DATA PROCESSING AGREEMENT
GDPR HERO APP

GDPR HERO AB, Trollebergsvägen 5A, 222 29 Lund

Ver. 2024:1

Data Processing Agreement

This data processing agreement (the “DPA”) is entered into in accordance with Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 (GDPR) of the European Parliament and of the Council.

The DPA forms an integral part of the general terms and conditions and any written supplementary agreements (the “Terms”) entered into between the parties. It governs how GDPR Hero AB (company registration number 559088-5116) (”GDPR Hero”), acting as data processor, processes personal data on behalf of the customer also referred to as the ”controller” or “data controller” within the framework of the cloud service GDPR Hero App (the ”Service”).

Table of Content

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1 - Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

Clause 2 - Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3- Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 – Optional Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6 - Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 - Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account

of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall

ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 - Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection

impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 - Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when

the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

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

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10 - Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the

controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ADDITIONAL CLAUSES

Right to compensation

GDPR Hero is entitled to compensation for work performed under this agreement, including but not limited to the following:

a) Implementation of new instructions in accordance with Annex II.

b) Assistance requested by the data controller in accordance with Clause 8.

c) Audits and inspections, in accordance with Clause 7.6(c).

d) Provision of copies of agreements with sub-processors in accordance with Clause 7.7(c).

Compensation will be paid in accordance with the applicable price list or as otherwise agreed between the Parties.

Liability

Where compensation for damage arising from the processing of personal data is payable to a data subject pursuant to a final court judgment or settlement, due to a breach of this DPA and/or applicable data protection law, Article 82 GDPR shall apply.

Any administrative fines imposed under Article 83 GDPR or Chapter 6, Section 2 of the Swedish Act (2018:218) with supplementary provisions to the EU General Data Protection Regulation shall be borne by the Party on which such fine is imposed, in accordance with applicable law.

If either Party becomes aware of any circumstance that may cause damage to the other Party, it shall inform the other Party without undue delay. The Parties shall thereafter cooperate actively to prevent and minimise any potential damage.

*****

ANNEX I – List of Parties

Data Controller

Name (company registration number): Customer, as specified in the agreement document(s) governing the Parties' cooperation (e.g. the Terms, quotations, or other agreements).

Adress: As specified in the agreement document(s) referred to above.

Contact person's name, title, and contact details: As specified in the agreement document(s) referred to above.

Signature and date of accession: As specified in the agreement document(s) referred to above or through digital signing.

Data processor

Name (company registration number): GDPR Hero AB (559088-5116)

Adress: Trollebergsvägen 5A, 222 29 Lund

Contact person's name, title and contact details: Julianne Ahlesten, lawyer, julianne@gdprhero.se.

Signature and date of accession: As executed by digital signature.

*****

ANNEX II – Description of processing

Categories of data subjects whose personal data are processed	The Customer's employees; contact persons at data processors, data controllers, and data protection officers; the Customer's data subjects in connection with the administration of data subject access requests or inquiries; and other categories of data subjects that the Customer chooses to document in the Service for the purpose of documenting and ensuring compliance with the GDPR.
Categories of personal data	The categories of personal data processed include, but are not limited to: name, telephone number, email address, job title, and workplace, as well as username and IP address.
Sensitive data processed	The Customer confirms that special categories of personal data and personal data relating to criminal convictions and offences are not recorded in the Service.
Nature of processing	The processing includes a range of activities that enable the Customer to meet its obligations under the GDPR. These activities include, but are not limited to, maintaining a record of processing activities, recording and managing information related to organisational security, creating and handling data subject access requests, and documenting and following up on personal data breaches. Access to the Service is logged. The Service also supports further processing of personal data through features such as to-do lists and free-text fields, where the Customer can structure its own data protection management. In addition, the processing includes the storage, structuring, and documentation of contact details for data processors, data controllers, and data protection officers, which facilitates administration and communication between relevant parties. There is also an option to receive automatic reminders by email.
Purpose of the processing on behalf of the data controller	To support the Customer in fulfilling its obligations under the GDPR, including documenting processing activities, handling data subject access requests and personal data breach reports, and ongoing monitoring of data protection-related matters. The processing also aims to clarify responsibilities and ensure traceability by documenting contact details for relevant parties. The Service provides the Customer with the tools necessary to systematically ensure GDPR compliance.
Duration of the processing	GDPR Hero will delete the personal data within 180 days after termination of the DPA. The Customer determines the retention period of personal data in the Service using the deletion/removal function.

ANNEX III - Technical and organisational measures

A description of the technical and organisational security measures that the relevant data processor(s) implemented (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purposes of the processing, as well as the risks to the rights and freedoms of natural persons.

- Data in the Service is only accessible through secure authentication.
- The data processor shall ensure that administrative access to the Service and the systems used to provide the Service is only possible from trusted devices and requires the use of multi-factor authentication (MFA).
- Backups are performed daily and retained for 7 days.
- Backup restoration logs are maintained.
- All personnel and sub-processors are subject to confidentiality obligations under binding confidentiality agreements.
- Changes to documentation in the Service are logged.
- Information is protected at rest through encryption.
- Intrusion Detection System (IDS): Implementation of an intrusion detection system that monitors and alerts potential security incidents.
- 24/7 monitoring: Continuous monitoring to detect and respond to threats in real time.
- Controlled physical access: Physical access to systems is restricted and logged using card-based controls.
- 24/7 CCTV monitoring: Continuous video surveillance to ensure physical protection of the facilities.
- Secured server environments: Servers are housed in separate, protected environments with electronic ID scanners to restrict access to authorised personnel.

*****

ANNEX IV - List of approved sub-processors

The data controller has authorised the processor to engage the following sub-processors to carry out specific processing activities under this agreement.

COMPANY NAME	COMPANY REGISTRATION NUMBER	DESCRIPTION OF PROCESSING PERFORMED BY THE SUB-PROCESSOR	LOCATION OF PERSONAL DATA PROCESSING
OMMH Scandinavia AB	556720-9092	To develop and maintain the functionality of GDPR Hero App, OMMH Scandinavia acts as a provider of system development services.	Sweden
Qnova Systems AB	556630-9182	To maintain our cloud service, we use Qnova as a provider of hosting and server infrastructure.	Sweden

*****