Data Processing Addendum

Last modified: March 02, 2025

This Data Protection Addendum ("**DPA**" or "**Agreement**") regarding procession of data by a third-party processor on behalf of a controller in the sense of Art. 28 sec. 3 of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ("**GDPR**") with its appendices has been entered into between

the "**Processor**": hema.to GmbH, Metzstr. 14B, 81667 Munich, Germany and

the "**Controller**": Customer

For the purpose of the contractual relationship, Processor and Controller each referred as a "**Party**" and together as the "**Parties**".

This DPA is supplemental to, and forms an integral part of, the contractual relationship ("**Contract**") entered into by the same Parties and is effective after the Controller has signed the Contract. Terms not otherwise defined in this DPA will have the meaning as set forth in the Contract. Controllers that do not agree with the content of Processors' DPA may contact legal@hema.to, in which case the parties will conclude a tailored data processing agreement.

This DPA is made available at https://www.hema.to/legal/dpa. For Controllers that would like to receive a signed copy of the DPA, they may reach out to legal@hema.to. The DPA is updated from time to time. Controllers with an active hema.to subscription, will be contacted via email or via in-app notification in such case.

1. **Subject matter and term of the Agreement**
   (1) **Subject matter**
   This Data Protection Addendum applies to all activities in the course of which the Processor is provided access to Personal Data of the Controller or of another data subject.

(2) **Term**
The term of this Agreement corresponds with the Term of the Contract.

2. Data Protection Agreement Details

(1) **Nature and Purpose of the intended Processing of Data**
Nature and purpose of processing of Personal Data by the Processor on behalf of the Controller are precisely defined in the Contract.
The contractually agreed processing of Personal Data shall be carried out exclusively within a member state of the European Union ("**EU**") or within a member state of the European Economic Area ("**EEA**").

(2) **Type of Data**
Subject to the processing are Personal Data comprised in the following data types/categories (List/Description of the data categories):

- Personal Master Data (Key Personal Data)
- Contact Data (e.g. telephone number, electronic mail addresses)
- Key Contract Data (Contractual/Legal Relationships, interest in Contract or Product Interest)
- Contract Billing and Payment Data

(3) **Categories of Data Subjects**
The Categories of "**Data Subjects**" comprise:

- Subscribers
- Employees
- Contact Persons

3. Technical and Organisational Measures

(1) The Processor implements all appropriate technical and organizational measures to safeguard a level of security appropriate to the risk, in order to ensure that the processing complies with the requirements under GDPR and applicable legislation.

(2) The Processor shall take at least the security measures as per Appendix 2 (*Technical and Organizational Measures*) hereto.

(3) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Processor to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and deletion of data

(1) The Processor may not on its own authority rectify, delete Personal Data or restrict the processing of such data being processed on behalf of the Controller, but only on written instructions from the Controller.
Insofar as Data Subject contacts the Processor directly referring to the any of the aforementioned points, the Processor will forward the Data Subject's request to the Controller without undue delay.

(2) Insofar as not included in the scope of the Contract, the erasure policy, 'right to be forgotten', rectification, data portability and access according to documented instructions of the Controller are to be secured by the Processor for a fee.

(3) If the Processor or persons subject to it who have access to Personal Data processed on behalf of the Controller process them due to their own legal obligations outside the limits of the order and the instructions of the Controller, the Processor shall notify the Controller of these legal obligations prior to the processing, unless the law prohibits such communication because of an important public interest.

(4) Any transfer to a third country requires the prior consent of the Controller and may only take place if the special requirements of Art. 44 et seq. GDPR are met.

5. Information obligations by the contracting Parties

If one of the Parties of the Agreement is subject of

- a review by the supervisory authority,
- an administrative offense or criminal proceeding,
- the liability claim of an affected person or the assertion of their rights within the meaning of Artt. 12 to 23 GDPR,
- or a third party or any other claim related to the processing of the order,

they are asked to assist each other to the best of their abilities.

6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Controller's data, even in the case of outsourced ancillary services.

