honeysales Terms and Conditions

Effective Date: 15.08.2025

1. Introduction

1.1 Scope and Service Overview

honeysales GmbH, based in Oranienstraße 10-11, 10997 Berlin, provides a subscription-based application for business-to-business (B2B) organizations to streamline sales processes. Key features include:

- Integrated lead database and automatic enrichment process.
- Prospect monitoring and fetching, scoring and ranking of sales signals.
- Automated Messaging: the honeysales application pre-writes personalized outreach messages.

1.2 Contractual Basis and Contract Formation

These Terms and Conditions (T&Cs) are part of every contract concluded between honeysales and the Client, unless otherwise agreed in the associated Service Level Agreement (SLA). This contract bindingly regulates the provision and use of the software provided. The contract is formalized upon written confirmation (e.g., digital or handwritten signature) of the subscription plan. It governs the relationship for the subscription period and renews unless terminated.

1.3 Amendments to the T&Cs

honeysales may amend these T&Cs due to changes in law, court rulings, regulatory requirements, market conditions, or updates of the honeysales application. Changes will be communicated via email at least four weeks before taking effect. The Client may object in writing within two weeks. If no objection is made, the changes will be deemed accepted, provided the notification explains this consequence.

For essential changes affecting core obligations, Client consent is required. If the Client objects, the agreement will continue under the previous terms, but honeysales may terminate the contract with one month's notice if the changes are operationally or legally necessary.

Minor changes, such as formatting or feature updates, that do not impact pricing, legal obligations, or major functionalities, may take effect immediately.

1.4 Definitions

- Service: honeysales application, its features and support.
- User: Individual accessing the honeysales services.
- Subscription Plan: Agreement detailing access scope, fees, and duration.
- Force Majeure: Events beyond reasonable control (e.g., natural disasters, cyber-attacks).
- Prospect: A prospect refers to any individual whose data is entered, transferred, or generated by the User within the honeysales application for the purpose of identifying, tracking, or managing potential business contacts or customer relationships.

2. User Responsibilities

2.1 Responsibilities using the honeysales application

The Client is solely responsible for all activities performed using the honeysales application, the results of these activities, and the processes behind them. This includes, but is not limited to:

- Compliance with applicable Laws: The Client is solely responsible for ensuring that their use of the honeysales application complies with all applicable data protection laws and competition laws, including GDPR and German UWG. This includes:
  - Establishing a lawful basis for processing personal data when using honeysales features.
  - Ensuring all data collected, provided, or migrated is accurate, complete, and lawful.
  - Use legal contact options for contacting prospects such as LinkedIn-Options, Email only in case of written consent.
- Proper Use of the Software: The Client agrees to use the honeysales application solely for its intended purpose as outlined in the contract. This includes:
  - Ensuring appropriate configuration and setup of features to achieve optimal results.
  - Assigning access only to authorized personnel and maintaining secure access credentials.
  - Avoiding misuse of the software, such as attempting to circumvent system safeguards or using it for unlawful purposes.
- Indemnification for Misuse: The Client agrees to indemnify honeysales against any claims, fines, or damages arising from:
  - Non-compliance with GDPR or other applicable regulations related to data protection and outreach activities.
  - Unlawful use of the honeysales application, including breaches of third-party rights or misuse of personal data.

Failure to comply with these responsibilities may result in restricted or suspended access to the Service, except in cases requiring immediate action to prevent harm to honeysales, its systems, or other users. Immediate action may include temporary suspension to address urgent issues, such as GDPR violations, data breaches, or actions jeopardizing system integrity.

In cases of proven non-compliance directly causing costs, such as third-party claims or regulatory fines, honeysales reserves the right to recover reasonable and documented costs from the Client.

2.2 Responsibilities for Configuration and Administration

The Client is solely responsible for configuring and administering their honeysales Account. This includes:

- Creation of user accounts, assignment of roles, and granting of appropriate access and rights.
- Ensuring that access to the honeysales application is granted only to personnel with appropriate roles and responsibilities.
- Ensuring that authorized personnel understand how to use the application, including the activation of features that may incur activation fees (3.1 Pricing Components: Activation Fee).
- Integration of honeysales services into the Client's third-party systems to ensure seamless operation.

These responsibilities ensure optimal use of the honeysales application and enable effective management of the Client's sales processes.

2.3 Technical and Operational Requirements

To ensure proper usage of the Service, the Client must:

- Maintain an internet connection with sufficient bandwidth and latency.
- Use the latest version of a supported browser (e.g., Google Chrome, Safari, or Microsoft Edge). Functional cookies must be enabled for full functionality. honeysales is not liable for restrictions arising from the Client's refusal to allow cookies.
- Implement state-of-the-art IT security measures to safeguard access and data integrity.
- Ensure all necessary technical configurations are in place, including secure networks (e.g., VPN) and non-shared accounts.

