Data processing agreement

Between the parties:
Vaimero ApS
Central Business Register (CVR) no. 44837498
Vesterbrogade 74, 3. sal
DK-1620 Copenhagen V
(hereinafter referred to as “Vaimero” or “Data Processor”)
&
Customer name
Reg. no.
Address
Country and city
(hereinafter referred to as “Customer” or “Data Controller”)

Vaimero and the Customer (individually referred to as a “party” and jointly as the “parties”) have entered into this Data processing agreement (hereinafter referred to as the “Data Processing Agreement”).

A. Background and purpose

a. The Data Controller and the Data Processor have entered into an agreement on Vaimero’s standard terms for the delivery of digital services (hereinafter referred to as the “Agreement”).

b. Under the Agreement, the Data Processor must process personal data on behalf of the Data Controller in connection with the delivery of the Platform(s).

c. This Data Processing Agreement (hereinafter referred to as the “Data Processing Agreement”) lays down terms and conditions for the Data Processor’s processing of the personal data (as defined in the Legislation, see clause A.d.) which the Data Controller, under the Agreement, transfers to the Data Processor when using the Platform(s) (hereinafter referred to as the “personal data”). In the event of discrepancies between the Agreement and the Data Processing Agreement, the Data Processing Agreement prevails. Unless otherwise expressly stated in the Data Processing Agreement, the provisions of the Agreement apply.

d. The purpose of the Data Processing Agreement is to ensure compliance of the personal data legislation in force from time to time, including the 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, and repealing

Directive 95/46/EC (“GDPR”), which entered into force on 25 May 2018 (hereinafter jointly referred to as the “Legislation”).

e. There are three appendices to this agreement. The appendices are an integral part of the Data Processing Agreement.

f. Appendix A of the Data Processing Agreement contains detailed information about the processing, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing based on which Platform is used.

g. Appendix B to the Data Processing Agreement contains the Data Controller’s conditions for the Data Processor’s use of sub-processors, and a link to the list of any sub-processors that the Data Controller has approved, depending on which Platform is used.

h. Appendix C to the Data Processing Agreement contains further instructions as to which processing the Data Processor shall perform on behalf of the Data Controller, which security measures which must be observed as a minimum and how the Data Processor and any sub-processors used are supervised, based on which Platform is used.

i. The Data Processing Agreement with attached appendices are stored in writing, including electronically by both parties.

j. This Data Processing Agreement does not release the Data Processor or the Data Controller for obligations under the General Data Protection Regulation or any other legislation directly imposed on the Data Processor and/or the Data Controller.

B. Types of personal data and the data processor’s general obligations

a. The types of personal data and categories of data subjects that the Data Processor must process for the Data Controller as part of the performance of the Agreement and the Data Processing Agreement are specified in Appendix A.

b. It is only the Data Controller that makes the decision which personal data will be processed by the Data Processor, and for which purposes this personal data may be processed. The Data Controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

c. The Data Processor only processes the personal data according to documented instructions from the Data Controller. If, contrary to the Data Controller's instructions, the Data Processor is obliged to perform processing of personal data under the Legislation to which the Data Processor is subject, the Data Processor must inform the Data Controller of this demand before processing, unless the said regulation prohibits such information on important grounds of public interest.

d. The Data Processor must process the personal data in compliance with applicable Legislation. The Data Controller must ensure that all personal data which the Data Controller transfers to the Data Processor, is made via functions in the Platform(s) and is not sent via an unsafe email or in other ways contrary to the Legislation.

e. In case the Danish Data Protection Authority makes inquiries regarding the processing of the personal data, the Data Controller and the Data Processor must cooperate on the reply to questions, disclosure of information or performance of any requests.

C. List of processing activities

a. The Data Processor must keep a list of all categories of processing made by the Data Processor on behalf of the Data Controller. The list, which is kept electronically and contains the relevant information as specified in Article 30 of the GDPR.

b. On request from the Data Controller or the Danish Data Protection Authority, the Data Processor must make available the list to the Data Controller and/or the Danish Data Protection Authority.