(2) The Processor may commission subcontractors (additional contract processors) only after prior explicit written or documented consent by the Controller. The Controller agrees to the commissioning of the subcontractors under the condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR (general approval) listed on Appendix 1 of this document, if applicable.

7. Supervisory powers of the Controller

(1) The Controller reserves the right, to review or to have reviewed by an auditor appointed on a case-by-case-basis in consultation with the Processor. He has the right to convince himself of the compliance with this Agreement by the Processor at Processor's premises by means of random checks, which are ordinarily to be announced in due time.

(2) The Processor shall ensure that the Controller is able to verify compliance with the obligations of the Processor according to Art. 28 GDPR. The Processor undertakes to give the Controller the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of such measures, which may not be limited to the scope of the concerned Contract, may be provided by current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor) and/or suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

8. Communication in the case of infringements by the Processor

(1) The Processor shall assist the Controller in complying with the obligations set in Artt. 32 to 36 GDPR concerning the security of Personal Data, reporting obligations for data breaches, data protection impact assessments and prior consultations. These include:

i. Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of rights as a result of security gaps and that enable an immediate detection of relevant infringements.
ii. The obligation to report a Personal Data breach immediately to the Controller.
iii. The obligation to assist the Controller with regard to the Controller's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.

iv. Supporting the Controller with regard to its data protection impact assessment.
v. Supporting the Controller with regard to prior consultation of the supervisory authority.

(2) The Processor may claim compensation for support services which are not included in the description of the services, and which are not attributable to failures on the part of the Processor.

9. Authority of the Controller to issue instructions

(1) The Controller immediately has to confirm oral instructions (at the minimum in text form).

(2) The Processor shall inform the Controller immediately if he considers that an instruction violates Data Protection Regulations. The Processor shall then be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

(3) For instructions that are not included in the description of the Contract, the Processor may claim a fee.

10. Deletion and return of Personal Data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Controller, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Controller, at the latest upon termination of the Contract, the Processor shall hand over to the Controller or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into their possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the order or Agreement shall be stored beyond the contract duration by the Processor in accordance with the respective retention periods. They may hand such documentation over to the Controller at the end of the contract duration to relieve the Processor of this contractual obligation.

Note regarding Technical and Organizational Measures
With regard to the following points, the current data protection and data security concept of hema.to GmbH applies:

1. Confidentiality (Art. 32 para. 1 b) GDPR)
2. Integrity (Art. 32 para. 1 b) GDPR)
3. Availability and Resilience (Art. 32 para. 1 b) GDPR)
4. Procedures for regular testing, assessment and evaluation (Art. 32 para. 1 d) GDPR; Art. 25 para. 1 GDPR)

Appendixes
Appendix 1: List of Subcontractors
Appendix 2: Technical and Organizational Measures

Appendix 1:
List of Subcontractors

Subcontractor (name, legal form, registered office of the company)	**Processing location (country)**	**Type/purpose of the service**
Google Cloud EMEA Limited 70 Sir John Rogerson's Quay, Dublin 2, Irland	Frankfurt, Germany	- Hosting of the hema.to product - Internal IT infrastructure service provider
Pipedrive Germany GmbH Julie-Wolfthorn-Straße 1 10115 Berlin, Germany	Dublin, Ireland Frankfurt, Germany Stockholm, Sweden	Management of customer relationships

Appendix 2:
Technical and Organizational Measures

Data Protection

hema.to implements the following Technical and Organizational Measures ("**TOMs**") for data security pursuant to Art. 32 GDPR.

Introduction and Framework

Taking into account the state of the art, the implementation costs, and the nature, scope, context and purposes of processing as well as the varying likelihood and severity of risk to the rights and freedoms of natural persons, hema.to has implemented appropriate TOMs to ensure a level of protection appropriate to the risk.
Within the framework of Art. 32 GDPR, hema.to is particularly committed to take the necessary technical and organizational steps to achieve the best possible solutions in line with the objectives of the GDPR and to ensure the security of the processing of personal data.