3. Payment Terms

3.1 Pricing Components
Below is an overview of the pricing components:

- Standard Onboarding: The Standard Onboarding package includes three sessions, facilitated by the honeysales Customer Success Team:
  - 1) (In-App) Onboarding Session: Comprehensive setup support, including technical configuration.
  - 2) (Virtual in-person) Go-Live Support: Training on how to effectively use the honeysales application.
  - 3) (Virtual in-person) Performance Review: Evaluation of tool usage, with actionable insights and tips for improvement.
  - Additional Support: Option to book additional assistance through a tailored consulting package.
- Additional Prospects: Clients gain access to the honeysales lead database, where they can filter, preview and add prospects.
  - Prospects can be added to monitoring if sufficient monitoring capacity is available.
  - Each prospect added to the monitoring via the database incurs a per-prospect charge.
- Organization Access: This is a monthly subscription fee that provides Clients with access to the honeysales application and its features for one user seat and capacity to monitor up to a set number of prospects, defined in the Subscription Plan.
- Extra User Seat: Clients can expand by purchasing additional user seats. Each user seat includes their own access to the honeysales application and monitoring capacity of 2,000 leads.
- Extra Monitoring Capacity: For Clients who wish to monitor more prospects - beyond the capacity included in their seat - additional monitoring capacity can be purchased.

3.2 Subscription Plans and Billing

- Subscriptions are available on monthly, quarterly, or annual billing cycles, as documented in the SLA. Fees for the entire subscription period are invoiced as an upfront payment at the start of the agreed billing cycle. Payment must be received within 3 days of the invoice date.
- Pro rata adjustments for mid-cycle changes are handled as follows: When adding user seats, the prorated costs for the remainder of the current cycle are invoiced immediately and are due upon receipt of the adjusted invoice. The new number of user seats is activated right away. When removing user seats, the change will only take effect at the start of the next billing period, and no immediate refund will be issued for the current cycle.

3.3 Payment Methods
Payments are accepted via credit/debit cards. The option to use bank transfers depends on the Client's headquarter location and payment amounts.

3.4 Taxes and Pricing
All prices are quoted net of VAT or applicable taxes. The Client is responsible for ensuring compliance with local tax regulations. VAT or equivalent taxes will be added to the invoice where applicable. The Client acknowledges that Stripe may charge separate transaction fees, which are not included in the honeysales fees.

3.5 Late Payments
If the upfront payment is not received within the agreed 3-day period from the invoice date, honeysales reserves the right to delay the start of the service or suspend access until all outstanding amounts are paid .

- Suspension of Services: honeysales reserves the right to suspend the Client’s access to the Service until all outstanding amounts, including applicable late fees, are fully paid. A written notice will be issued prior to suspension.
- Late Payment Interest: For overdue payments, honeysales may charge interest as follows: For business Clients (B2B): Interest is calculated at the statutory rate of 9 percentage points above the base interest rate (§288(2) BGB). The applicable base interest rate is determined by the Deutsche Bundesbank.
- Administrative Fees: In addition to interest, honeysales may charge a fixed administrative fee of €40 per overdue invoice, as permitted under §288(5) BGB. Additional collection costs incurred due to the delay, such as legal or agency fees, may also be billed to the Client.
- Acceleration Clause: In the event of non-payment extending beyond 30 days, honeysales reserves the right to:
  - Declare all outstanding amounts under the contract immediately due and payable.
  - Terminate the agreement for cause in accordance with Clause 6.2.
- Notification of Late Payments: honeysales will notify the Client of overdue payments via email or in-app notifications. The Client must remit payment within 3 days of receiving the notification to avoid further action.

3.6 Disputed Payments
Users must notify honeysales of any billing disputes within 3 days of the invoice date by contacting finance@honeysales.io. Disputed amounts will be reviewed promptly. Undisputed amounts must be paid by the due date to avoid service interruptions.

3.7 Refund Policy
Refunds are not issued for early cancellation. For SLA breaches, honeysales may issue service credits at its discretion for downtime exceeding 1% of the agreed annual uptime guarantee. No refunds are applicable for downtime caused by scheduled maintenance, force majeure, or Client-side issues. Refunds may be provided for non-delivery of services (inability to access the service for 48 hours or more), subject to review by honeysales. No refunds, including prorated refunds, will be issued for early termination of subscription plans, even in the case of upfront payments. Refunds are not issued for early cancellation.

4. Grant of Rights

4.1 Use and Retention of Anonymized Data
To improve and develop its Service, honeysales is authorized to anonymize and retain data collected during the term of this agreement. Anonymized data is data that has been stripped of all personal identifiers and cannot be traced back to an individual. The Client agrees that honeysales may retain and use anonymized data for purposes such as:

- Enhancing algorithms and service functionality.
- Conducting analytics and market research.
- Developing diagnostic and security improvements.

