plugilo

Data processing agreement

between

the Customer

as the controller (hereinafter referred to as the "**Controller**"),

and

Plugilo Inc., 200 Continental Drive, Suite 401, Newark, Delaware 19713, USA

as the processor (hereinafter referred to as the "**Processor**,"
Controller and Processor collectively referred to as the "Parties")

Preamble

The Controller has commissioned the Processor in the contract already concluded (hereinafter referred to as the "Main Contract") for the services specified therein. Part of the performance of the contract involves the processing of personal data. In particular, Art. 28 GDPR imposes certain requirements on such processing. In order to comply with these requirements, the Parties enter into the following data

processing agreement (hereinafter referred to as the "Agreement"), the performance of which shall not be remunerated separately, unless expressly agreed otherwise.

§ 1 Definitions

(1) Pursuant to Art. 4 (7) GDPR, the controller is the entity that, alone or jointly with others, determines the purposes and means of the processing of personal data.

(2) Pursuant to Art. 4 (8) GDPR, a processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

(3) Pursuant to Art. 4 (1) GDPR, personal data is any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); A natural person is considered identifiable if they can be identified, directly or indirectly, in particular by association with an identifier such as a name, an identification number, location data, an online identifier or one or more special characteristics that express the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(4) Sensitive personal data are personal data pursuant to Art. 9 GDPR, which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of data subjects, personal data pursuant to Art. 10 GDPR on criminal convictions and offenses or related security measures, as well as genetic data pursuant to Art. 4 (13) GDPR, biometric data pursuant to Art. 4 (14) GDPR, health data pursuant to Art. 4 (15) GDPR, and data concerning the sex life or sexual orientation of a natural person.

(5) Processing is, pursuant to Art. 4 (2) GDPR, 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, distribution or other forms of provision, alignment or combination, restriction, erasure or destruction.

(6) Pursuant to Art. 4 (21) GDPR, a supervisory authority is an independent public authority established by a Member State pursuant to Art. 51 GDPR.

§ 2 Subject matter of the contract

(1) The processor shall provide the controller with the services specified in the main contract. In doing so, the processor shall have access to personal data, which the processor shall process for the controller exclusively on behalf of and in accordance with the instructions of the controller. The scope and purpose of data processing by the processor are set out in the main contract and any associated service descriptions. The controller is responsible for assessing the permissibility of data processing.

(2) The parties conclude this agreement in order to specify their mutual rights and obligations under data protection law. In case of doubt, the provisions of this agreement shall take precedence over the provisions of the main contract.

(3) The provisions of this contract 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 or collected for the controller.

(4) The term of this contract is based on the term of the main contract, unless the following provisions give rise to further obligations or rights of termination.

§ 3 Right to issue instructions

(1) The processor may only collect, process, or use data within the scope of the main contract and in accordance with the instructions of the controller. If the processor is required by European Union or Member State law to which it is subject to carry out further processing, it shall inform the controller of these legal requirements prior to processing.

(2) The instructions of the controller shall initially be laid down in this contract and may subsequently be amended, supplemented or replaced by the controller in writing or in text form by means of individual instructions (individual instructions). The controller shall be entitled to issue such instructions at any time. This includes instructions regarding the correction, deletion and blocking of data.

(3) All instructions issued shall be documented by the controller. Instructions that go beyond the services agreed in the main contract shall 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 immediately notify the controller. The processor is entitled to suspend the execution of the instruction in question until it is confirmed or amended by the controller. The processor may refuse to execute an instruction that is obviously unlawful.

§ 4 Types of data processed, group of data subjects, third country

(1) In the course of performing the main contract, the processor shall have access to the personal data specified in more detail in **Annex 1**.

(2) The group of data subjects affected by the data processing is set out in **Appendix 2**.

(3) Personal data may be transferred to a third country (outside the EEA) under the conditions set out in Art. 44 et seq. GDPR.

§ 5 Protective measures of the processor

(1) The processor is obliged to comply with the statutory provisions on data protection and not to disclose the information obtained from the controller to third parties or to grant them access to it. Documents and data must be secured against access by unauthorized persons, taking into account the state of the art.

(2) The processor shall organize its internal operations in its area of responsibility in such a way that they meet the special requirements of data protection. It shall have taken the technical and organizational measures specified in **Annex 3** for the adequate protection of the controller's data in accordance with Art. 32 GDPR, which the controller recognizes as adequate. The processor reserves the right to change the security measures taken, ensuring that the contractually agreed level of protection is not compromised.