In particular, hema.to undertakes to handle customer data responsibly and thus, implements the necessary TOMs to achieve this.

The following sections first explain the criteria and measures specified in Art. 32 GDPR and then outline the individual TOMs implemented by hema.to to ensure data protection standards are met.

1. **Scope**
   The following descriptions refer to the processing of personal data within the company as a whole, unless the following and/or the list of processing activities contain restrictions to individual procedures.

2. **Responsibilities**
   In order to ensure and improve the level of security and to review the technical and organizational measures, hema.to conducts investigations to verify compliance

with data protection standards. Any incidents relevant to data protection are reviewed and resolved by the data protection officer. hema.to's contact person for data protection issues is **Patrick Wellbrock**, who can be reached at Patrick.Wellbrock@rhenus.com.

2.1. **Ensuring Confidentiality (acc. to Art. 32 (I) (b) GDPR): Physical Access Control**

Access to company premises is restricted by the following measures:

- Documented key issuance only to authorized persons; defined key management
  - Application of the principle of least privilege
  - Revocation, blocking, or withdrawal of access rights upon leaving the company or changing departments
- Subtenants in the office space have signed an NDA
- Access to property/office for subtenants via pin code and allowed during designated office hours only
- Designated desk area for subtenants
- Visitors allowed only when accompanied by employees and after prior registration
- Careful selection of cleaning staff
- Premises secured with appropriate security technology (manual lock system with double-cylinder security / doors with external knobs / chip-card system)
- Access to locked IT distribution panels and routers/firewalls only for authorized employees
- Doors locked when premises are unattended

2.2. **Ensuring Confidentiality (acc. to Art. 32 (I) (b) GDPR): System Access Control**

To ensure secure system access, the following measures are in place:

- IT systems/devises usable only after password-based network authentication with user ID
- Limitation of failed login attempts
- Use of user codes for data and programs (authentication via username or username + password)
- Passwords must meet minimum requirements and be changed regularly

- Initial passwords must be changed immediately
- Changed passwords must not resemble the last six passwords
- Use of encryption routines for hard drives (BitLocker) in line with state-of-the-art
- Management and assignment of user rights (differentiated access restrictions, e.g., by segment blocks and user roles)
- Use of a firewall with respective proper configuration
- Use of antivirus software
- Automatic screen lock after three minutes of inactivity
- Privacy filters on monitors
- Virus protection policy in place
- All employees are made familiar with and bound by data confidentiality

2.3. **Ensuring Confidentiality (acc. to Art. 32 (I) (b) GDPR): Data Access Control**

To prevent unauthorized activities within hema.to's systems beyond granted authorizations, the following measures are in place:

- Implementation of role structures to differentiate access rights
- Database rights assigned by IT based on HR specifications
- Access rights restricted to an absolute minimum
- Minimal number of administrators
- Protection against unauthorized internal and external access via passwords and firewalls
- Regular application of security updates
- Printed documents with personal data or project related information no longer needed are destroyed using a shredder
- Hard drives of departing employees are overwritten multiple times

2.4. **Purpose Limitation (acc. to Art. 28 (3) sentence 2 (b) GDPR): Separation Control**

Separate processing of data collected for different purposes is achieved as follows:

- Data minimization via defined database rights
- Separation of processing systems (backend: networks, software)
- Control via authorization concepts
- Internal multi-client capability/purpose limitation

- Separation of functions

2.5. **Integrity (acc. to Art. 32 (1) (b) GDPR): Transfer Control**

Measures to ensure that personal data cannot be read, copied, modified or removed in an unauthorized manner during electronic transmission or during transport or storage on data carriers, and that it is possible to check and determine at which points personal data is to be transmitted by data transmission facilities. To ensure confidentiality during electronic data transmission encryption techniques and virtual private networks can be used.
Measures for data carrier transport or data transfer include transport containers with locking devices and regulations for the destruction of data carriers in accordance with data protection requirements.