Anonymized data will be stored separately from personal data and is not subject to deletion obligations under GDPR.

4.2 Marketing and Public Relations
The Client agrees that honeysales may reference the cooperation between the parties for marketing purposes. This includes, but is not limited to:

- Press releases highlighting the partnership.
- Social media posts about the collaboration.

- Mentions on the honeysales homepage (e.g., success stories).

honeysales agrees to represent the Client positively in all such materials. The Client may withdraw this consent at any time with future effect by providing written notice to honeysales. Upon withdrawal, honeysales will refrain from future use of the Client's name and logo.

4.3 Licence to Use Software
Depending on the subscribed service level, honeysales grants the Client a non-exclusive, non-transferable, and time-limited right to use the subscribed software for the duration of the contractual agreement. The Client agrees to not transfer the software or allow third-party access without prior written consent from honeysales. For the use of third-party systems and the integration of partner services, the respective provider's T&Cs apply.

5. Term and Termination
5.1 Licence Term
The standard term is twelve months. Unless otherwise agreed, the licence automatically renews for an additional twelve months unless either party terminates the agreement with one months' (30 days) notice prior to the renewal date.

5.2 Extraordinary Termination
The right to terminate the contract for good cause remains unaffected. Good cause is deemed to exist in particular if:

- Serious Breach of Contract: Either party commits a material breach of contract that makes it unreasonable to continue the agreement, provided that:
    - The non-breaching party has issued a written notice detailing the breach and provided a 14-day period to remedy the breach.
    - If the breach is not remedied within this period, the non-breaching party may terminate the agreement with immediate effect.
- Payment Defaults: The Client is more than two months overdue on payments despite a written reminder and a 14-day grace period to settle the outstanding amounts.
- Insolvency proceedings are initiated, rejected due to lack of assets, or the Client fails to meet financial obligations such as two consecutive late payments. Financial deterioration includes instances where credit ratings are downgraded, or significant financial risk is documented.
- Legal Non-Compliance: Either party becomes subject to regulatory or legal constraints that make it impossible to continue the agreement in compliance with applicable laws.

5.3 Data Management Before Contract Termination
The Client is responsible for securing their data in a timely manner before the end of the contract. honeysales will provide reasonable assistance for data transfer. After the contract ends, honeysales generally cannot guarantee access to the Client's data for technical reasons. The data will remain accessible until 30-days post-termination. During the term of the contract, honeysales will not delete any data entered by the Client into the application unless legally required to do so (e.g., due to data protection laws or violations).

5.4 Form of Termination
Termination must be made in text form, such as via email or written notice.

6. Service Features and Availability
6.1 Service Commitment
honeysales strives to achieve 99% annual uptime, excluding scheduled maintenance, force majeure events, third-party disruptions, or user misconfigurations. While honeysales strives to meet the stated uptime target, the Client acknowledges that occasional disruptions may occur due to factors beyond honeysales' control or in the course of ensuring service improvements. This service commitment reflects honeysales' best efforts to provide reliable service but does not constitute a guarantee. honeysales is not liable for downtime caused by force majeure, third-party providers, or other factors beyond its reasonable control. This includes, but is not limited to, any service disruptions, payment processing failures, or data breaches caused by Stripe or other third-party payment providers. This service commitment represents honeysales' sole obligation regarding service availability.

6.2 Modifications to the Service
Material changes will be communicated at least 30 days in advance, except for immediate changes required for compliance or security reasons.

6.3 Third-Party Integrations
honeysales integrates with CRMs and other tools. By enabling integrations, Users consent to data sharing with third-party systems. honeysales is not liable for data handling practices of third parties
By making a payment through Stripe, the Client agrees to the transfer of necessary data (e.g., billing information) to Stripe. The Client acknowledges that honeysales has no control over or liability for the data processing practices of Stripe. For more information, please refer to Stripe's privacy policy and terms of service.

7. Data Protection
7.1 Role and Responsibilities
honeysales acts as a Data Processor on behalf of the Client, who serves as the Data Controller. All processing activities comply with the European General Data Protection Regulation (GDPR) and are governed by the Data Processing Agreement (DPA; in German: Auftragsverarbeitungsvertrag / AVV) attached to this document. By accepting these Terms, the Client also agrees to the terms of the DPA.

7.2 Scope of Data Processing
honeysales processes personal data solely fulfil its contractual obligations and in accordance to applicable GDPR laws. This includes data provided by the Client or collected from public and professional sources, such as:

- Publicly available websites.
- Professional platforms (e.g., LinkedIn).
- Public posts and comments on social media platforms (e.g., Facebook, Instagram, Twitter), provided they are shared openly by the authors.