D. The data processor's use of subprocessors

a. The Data Controller hereby gives general consent that the Data Processor may use processors ("sub-processors") to perform the Data Processor's services under the Agreement. It is the Data Processor's responsibility that any sub-processors comply with their data protection obligations under the Legislation.

b. The full list of sub-processors which are applicable for the Data Controller's use of the Platform(s) is available at the subprocessors page. The Data Processor informs the Data Controller of any planned changes in the use of sub-processors, including addition or replacement of sub-processors and use of new sub-processors not listed on the subprocessors page . Such notification must be given to the Data Controller as soon as possible. The Data Controller has the option of objecting to such changes within fourteen (14) days of the notification.

c. If the Data Controller cannot accept the changes in the Data Processor's appointment of a subprocessor on reasonable grounds relating to the protection of the Personal Data, then either the Data Processor will not appoint the subprocessor or the Data Processor may elect to suspend or terminate this agreement. Notwithstanding the provision in clause 3.3 of the Agreement, the Agreement automatically ceases with the termination of the Data Processing Agreement. Payments made by the Data Controller are not refunded.

d. Any transfer of personal data to third countries or international organizations may only be made by the Data Processor on the basis of documented instructions from the Data Controller, and must always be made in compliance with chapter V of the General Data Protection Regulation. The current permitted sub-processors are listed on the subprocessors page.

e. The Data Processor ensures that the necessary measures which regulate the transfer of personal data to unsafe third countries exist, including the implementation of the European Commission's Standard Contractual Clauses in force from time to time, or a sub-processor agreement with implemented Binding Corporate Rules.

f. If a sub-processor is established in a third country outside the EU/EEA, it rests with the Data Processor to ensure that the personal data is kept inside the EU/EEA and is not transferred to the said third country unless transfer is necessary to comply with applicable legislation applying to the Data Processor or its sub-processors, or as a result of requirements from a competent public authority that are binding on the Data Processor or its sub-processors. The Data Processor will always make an effort to object to such demands or requests if it will entail that transfer of personal data kept in the Platform(s) to unsafe third countries takes place. The Data Processor must give the Data Controller reasonable notice if such demands are made to the Data Processor or its sub-processors, and must strive to give the Data Controller the possibility to object or use relevant remedies unless the Data Processor or its sub-processors are prevented from this under applicable legislation.

g. The Data Processor makes a qualified effort that personal data is not transferred to third countries by the Data Controller's use of the Data Processor's Platform, whether or not such transfer is made for technical or commercial reasons.

h. When the Data Processor has obtained the Data Controller's approval to use a sub-processor, the Data Processor ensures to impose on the sub-processor the same data protection obligations as those determined in this Data Processing Agreement, through an agreement or other legal document under EU law or the national law of the member states, whereby in particular the required guarantees are made that the sub-processor will implement appropriate technical and organizational measures in such a way that the processing complies with the requirements of the General Data Processing Regulation.

i. Thus, the Data Processor is responsible – via the entering into a sub-processing agreement – for imposing on any sub-processor at least the obligations to which the Data Processor is subject according to the data protection rules.

E. Storage and deletion

a. The personal data is retained until deleted by the Data Controller, or until the Customer relationship ceases, after which the Data Processor will delete the data within ninety (90) days after the Data Controller requests the Data Processor to delete the information, unless national or EU regulations impose on the Data Processor a longer retention period.

b. On cessation of the Data Processing Agreement, irrespective of the reason, the provisions in clauses 3.6 to 3.8. of the Agreement apply.

c. On cessation of the Data processing Agreement, the Data Processor must delete all existing personal data in the Platform(s) unless EU law or national law prescribes retention of the personal data.

d. The Customer’s data is kept in the Platform(s) until either the Customer itself deletes it or requests Vaimero to delete it.

F. Requirements for information security and data protection

a. The Data Processor must make the required technical and organizational security measures against the personal data being accidentally or unlawfully destroyed, lost or impaired and against it becoming known to third parties, is abused or otherwise is processed contrary to the Legislation.