(3) Persons employed by the processor in data processing are prohibited from collecting, processing, or using personal data without authorization. The processor

shall impose corresponding obligations on all persons entrusted by it with the processing and performance of this contract (hereinafter referred to as "employees") (confidentiality obligation, Art. 28 (3) (b) GDPR) and shall ensure compliance with this obligation with due care.

(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, suspected data breaches or breaches of contractual obligations by the processor, suspected security incidents or other irregularities in the processing of personal data by the processor, persons employed by the processor within the scope of the contract or by third parties, the processor shall inform the controller without delay. The same applies to audits of the processor by the data protection supervisory authority. The notification of a personal data breach shall contain at least the following information:

a) a description of the nature of the personal data breach, including, where possible, the categories and number of data subjects concerned, the categories and number of personal data records concerned;

b) a description of the measures taken or proposed by the processor to address the breach and, where appropriate, measures to mitigate its possible adverse effects;

c) a description of the likely consequences of the personal data breach.

(2) The processor shall immediately take the necessary measures to secure the data and mitigate any possible adverse consequences for the data subjects, inform the controller thereof, and request further instructions.

(3) The processor shall also be obliged to provide the controller with information at any time if its data is affected by a breach pursuant to paragraph 1.

(4) The processor shall inform the controller of any significant changes to the security measures pursuant to Section 5 (2).

Section 7 Control rights of the controller

(1) The controller may verify the technical and organizational measures taken by the processor before the start of data processing and then annually. To this end, the controller may, for example, obtain information from the processor, request existing expert opinions, certifications, or internal audits, or personally inspect the technical and organizational measures of the processor after timely consultation during normal business hours, or have them inspected by a competent third party, provided that this third party is not in a competitive relationship with the processor. The controller shall only carry out checks to the extent necessary and shall not disproportionately disrupt the operational processes of the processor.

(2) The processor undertakes to provide the controller, upon its verbal or written request, with all information and evidence necessary to carry out a check of the processor's technical and organizational measures within a reasonable period of time.

(3) The controller shall document the results of the inspection and communicate them to the processor. In the event of errors or irregularities identified by the controller, in particular during the review of order results, the controller shall inform the processor immediately. If the review reveals circumstances that require changes to the prescribed procedure in order to be avoided in the future, the controller shall immediately inform the processor of the necessary procedural changes.

§ 8 Use of service providers

(1) The contractually agreed services shall be performed with the involvement of the service providers listed in **Annex 4** (hereinafter referred to as "sub-processors"). The controller shall grant the processor its general authorization within the meaning of Art. 28 (2) sentence 1 GDPR to engage further sub-processors or to replace those already engaged within the scope of its contractual obligations.

(2) The processor shall inform the controller in advance by email newsletter of any intended change regarding the engagement or replacement of a subprocessor. The controller will receive the email newsletter after sending an email with the subject line "Subscribe" to service.provider@plugilo.com. The controller may object to the

intended engagement or replacement of a sub-processor for important data protection reasons.

(3) The objection to the intended involvement or replacement of a sub-processor must be raised within 2 weeks of the information being sent in the email newsletter. If no objection is raised, the involvement or replacement shall be deemed approved. If there is an important reason under data protection law and it is not possible to find a mutually acceptable solution between the controller and the processor, the controller shall have a special right of termination at the end of the month following the objection.

(4) When engaging subcontractors, the processor shall oblige them to comply with the provisions of this agreement.

(5) A subcontracting relationship within the meaning of these provisions does not exist if the processor commissions third parties to provide services that are to be regarded as purely ancillary services. These include, for example, postal, transport, and shipping services, cleaning services, telecommunications services without any specific connection to services provided by the processor for the controller, and security services. Maintenance and testing services constitute subcontracting relationships requiring approval if they are provided for IT systems that are also used in connection with the provision of services for the controller.

§ 9 Requests and rights of data subjects

(1) The processor shall support the controller, where possible, with appropriate technical and organizational measures in fulfilling its obligations under Articles 12–22 and 32 to 36 GDPR.

(2) If a data subject asserts rights, such as the right to information, correction, or deletion of their data, directly against the processor, the processor shall not respond independently, but shall refer the data subject to the controller and await the controller's instructions.

§ 10 Liability

(1) In the internal relationship with the processor, the controller alone shall be liable to the data subject for compensation for damages suffered by the data subject as a result of data processing or use that is inadmissible or incorrect under data protection laws in the context of order processing.

(2) The processor shall be liable without limitation for damages insofar as the cause of the damage is based on an intentional or grossly negligent breach of duty by the processor, its legal representative, or vicarious agent.

(3) The processor shall only be liable for negligent conduct in the event of a breach of an obligation whose fulfillment is essential for the proper execution of the contract and on whose compliance the controller regularly relies and may rely, but limited to the average damage typical for the contract. Otherwise, the liability of the processor—including for its vicarious agents and assistants—is excluded.