The scope is limited to professional data such as names, job titles, email addresses, and company affiliations. honeysales does not process sensitive data (e.g., medical or demographic information) unless explicitly authorized and required by law.

7.3 Data Security
honeysales employs robust technical and organizational measures to safeguard personal data against unauthorized access, alteration, and misuse. These measures include:

- Encryption: Data is encrypted during both storage and transmission.
- Access Control: Only authorized personnel have access to personal data.
- Breach Management: A protocol is in place to detect, report, and address data breaches promptly in compliance with GDPR.
- Regular Audits: Periodic assessments are conducted to maintain high-security standards.

7.4 Data Retention and Deletion
honeysales retains personal data only for as long as necessary to fulfil the agreed services or as legally required. Specifically:

- Data is deleted upon termination of the agreement, unless retention is legally mandated.
- Clients can request the deletion of personal data by contacting datasecurity@honeysales.io.

honeysales will process such requests promptly, except for data subject to legal retention requirements.

7.5 Client Obligations
As the Data Controller, the Client is responsible for ensuring all personal data shared with honeysales complies with GDPR. This includes:

- Establishing a lawful basis for processing personal data.
- Ensuring shared data is accurate, relevant, and free from sensitive information unless explicitly required and legally justified.
- Informing affected individuals, where applicable, of the data processing activities carried out by honeysales on their behalf.

7.6 Third-Party Data Sharing
If honeysales provides the Client with personal data of third parties, the Client agrees to use such data exclusively for the purposes specified in this agreement and in compliance with GDPR. The Client must obtain additional consents if required for further processing or sharing of such data. With use inside the EU the Client should use the LinkedIn outreach-option instead of the Email-option, as far the Client has not the consent of the prospect to contact him via Email-Option The Client agrees to process shared third-party data in accordance with GDPR and to secure the necessary consents where required. honeysales will not be liable for Client misuse of third-party data provided through the Service.

7.7 Legitimate Interest
honeysales processes data based on the legitimate interest of the Client to facilitate relevant business outreach and commercial activities. The Client acknowledges that this serves as the legal basis for processing under this agreement.

7.8 Data Subject Rights
The Client, as the Data Controller, is responsible for addressing data subject requests under GDPR. honeysales, as the Data Processor, will provide reasonable support to the Client, where necessary, to facilitate compliance with these requests. Such requests, which may include access, rectification, deletion, restriction, or portability of personal data, should be submitted to datasecurity@honeysales.io. honeysales will process requests in accordance with GDPR and within reasonable timeframes, based on the scope of the services provided.

7.9 Data Breaches
honeysales will notify the Client of any personal data breach affecting their data within 72 hours of becoming aware of the breach.

- A description of the breach and the data involved.
- Contact details of the data protection officer or relevant contact.
- Likely consequences of the breach.
- Measures taken to address and mitigate the breach.

7.10 Termination and Data Deletion
Upon termination of the agreement, honeysales will delete all personal data processed on behalf of the Client, unless retention is required by law. A written confirmation of deletion can be provided upon request.

8. Intellectual Property
8.1 Ownership and User Rights
honeysales owns all intellectual property, including software and algorithms. Users may not reverse-engineer, replicate, or sublicense the application.

8.2 Enforcement
honeysales will take legal action against unauthorized use or infringement of its intellectual property.

9. Warranties and Liability
9.1 Defect Liability
The Client must promptly report any defects or disruptions, including details of their occurrence, to honeysales. honeysales will endeavour to resolve reported issues in a reasonable timeframe and may implement temporary workarounds if they are acceptable to the Client. honeysales will provide the Service in a condition suitable for its intended use and maintain it free from material or legal defects.

9.2 Limitation of Liability
honeysales is liable only for damages caused by:

- Intentional misconduct or gross negligence by honeysales, its legal representatives, or agents;
- Negligent breach of essential contractual obligations (cardinal duties), but only for foreseeable damages typical of such agreements;
- Injury to life, body, or health caused by negligence;
- Mandatory statutory liability.

The Client's claims for damages are limited to the total amount of service fees paid by the Client in the 12 months preceding the event giving rise to the claim. Any further claims, including but not limited to indirect or consequential damages, loss of profits, or financial losses, are excluded to the extent permitted by law.
This limitation of liability does not apply where mandatory statutory provisions prohibit such exclusions or limitations.

9.3 Exclusion of Strict Liability
Liability for initial defects under § 536a I Alt. 1 BGB is excluded unless the defect was caused intentionally or through gross negligence.

9.4 Warranty Period
Claims for defects must be asserted within three (3) months of the provision of the Service. This timeframe does not limit statutory rights for damages under Clause 10.2 or other mandatory legal provisions.