G. Security events

a. The Data Processor must establish and implement procedures for the handling of personal data breaches, see the General Data Protection Regulation, article 4(12) and article 33(2).

b. The Data Processor must without undue delay, after having become aware thereof, inform the Data Controller in writing of a personal data breach, including information on who has processed the Data Controller’s information and when for the purpose that the Data Controller has the option to make police investigation into the breach.

c. In the event of a personal data breach, the Data Processor must, without undue delay, but no later than thirty-six (36) hours after the Data Processor has become aware of the personal data breach, inform the Data Controller thereof in writing to the effect that the Data Controller has the option to comply with its potential obligation to report the breach to the supervisory authority within seventy-two (72) hours and as a minimum state the following:

i. a description of the nature of the personal data breach, including – where possible – the categories and the approximate number of affected data subjects, and the categories and the approximate number of affected registrations of personal data
ii. a description of the likely consequences of the personal data breach
iii. a description of the measures that the Data Processor has made or suggests be made to handle the personal data breach, including measures to mitigate potential adverse effects
iv. Name and contact information of the Data Protection Officer, if such has been appointed by the Data Processor, or other contact point where further information can be obtained.
v. When, and if it is not possible to provide the information in one process, the information may be given in steps without further undue delay.

d. The Data Processor's notifications to the Data Controller about a personal data breach under clause G does not entail that the Data Processor has accepted being in breach of the Agreement or being liable for damages to the Data Controller for the said personal data breach.

H. The data processor's obligation to assist the data controller

a. The Data Processor must, taking into consideration the nature of the processing and the personal data which is processed by the Data Processor, assist the Data Controller with ensuring compliance with the legislative provisions on the right of the data subject as regards personal data. The Data Processor must also, by means of appropriate technical and organizational measures, assist the Data Controller with the handling of inquiries from a data subject, including, but not limited to, request for access, rectification, blocking or erasure of personal data. To the extent that the Data Controller can itself handle inquiries from a data subject via functions in the Platform(s), the Data Controller must use these.

b. Further, taking into account the nature of the processing and the personal data that is processed by the Data Processor, the Data Processor must assist the Data Controller to comply with other obligations resting with the Data Controller under the legislation where this is assumed or necessary for the Data Controller being able to comply with its obligations. As part thereof, the Data Processor must assist the Data Controller with securing compliance of i.a. the obligations under articles 32-36 of the GDPR.

I. Audit and audit opinion

a. At the request of the Data Controller, the Data Processor must give the Data Controller such information necessary for that party to ensure that the Data Processor and its sub-processors comply with the requirements as determined in the Data Processing Agreement, including that they have taken the required technical and organizational security measures and that the measures are complied with.

b. The Data Controller may, through an auditor or other trusted party that has been approved by the Data Controller and the Data Processor, control (within usual business hours) that the Data Processor complies with its obligations.

c. The Data Processor fulfills this right to audit by providing the Data Controller access to the audit opinion ISAE 3000, relevant ISO certificates, and/or other similar certifications/audit reports, on an annual basis. The opinion/certificate will be provided upon request, no later than 31 March of the following calendar year and at no additional cost to the Data Controller.

d. The Data Controller is also entitled, at its own expense, to have an independent third party approved by both the Data Processor and the Data Controller, make an annual audit of the Data Processor's processing of personal data. This annual audit must be made within usual business hours and may not disturb the daily workflow with the Data Processor.

e. The Data Processor is obliged to give authorities which according to the legislation applicable from time to time have access to the facilities of the Data Controller and the Data Processor, or representatives who act on behalf of the authority, access to the physical facilities of the Data Processor against prior signing of a non-disclosure Agreement.

J. The data controller's obligations and liability

a. It is the responsibility of the Data Controller to ensure that the required basis under the legislation for processing of personal data exists, and in the processing of the personal data, the Data Controller must comply with and meet the Legislation.

b. The Data Controller must comply with the security measures applicable from time to time that the Data Processor may inform the Data Controller of regarding access to and use of the Platform(s).

c. The Data Controller must indemnify the Data Processor for the institution of legal proceedings, claims, costs (including reasonable expenses for lawyer assistance), losses,

liability, expenses or damage as a result of the Data Controller's non-compliance with the legislation or the security measures stated by the Data Processor concerning access to or use of the Platform, or other misuse of this Data Processing Agreement.

K. Costs and payment

a. The Data Processor may request payment for services delivered by the Data Processor to the Data Controller under this Data Processing Agreement if it has been agreed between the parties in advance.

