following measures ensure that persons authorised to use a data processing system have access only to data subject to their right of access and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after storage.

* + 1. Users are granted access to specific, relevant data to each user and not the entirety.
		2. Files containing personal information will only be kept on servers for the time needed to successfully complete the associated task.
		3. Files are to be deleted in a secure and conscientious manner.
		4. A general clear desk and screen policy is implemented at Next Matter.
	1. **Separation Control**

The following measures to ensure that data collected for different purposes are processed separately and used for the correct purposes.

* + 1. Access to data records is only possible through applications that fulfil this separation requirement.
		2. Every record must be linked to specific purpose.
		3. Productive and test systems are operated separately.
		4. Databases are separated in a logical manner following a structured file storage
1. **Integrity (Art 32 (1)(b) GDPR)**

Integrity meaning the correctness (integrity) of data and the correct functioning of systems. The term integrity in in connection with data, expresses that the data is complete and unchanged.

* 1. **Transmission Control**

The following measures ensure that data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data carriers.

* + 1. Communication transpires through secure networks and encrypted systems in accordance to current security standards.
		2. Data carriers are disposed in a secure manner.
		3. All paper files containing customer data are not thrown out, but shredded.
		4. Time stamps of when personal data is retrieved, transmitted or handled are logged.
		5. Hardware or software not authorized by Next Matter Management is not to be used.
		6. Information is not to be shared on external IT services (data transfer to private email accounts, unauthorized cloud storages etc.).
		7. Data transfer generally is only to be executed on a strict must have basis.
	1. **Input Control**

The following measures ensure that it can be subsequently verified and established whether and by whom personal data has been entered, modified or removed in data processing systems:

* + 1. Every data entry, modification, or removal is logged and recorded.
		2. Passing on passwords or usernames is strictly prohibited.
		3. Strict protocol for the case a password becomes known.
1. **Availability & Resilience**

Availability meaning that data and the associated systems necessary for their processing are functioning when required

* 1. **Availability Control**

The following measures shall ensure that personal data is protected and available against accidental destruction or loss.

* + 1. Documented backups and recovery concepts are created in regular intervals.
		2. Security controls and virus protection as well as strong, maintained firewalls are implemented.
		3. Redundant storage systems are implemented.
		4. Surge protection and uninterruptible power supply at server location is guaranteed.
		5. Regular updates are ensured through previously defined workflows.
	1. **Resilience Control**

The following measures shall ensure that personal data is stored in a resilient manner.

* + 1. Security controls and virus protection as well as strong, maintained firewalls are implemented.
		2. Surge protection and uninterruptible power supply at server location is guaranteed.
		3. Servers are hosted in professional data centres in air-conditioned rooms equipped with fire and smoke detections systems.
		4. Data is stored in redundant systems, backed up daily and can be restored on a 14-day rolling basis.

1. **Other Kinds Of Measures Art 32(1)(d) GDPR; Art 25(1) GDPR)**
	1. **Governance**

The following measures ensure that the governance setup regarding personal data processing remain effective in the long term.

* + 1. Data protection and information security is overseen by the management team and executed by respective functional teams and team members.
		2. All employees have signed confidentiality agreements as part of their employment contract with a specific reference to the protection of customer data and data processed on behalf of customers.
		3. Employees receive regular trainings on handling confidential data with a dedicated focus on customer data and data processed on behalf of customers, beyond their professional training to date as information technology and business professionals.
		4. Next Matter is built with data protection by default. Customers independently define which data of their employees and customers they need to capture in operations processes automated through Next Matter to achieve the desired process outcomes.
		5. Requests from data subjects and any data protection inquiries by customers and employees are raised directly to management and are dealt with as a priority.
		6. While the company does not yet meet the regulatory requirements for the appointment of a data protection officer beyond the direct responsibility of management for data protection, a contract with a professional data protection officer was signed in March 2021. The data processing agreement will be updated accordingly once the data protection officer has been appointed in April 2021.
	1. **Job Control**

The following measures ensure that personal data processed on behalf of others are processed strictly in accordance with the principal’s instructions.

* + 1. Subcontractors all must be GDPR compliant.
		2. Contracts ensuring detailed instructions must be followed by subcontractors considering all data protection issues.
		3. Subcontractors’ employees only have access to information they absolutely must know.
		4. All subcontractor personnel must comply with all data protection principles specified by GDPR, particularly the confidentiality of data.

* 1. **Privacy Management**

The following measures shall ensure that the technical and organisational measures taken remain effective in the long term.

* + 1. Regular monitoring of the technical and organizational measures taken.
		2. Messages and reports on unusual occurrences should be evaluated.
		3. Training of employees in the handling of data privacy, confidentiality, IT, and IT security awareness.
	1. **Data Protection Management**

The following measures shall ensure that even in case of a breach, the absolute minimum of sensitive data is available.

* + 1. Erasure of data no longer needed.
		2. Secure disposal of defective hardware/hardware no longer needed.
		3. Secure disposal of documents/file shredder.
		4. Employees trained and obliged to maintain confidentiality and data secrecy.

Annex 4 – Approved subcontractors

The following companies are approved subcontractors under Section 10:

* Amazon Web Services, 38 Avenue John F. Kennedy, L-1855, Luxembourg
(data stored in Frankfurt, Germany, AWS region eu-central-1)
* Datadog, 620 8th Avenue, 45th floor, New York, NY 10018, USA
* Mixpanel, One Front Street, Floor 28, San Francisco, CA 94111, USA
* Sendgrid, 375 Beale Street, 3rd Floor, San Francisco, CA, USA
* Sentry, 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA

Annex 5 – Persons authorised to issue instructions

The Customer's persons authorised to issue instructions are

* NAME ( EMAIL)

Next Matter's persons receiving instructions are

* Johannes (Jan) Hugenroth (jan.hugenroth@nextmatter.com)
* Tassilo Karunarathna (tassilo.karunarathna@nextmatter.com)