9.5 Force Majeure
honeysales shall not be liable for any delay or failure to perform its obligations under this agreement if such delay or failure is caused by events beyond its reasonable control (Force Majeure). These events include, but are not limited to:

- Natural disasters (e.g., earthquakes, floods, hurricanes).
- Pandemics, epidemics, or other public health crises, including government-imposed lockdowns.
- Acts of terrorism, war, or civil unrest.
- Cyber-attacks or prolonged technical disruptions affecting global internet infrastructure.
- Power outages or government-imposed restrictions on utilities or operations.
- Prolonged disruptions in supply chains caused by unforeseen global events.

Obligations affected by Force Majeure will resume promptly once the event has ceased. If a Force Majeure event persists for more than 60 consecutive days, either party may terminate the agreement with written notice. Any prepaid fees will not be refunded unless honeysales is unable to deliver any part of the agreed Service for the duration of the Force Majeure event.

10. Confidentiality
10.1 Obligation of Confidentiality
Both parties agree to keep all confidential information disclosed during the contractual relationship strictly confidential. Confidential information includes, but is not limited to:

- Operational processes, business relationships, trade secrets, know-how, work results, and the business model of honeysales.
- Any information labelled as confidential or reasonably understood as confidential based on the circumstances.

Confidential information may not be disclosed to third parties or used for purposes other than fulfilling contractual obligations, except with prior written consent from the disclosing party.

10.2 Exceptions to Confidentiality
The confidentiality obligation does not apply to the aforementioned section 4.3 and to information that:

- Was already known to the receiving party before disclosure by the disclosing party, as evidenced by written records.
- Becomes publicly known without breach of this agreement.
- Is lawfully received from a third party without violation of confidentiality obligations.
- Must be disclosed due to legal requirements, court orders, or regulatory obligations. Where permissible, the disclosing party must notify the other party in advance of such disclosure.

10.3 Employee and Contractor Confidentiality
Each party shall ensure that their employees, contractors, or agents comply with these confidentiality obligations. Confidential information may only be disclosed to individuals who require it to perform contractual duties.

10.4 Penalties for Breach
If the Client breaches this confidentiality obligation, honeysales is entitled to:

- Liquidated Damages: A fixed penalty of €50,000 per breach, subject to reduction or increase if deemed unreasonable by a competent court, taking into account the actual damages suffered.
- Further Compensation: If the actual damages exceed the liquidated amount, honeysales may claim additional compensation for the proven loss.

10.5 Injunctive Relief
honeysales reserves the right to seek immediate injunctive relief in addition to any monetary remedies if a breach of confidentiality threatens irreparable harm.

11. Final Provisions
11.1 Severability Clause
If any provision of this agreement is found to be invalid, illegal, or unenforceable, the remaining provisions will remain in effect. The invalid or unenforceable provision shall be replaced by a legally valid provision that closely reflects the economic intent of the original clause, as determined by a court of competent jurisdiction. If the parties cannot agree on a replacement provision, it will be determined by judicial interpretation through supplementary contract construction. The same applies to any gaps in this agreement.

11.2 Governing Law and Jurisdiction
This agreement is governed by the laws of the Federal Republic of Germany, excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG). The exclusive place of jurisdiction for all disputes arising from or in connection with this agreement, to the extent legally permissible, is Berlin, Germany.

Appendix 1 - Data Processing Agreement (DPA/AVV)

Data Processing Agreement between the client as the controller (hereinafter referred to as "Controller") and honeysales GmbH, Oranienstraße 10-11, 10997 Berlin as the processor (hereinafter referred to as "Processor", Controller and Processor collectively referred to as the “Parties”).

Preamble

The Controller has commissioned the Processor in an already concluded contract (hereinafter referred to as “Main Contract”) for the services specified therein. Part of the contract execution involves the processing of personal data. In particular, Art. 28 GDPR sets certain requirements for such processing. To comply with these requirements, the Parties conclude the following Data Processing Agreement (hereinafter referred to as the “Agreement”), the fulfillment of which will not be separately compensated unless expressly agreed otherwise.

§ 1 Definitions

(1) Controller is defined according to Art. 4 para. 7 GDPR as the entity that alone or jointly with others determines the purposes and means of the processing of personal data.

(2) Processor is defined according to Art. 4 para. 8 GDPR as a natural or legal person, authority, institution, or other entity that processes personal data on behalf of the Controller.

(3) Personal data is defined according to Art. 4 para. 1 GDPR as any information relating to an identified or identifiable natural person (hereinafter referred to as “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, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

(4) Special categories of personal data are defined according to Art. 9 GDPR as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of Data Subjects, personal data according to Art. 10 GDPR concerning criminal convictions and offenses or related security measures, as well as genetic data according to Art. 4 para. 13 GDPR, biometric data according to Art. 4 para. 14 GDPR, health data according to Art. 4 para. 15 GDPR, and data concerning the sexual life or sexual orientation of a natural person.