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

Section 11 Standard Contractual Clauses

(1) The parties agree that the EU Standard Contractual Clauses ("EU SCC") pursuant to Implementing Decision 2021/914 of the European Commission of June 4, 2021, are hereby incorporated by reference and form an integral part of this DPA, provided that this is required under applicable data protection laws and a transfer to a third country takes place.

The applicable modules of the EU SCC are as follows: Module 2 may apply if the controller acts as controller and data exporter, and Module 3 may apply if the controller acts as processor and data exporter.

Where applicable, the following applies to each module:

(a) In Clause 7, the optional docking clause does not apply.

(b) In Clause 9, Option 2 applies, and the period for prior notice of changes to subprocessors is set out in § 8 of this DPA.

(c) In Clause 11, the optional wording does not apply.

(d) In Clause 17, Option 1 applies, and the EU SCCs are governed by German law.

(e) In Clause 18(b), disputes shall be settled before the courts of Germany.

(f) The Annex to the EU SCCs is completed as follows:

The information required for Annex I(A) is contained in this GTC, the contract, and/or the relevant orders.

The information required for Annex I(B) is contained in Annex 1 (Details of Processing) to this GTC.

The competent supervisory authority in Annex I(C) is determined in accordance with the applicable data protection law; and

The information required for Annex II is contained in Annex 3.

The information required for Annex III can be found in Annex 2.

§ 12 Termination of the main contract

(1) Upon termination of the main contract, the processor shall return all documents, data, and data carriers provided to it to the controller or, at the request of the controller, delete them, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany. This also applies to any data backups held by the processor. The processor shall keep documented evidence of proper deletion upon request.

(2) The controller shall have the right to monitor the complete and contractually compliant return or deletion of the data by the processor in an appropriate manner.

(3) The processor is obliged to treat the data that has become known to it in connection with the main contract as confidential even after the end of the main contract. This agreement shall remain valid beyond the end of the main contract for as long as the processor has personal data that has been forwarded to it by the controller or that it has collected for the controller.

§ 13 Final provisions

(1) Insofar as the processor does not expressly perform support activities 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) Amendments and supplements to this agreement must be made in writing. This also applies to any waiver of this formal requirement. The priority of individual contractual agreements remains unaffected by this.

(3) Should individual provisions of this agreement be or become wholly or partially legally ineffective or unenforceable, this shall not affect the validity of the remaining provisions.

(4) This agreement is subject to German law.

Appendices

Appendix 1 – Description of data/data categories

Last name, first name, address, contact details, preference data, IP addresses, usage behavior within software applications and/or widgets.

Appendix 2 – Description of data subjects/data subject groups

Controllers, customers of the controller

Appendix 3 – Technical and organizational measures of the processor

Introduction

This appendix summarizes the technical and organizational measures taken by the processor within the meaning of Art. 32 (1) GDPR. These are measures with which the processor protects personal data. The purpose of the document is to support the processor in fulfilling its accountability obligation under Art. 5 (2) GDPR.

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

Entry Control

The following implemented measures prevent unauthorized entry to data processing facilities:

- Alarm system
- Automatic access control system

- Security locks
- Video surveillance of entrances
- Person control at the gatekeeper or reception
- Careful selection of security personnel
- Mandatory wearing of employee and guest ID cards
- Visitors only when accompanied by employees
- Careful selection of cleaning staff
- Instruction to employees not to work in publicly accessible spaces (e.g. cafés)
- Working from home: Instruction to employees, if possible, to work in workrooms separated from living areas

Admission control

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

- Authentication with username and password
- Use of anti-virus software
- Use of firewalls
- Use of VPN technology for remote access
- Blocking of external interfaces (e.g. USB ports)
- Encryption of data carriers
- Automatic desktop lock
- Encryption of notebooks/tablets

- Management of user permissions
- Creation of user profiles
- Central password rules
- Use of 2-factor authentication
- Person control at the concierge or reception
- Visitor logging (e.g. visitor book)
- General company policy on data protection or security
- Company policy for secure passwords
- Company policy "Deletion/Destruction"
- Company policy "Clean Desk"
- General instruction to manually lock the desktop when leaving the workplace

Access control

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

- Use of document shredders (with cross-cut function)
- Logging of access to applications (especially for data entry, modification, and deletion)
- Implementation of an authorization concept

- Number of administrators kept as small as possible
- Secure storage of data carriers
- Management of user rights by system administrators
- Instruction to employees that only absolutely necessary data should be printed