With regard to the transfer of personal data the following measures are taken:

- Use of an up-to-date firewall
- Encryption of data on data carriers
  - Where feasible, data/e-mail messages are transmitted in encrypted form (depending on the state-of-the-art).
  - Encrypted FTP via TLS
- Assignment of rights in programs and applications to define authorized persons (see: Access Control)
- Separate storage of confidential data in security cabinets
- If mobile data carriers are required, the IT department provides encrypted USB sticks

2.6. **Integrity (acc. to Art. 32 (1) (b) GDPR): Input Control**

The traceability of data entries, changes and deletions is ensured by the system through the following measures:

- Logging of data entries, changes and deletions
- Each employee has a traceable ID in the system so that changes can be assigned
- Access to data is based on authorizations. This ensures that no data changes can be made unnoticed
- All employees are bound to data secrecy

2.7. **Availability and Resilience (Art. 32 (1) (b) GDPR): Availability Control**

The following measures are taken to ensure the availability of the systems:

- Regular back-up procedure for rapid data recovery, ensured by the IT department as part of regular daily/weekly/monthly back-ups.
- Additional use of automatic storage mechanisms
- Fire protection plan
- Annual safety training for employees
- Designated first aiders and fire protection officers
- Mirroring of hard drives
- Uninterruptible power supply (UPS)

2.8. **Procedure for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR): General**

General procedures for regular review, assessment and evaluation:

- Regular review of data protection-related processes
- Regular training and awareness-raising for employees
- Appointment of a data protection officer
- Keeping an overview of processing activities (Art. 30 GDPR)
- No calls on desk-policy (only in phone booths or meeting rooms)
- If necessary, carrying out data protection impact assessments (Art. 35 GDPR)

2.9. **Procedure for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR): Order Control**

hema.to only works with processors who provide sufficient guarantees that appropriate technical and organizational measures are implemented in such a way that processing is carried out in accordance with the requirements of the GDPR and the protection of the rights of the data subject is ensured. Processing by a processor is carried out on the basis of a contract in accordance with Art. 28 GDPR, which specifies, among other things, the subject matter and duration of the 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.

Additionally, the following measures are also taken to ensure order control:

- Clear contract design
- Checking work results
- Separation of responsibilities and obligations between hema.to and the client
- Regular training of hema.to employees in data protection law
- When external service providers or third parties are involved, a data processing agreement is concluded in accordance with the relevant

2.10. **Procedures for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR): Incident response management**

- Preventive: Firewalls and virus scanners are constantly updated
- Use and regular updating of spam filters
- Responsibilities and processes defined in the event of security breaches
- Reporting process for data breaches pursuant to Art. 4 (12) GDPR to the supervisory authorities (Art. 33 GDPR)
- Reporting process for data breaches in accordance with Art. 4 (12) GDPR to the persons concerned (Art. 34 GDPR)

2.11. **Privacy-friendly default settings and data protection through technology (Art. 25 (2) GDPR)**

Measures that result in increased protection of personal data are firstly, the principle of "privacy by design", which incorporates data protection into the technical design of a program. And, secondly, "privacy by default" which strengthens data protection through user-friendly (default) settings.

The privacy-friendly default settings are supported by the following IT systems:

- All systems that can be used to process personal data are used with privacy-friendly default settings in accordance with the software options available
- No more personal data is collected than is necessary for the respective purpose
- Easy exercise of the data subject's right of revocation through technical measures

- Default settings must be provided for the development of new applications/systems and the establishment of new data processing procedures in order to ensure role and rights configuration and to define the type and scope of personal data with regard to its processing and storage.

2.12. **Further Measures**

Any and all employees of hema.to who process personal data are obliged to maintain confidentiality in writing in accordance with Art. 28 (3) (b) GDPR. Employees are regularly sensitized and trained in the handling of personal data.

3. **Final Provision**

The data protection measures at hema.to are kept up to date with the latest technical and legal developments through a continuous improvement process. The technical and organizational measures are evaluated and adapted on an ongoing basis.