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

(6) Supervisory authority is defined according to Art. 4 para. 21 GDPR as an independent public authority established by a member state in accordance with Art. 51 GDPR.

§ 2 Subject Matter of the Contract

(1) The Processor provides the services specified in the Main

Contract for the Controller. In doing so, the Processor gains access to personal data, which the Processor processes exclusively on behalf of and according to the instructions of the Controller. The scope and purpose of the data processing by the Processor are derived from the Main Contract and any associated service descriptions. It is the responsibility of the Controller to assess the legality of the data processing.

(2) To specify the data protection rights and obligations of both parties, the Parties enter into this Agreement. The provisions of this Agreement take precedence over those of the Main Contract in case of doubt.

(3) The provisions of this Agreement apply to all activities related to the Main Contract in which the Processor and its employees or agents come into contact with personal data originating from the Controller or collected on behalf of the Controller.

(4) The duration of this Agreement is determined by the duration of the Main Contract, unless further obligations or termination rights arise from the following provisions.

§ 3 Right to Issue Instructions

(1) The Processor may only collect, process, or use data within the framework of the Main Contract and according to the instructions of the Controller. If the Processor is required to carry out further processing by the law of the European Union or the member states to which it is subject, it shall inform the Controller of these legal requirements before processing.

(2) The instructions of the Controller are initially set out in this contract and may be subsequently changed, supplemented, or replaced by the Controller in writing or in text form through individual instructions (specific instruction). The Controller is entitled to issue corresponding instructions at any time. This includes instructions regarding the correction, deletion, and blocking of data.

(3) All instructions issued must be documented by the Controller. Instructions that go beyond the services agreed upon in the Main Contract will be treated as a request for a change in services.

(4) If the Processor believes that an instruction from the Controller violates data protection regulations, it must notify the Controller immediately. The Processor is entitled to suspend the execution of the relevant instruction until it is confirmed or modified by the Controller. The Processor may refuse to execute an obviously unlawful instruction.

(5) The Processor informs the Controller that contacting individuals whose contact details have been generated and transmitted in several European countries is only permissible if prior consent has been obtained from those individuals. This is regularly the case when contacting via social networks such as LinkedIn. Therefore, this method is explicitly offered and recommended by the Processor. Contacting via email is only permissible with the prior consent of the contacted person.

§ 4 Types of Processed Data, Circle of Affected Persons, Third Country

(1) In the context of executing the Main Contract, the Processor gains access to the personal data specified in Appendix 1.

(2) The circle of affected persons by the data processing is outlined in Appendix 2.

(3) The transfer of personal data to a third country (outside the EEA) may only take place under the conditions of Art. 44 et seq. GDPR.

§ 5 Processor's Protection Measures

(1) The Processor is obliged to comply with the legal provisions on data protection and not to disclose or allow access to the information obtained from the Controller to third parties. Documents and data must be secured against unauthorized access, taking into account the state of the art.

(2) The Processor will organize its internal structure in a way that meets the special requirements of data protection. It has implemented the technical and organizational measures specified in Appendix 4 for the adequate protection of the Controller's data in accordance with Art. 32 GDPR, which the Controller recognizes as adequate. Any changes to the security measures taken are reserved for the Processor, provided that the contractually agreed level of protection is not undermined.

(3) Persons employed by the Processor in data processing are prohibited from unlawfully collecting, processing, or using personal data. The Processor will obligate all persons entrusted with the processing and fulfillment of this contract (hereinafter referred to as “Employees”) accordingly (obligation to confidentiality, Art. 28 para. 3 lit. b GDPR) and will ensure compliance with this obligation with due diligence.

(4) The Processor has appointed a Data Protection Officer. The Data Protection Officer of the Processor is heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 6 Information Obligations of the Processor

(1) In the event of disruptions, suspicion of data protection violations or breaches of contractual obligations by the Processor, suspicion of security-related incidents, or other irregularities in the processing of personal data by the Processor, persons employed by it in the context of the assignment, or by third parties, the Processor shall inform the Controller immediately. The same applies to audits of the Processor by the data protection supervisory authority. The report of a data protection breach must at least contain the following information: a) a description of the nature of the data protection breach, if possible, indicating the categories and number of affected persons, the affected categories, and the number of affected personal data records; b) a description of the measures taken or proposed by the Processor to remedy the breach and, if applicable, measures to mitigate its possible adverse effects; c) a description of the likely consequences of the data protection breach.

(2) The Processor will immediately take the necessary measures to secure the data and mitigate possible adverse effects on the affected persons, inform the Controller about this, and request further instructions.