Separation control

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

- Physically separate storage on separate systems or data carriers
- Separation of production and test system

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

Transfer control

It is ensured that personal data cannot be read, copied, altered, or removed without authorization during transmission or storage on data carriers and that it can be verified which persons or entities have received personal data. The following measures are implemented to ensure this:

Establishment of VPN tunnels

- WLAN encryption (WPA2 with strong password)
- Logging of access and retrievals

- Provision of data via encrypted connections such as SFTP or HTTPS
- Use of signature procedures
- Creation of an overview of regular retrieval and transmission processes
- Transfer of data in anonymized or pseudonymized form

Input control

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

- Logging of input, modification, and deletion of data
- Manual or automatic control of logs
- Traceability of data input, modification, and deletion through individual usernames (not user groups)
- Clear responsibilities for deletions

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 extinguishers in server rooms
- Fire and smoke detection systems
- Air conditioning in server rooms

- Protected power strips in server rooms
- Uninterruptible power supply (UPS)
- Data protection vault
- RAID system / disk mirroring
- Regular backups
- Creation of a backup & recovery concept
- Monitoring of the backup process
- Creation of an emergency plan (e.g., BSI IT-Grundschutz 100-4)
- Regular tests for data recovery and logging of results
- No sanitary facilities in or above the server room
- Separation of operating systems and data

Procedures for regular review, assessment, and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Data protection management

The following measures are intended 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 heyData as the data protection officer
- Obligation of employees to data secrecy
- Regular training of employees in data protection
- Keeping a record of processing activities (Art. 30 GDPR)

Incident-Response-Management

The following measures ensure that reporting processes are triggered in the event of data protection violations:

- Reporting process for data protection violations according to Art. 4 No. 12 GDPR to the supervisory authorities (Art. 33 GDPR)
- Reporting process for data protection violations according to Art. 4 No. 12 GDPR to the data subjects (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data breaches
- Use of anti-virus software
- Use of firewalls

Privacy-friendly default settings (Art. 25 para. 2 GDPR)

The following implemented measures take into account the principles of "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 necessary for the respective purpose.

Order control

By the following measures, it is ensured that personal data can only be processed according to instructions:

- Written instructions to the contractor or instructions in text form (e.g., via data processing agreement)

- Ensuring the destruction of data after the end of the contract, e.g., by requesting corresponding confirmations

- Confirmation from contractors that they obligate their own employees to data secrecy (typically in the data processing agreement)

- Careful selection of contractors (especially regarding data security)

- Ongoing review of contractors and their activities
- Previous verification of the security measures taken by contractors and corresponding documentation

Appendix 4 – Current subcontractors

Name	Function	Server location
Google Alphabet Inc 1600 Amphitheatre Parkway, Mountain View, CA 94043, US	Google Analytics 4: Next-generation analytics platform with event-based tracking, machine learning insights, and	EU

	cross-platform measurement	
	Google Workspace: Cloud-based productivity and collaboration suite including Gmail, Drive, Docs, and communication tools	EU
	Google Cloud: Cloud Vision API and Firebase services using service accounts with no personal data processing	EU and US
	Google OAuth: OAuth 2.0 authentication service for secure user login and authorization	EU and US
	Google Tag Manager: Tag management system for deploying and managing marketing and analytics tags	EU and US
	Google Cloud Vertex AI: AI-powered language models and cognitive services integration	US
Brevo	SendinBlue Email: All-in-one email marketing	EU

106 boulevard Haussmann, 75008 Paris, France	platform with automation, templates, and contact management SendinBlue Marketing Automation: Marketing automation platform with CRM functionality, workflow automation, and customer segmentation	 EU
Amazon.com, Inc 410 Terry Avenue North, Seattle, WA 98109, US	AWS Amazon: Newsletter email server and SMTP services for bulk email delivery	EU
Amplitude, Inc., 631 Howard St. Floor 5. San Francisco, CA 94105, USA	Form optimization and conversion analysis tools for user experience insights	EU
Anthropic PBC, 548 Market St, PMB 90375, San Francisco, CA 94104, USA	Claude - AI functions	USA
OpenAI Ireland Ltd., 1st Floor, The Liffey Trust Centre, 117-126 Sheriff	ChatGPT: AI functions	USA

Street Upper, Dublin 1, D01 YC43, Irland		
DCI Database for Commerce and Industry Romania S.R.L., 28 Strada Transilvaniei Brașov Județul Brașov 500209	Customer	EU
DCI Database for Commerce and Industry AG, Enzianstr. 2, 82319 Starnberg	Holding, newsletter distribution	EU
Content Factory 1 GmbH Enzianstr. 2 82319 Starnberg	Data maintenance	EU