(3) Furthermore, the Processor is obliged to provide the Controller with information at any time, as far as the Controller's data is affected by a breach according to paragraph 1.

(4) The Processor shall inform the Controller of any significant changes to the security measures under § 5 para. 2.

§ 7 Controller's Control Rights

(1) The Controller may verify the technical and organizational measures of the Processor before the data processing begins and then annually. For this purpose, it may, for example, request information from the Processor, have existing expert attestations, certifications, or internal audits presented, or personally inspect the technical and organizational measures of the Processor after timely coordination during normal business hours or have them inspected by a knowledgeable third party, provided that this third party is not in a competitive relationship with the Processor. The Controller will conduct inspections only to the extent necessary and will not unduly disturb the operational processes of the Processor.

(2) The Processor agrees to provide the Controller with all information and evidence necessary for conducting an inspection of the technical and organizational measures of the Processor within a reasonable time frame upon the Controller's oral or written request.

(3) The Controller documents the inspection results and communicates them to the Processor. In the event of errors or irregularities identified by the Controller, particularly in the examination of the results of the assignment, it must inform the Processor immediately. If circumstances are identified during the inspection that require changes to the prescribed process flow to avoid future occurrences, the Controller must promptly inform the Processor of the necessary procedural changes.

§ 8 Use of Service Providers

(1) The contractually agreed services are carried out with the involvement of service providers (hereinafter referred to as “Sub-Processors”). A list of Sub-Processors can be requested in writing by the client. The Controller grants the Processor its general approval within the meaning of Art. 28 para. 2 sentence 1 GDPR to commission further Sub-Processors or to replace those already commissioned within the framework of its contractual obligations.

(2) The Processor will inform the Controller before any intended change regarding the engagement or replacement of a Sub-Processor. The Controller may object to an intended engagement or replacement of a Sub-Processor for important data protection reasons.

(3) The objection against the intended engagement or replacement of a Sub-Processor must be raised within 2 weeks after receipt of the information about the change. If no objection is raised, the engagement or replacement is deemed approved. If there is an important data protection reason and an amicable solution between the Controller and the Processor is not possible, the Processor has a special right of termination at the end of the month following the objection.

(4) The Processor is obliged to contract Sub-Processors in accordance with the provisions of this Agreement.

(5) A Sub-Processing relationship in the sense of these provisions does not exist if the Processor commissions third parties with services that can be considered pure ancillary services. This includes, for example, postal, transport, and shipping services, cleaning services, telecommunications services without a specific reference to services provided by the Processor for the Controller, and security services. Maintenance and inspection services represent Sub-Processing relationships requiring approval, as far as they are provided for IT systems that are also used in connection with the provision of services for the Controller.

§ 9 Inquiries and Rights of Data Subjects

(1) The Processor supports the Controller as far as possible with appropriate technical and organizational measures in fulfilling its obligations under Art. 12–22 and 32 to 36 GDPR.

(2) If a Data Subject asserts rights, such as the right to information, correction, or deletion regarding their data directly against the Processor, the Processor will not respond independently but will refer the Data Subject to the Controller and await its instructions.

§ 10 Liability

(1) For the compensation of damages that a Data Subject suffers due to unlawful or incorrect data processing or use under data protection laws within the framework of the data processing, only the Controller is responsible towards the Data Subject in the internal relationship with the Processor.

(2) The Processor is liable for damages without limitation, insofar as the cause of the damage is based on an intentional or grossly negligent breach of duty by the Processor, its legal representatives, or vicarious agents.

(3) For negligent behavior, the Processor is liable only in the event of a breach of a duty whose fulfillment is essential for the proper execution of the contract and on which the Controller regularly relies and may rely, but limited to the typical average damage for the contract. Otherwise, the Processor's liability - including for its vicarious agents - is excluded.

(4) The limitation of liability according to § 10.3 does not apply to claims for damages arising from injury to life, body, health, or the assumption of a guarantee.

§ 11 Termination of the Main Contract

(1) Upon termination of the Main Contract, the Processor will return all documents, data, and data carriers entrusted to it to the Controller or - at the Controller's request, unless there is an obligation to retain personal data under Union law or the law of the Federal Republic of Germany - delete them. This also applies to any backups held by the Processor. The Processor must provide documented proof of proper deletion upon request.

(2) The Controller has the right to verify the complete and contractual return or deletion of the data with the Processor in an appropriate manner.

(3) The Processor is obliged to treat confidentially the data it has become aware of in connection with the Main Contract even beyond the end of the Main Contract. This Agreement remains valid beyond the end of the Main Contract as long as the Processor has personal data that has been provided to it by the Controller or that it has collected for the Controller.

§ 12 Final Provisions

(1) Insofar as the Processor does not expressly carry out support actions under this Agreement free of charge, it may charge the Controller a reasonable fee for this, unless the Processor's own actions or omissions have made this support directly necessary.

(2) Changes and additions to this Agreement must be made in text form. This also applies to the waiver of this formal requirement. The priority of individual contractual agreements

remains unaffected.

(3) Should individual provisions of this Agreement be wholly or partially ineffective or unenforceable, the validity of the remaining provisions shall not be affected.

(4) This Agreement is subject to German law.

Appendix 1 – Description of Data Categories (if found): First name, Last name, Email, LinkedIn Profile URL, Company department, Seniority, Job title, Location (City, Country), Gender, Company name, Last contact time, Last response time

Appendix 2 – Description of Affected Persons/Affected Groups: Controllers, Customers of the data controller, Persons who may be interested in the offers of the client, Other third parties

Appendix 3 – Technical and Organizational Measures of the Processor

1. Introduction

This appendix summarizes the technical and organizational measures taken by the Processor in accordance with Art. 32 para. 1 GDPR. These measures protect personal data. The document aims to assist the Processor in fulfilling its accountability obligations under Art. 5 para. 2 GDPR.

2. Confidentiality (Art. 32 para. 1 lit. b GDPR)

2.1. Access Control

The following implemented measures prevent unauthorized access to data processing systems:

- Alarm system
- Automated access control system
- Chip card / transponder locking system
- Light barriers / motion detectors
- Locking system with code lock
- Intercom system with camera
- Visitors only accompanied by employees
- Security locks
- Doors with knobs on the outside
- Care in selecting cleaning services

2.2. Access Control

The following implemented measures prevent unauthorized access to data processing systems:

- Authentication with user and password
- Central password rules
- Use of two-factor authentication
- Encryption of data carriers
- Managing user permissions
- Creating user profiles
- Central password issuance
- "Secure Password" policy
- "Deletion / Destruction" policy
- "Clean desk" policy
- General data protection and/or security policy
- Mobile Device Policy
- Instructions for "Manual Desktop Locking"

2.3. Access Control

The following implemented measures ensure that unauthorized persons do not have access to personal data:

- Management of user rights by system administrators
- The number of administrators is kept as small as possible
- Use of a permission concept

2.4. Separation Control

The following measures ensure that personal data collected for different purposes are processed separately:

- Separation of production and test systems
- Logical tenant separation (software-based)
- Control via permission concept

3. Integrity (Art. 32 para. 1 lit. b GDPR)

3.1. Transfer Control

It is ensured that personal data cannot be unlawfully read, copied, altered, or removed during transmission or storage on data carriers, and it can be verified which persons or entities have received personal data. The following measures are implemented to ensure this:

- Email encryption
- Provision via encrypted connections such as sftp, https

3.2. Input Control

The following measures ensure that it can be verified who has processed personal data at what time in data processing systems:

- Logging of data input, modification, and deletion
- Traceability of input, modification, and deletion of data by individual usernames
- Granting of rights for input, modification, and deletion of data based on a permission concept
- Retention of forms from which data has been transferred to automated processing
- Clear responsibilities for deletions

4. Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the client:

- Fire and smoke alarm systems

5. Procedures for Regular Review, Assessment, and Evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

5.1. Data Protection Management

The following measures aim to ensure that an organization meeting the basic requirements of data protection law is in place:

- Use of the heyData platform for data protection management
- Appointment of the data protection officer heyData
- Obligation of employees to confidentiality
- Regular training of employees in data protection
- Keeping an overview of preparatory activities (Art. 30 GDPR)
- Central documentation of all processes and regulations regarding data protection with access for employees as needed/authorized (e.g., Wiki, Intranet, etc.)
- An annual review of the effectiveness of technical protection measures
- The organization complies with the information obligations under Art. 13 and 14 GDPR

5.2. Incident Response Management

- The following measures aim to ensure that reporting processes are triggered in the event of data protection violations:
- Reporting process for data breaches according to Art. 4 No. 12 GDPR to the supervisory authorities (Art. 33 GDPR)
- Reporting process for data breaches according to Art. 4 No. 12 GDPR to the affected individuals (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data breaches
- Use of spam filters and regular updates

5.3. Data Protection Friendly Defaults (Art. 25 para. 2 GDPR)

The following implemented measures take into account the requirements of the principles "Privacy by design" and "Privacy by default":

- Training of employees in "Privacy by design" and "Privacy by default"
- No more personal data is collected than is necessary for the respective purpose.

5.4. Contract Control

The following measures ensure that personal data can only be processed in accordance with the instructions:

- Written instructions to the contractor or instructions in text form (e.g., through the Data Processing Agreement)
- Ensuring the destruction of data after the termination of the contract (e.g., by requesting relevant confirmations)
- Confirmation from contractors that they obligate their own employees to confidentiality (typically in the Data Processing Agreement).