L. Amendments to the data processing agreement

a. The parties may, at reasonable prior written notice, decide upon other clauses concerning the provision of the personal data processing, as long as they do not contradict directly or indirectly with the Agreements between the parties or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

b. If a material change or adjustment of the Data Processing Agreement is made under clause L.a. to the detriment of the Data Processor, the Data Processor may terminate the Data Processing Agreement at three (3) months' notice to the end of a month, notwithstanding clause 3.3. of the Agreement. Payments made by the Customer are not refunded.

M. Breach

a. If the Data Processor receives notification from the Data Controller or the Data Processor becomes aware of non-compliance with requests according to the legislation or the Data Controller's instructions for processing personal data, the Data Processor must without undue delay remedy the non-compliance.

b. The provisions of clause 18 of the Agreement apply in the event of a party's breach of the Data Processing Agreement.

c. Neither Party is liable for financial or non-financial claims, including, but not limited to; fines, claims for damages from third parties, etc., which are directed against the other party, in addition to the limitations of clause 10.2-10.5 of the Agreement.

N. Non-disclosure agreement

a. The Data Processor ensures that its employees who are given access to information from the Data Controller have signed a non-disclosure agreement to the effect that they have a duty of non-disclosure to third parties as regards their access to the Data Controller's data. The duty of non-disclosure applies both during employment and after cessation of employment.

b. The Data Processor must ensure that sub-processors, employees and others assisting the Data Processor in connection with the performance of the Agreement and the Data Processing Agreement are subject to obligations that correspond to the obligations therein.

Appendix A – Information about the processing

Types of personal data and documents

A.1 The processing includes the following types of personal data about the data subjects:

May include all types of personal data so that the Platform(s) can function under clause 2 of the Agreement. This personal data may include all types of personal data that can be processed by the Data Controller under the parties' Agreement on the Data Processor's delivery of the Platform(s), to the Data Controller. This information may include, but is not limited to:

- Names
- Email address
- Telephone number
- Information on the Data Controller's employees'/ users'/ clients'/ customers' use of the system, including information about events, times, unique session IDs, IP addresses, browser information, geographical location, user-selected language preference
- Usage Metadata

A.2 The purpose of the Data Processor's processing of personal data on behalf of the data controller is:

The purpose of the processing in the Vaimero Platform is to agree on a meeting date between Clients and the Data Controller, and thus to perform the Agreement between the Data Controller and the Data Processor.

A.3 The Data Processor's processing of personal data on behalf of the Data Controller is primarily about (the nature of the processing):

The Data Processor makes available the Data Processor's standard SaaS Platform(s), to the Data Controller and thus processes and retains personal data about the Data Controller, the Data Controller's Customer, Clients and other affiliates as instructed by the Data Controller.

A.4 The processing includes the following categories of data subjects:

a. Persons which are current clients of, or have previously been clients of, or have been identified as potential clients (leads) by the Data Controller. Persons which are affiliated with the Data Controller.
b. Persons that may be considered third parties, see clause 11 of the Agreement.

A.5 The Data Processor's processing of personal data on behalf of the Data Controller can be commenced once the Agreement has entered into force. The processing is of the following duration:

The Data Processor sets up means for the Data Controller to automatically delete personal data on an ongoing basis in the Platform(s).

The processing of personal data which is not deleted by the Data Controller will be processed until:

a. Ninety (90) days after the Agreement is terminated or canceled by one of the parties.
b. Until the relevant third party deletes the personal data from their own personal archive.

Appendix B – Conditions for the data processor's use of sub-processors and a list of approved sub-processors

B.1 Conditions and approval for the Data Processor's use of any sub-processors

The Data Processor has the Data Controller's general approval to use sub-processors. On commencement of the Data Processing Agreement, the Data Controller has specifically approved the use of the listed sub-processors. See the list of approved sub-processors on the subprocessors page.

B.2 Notification of planned changes of sub-processors

The Data Processor must inform the Data Controller of any planned changes concerning addition or replacement of other sub-processors and thus give the Data Controller a possibility of objecting to such changes. If the Data Controller has any objections against the changes, the Data Controller must inform the Data Processor within fourteen (14) days after receipt of the notification. The Data Controller may only object if the Data Controller has reasonable, concrete reasons to do so.

Appendix C – Instructions on the processing of personal data

C.1 The subject of the processing/instructions

The Data Processor's processing of personal data on behalf of the Data Controller takes place by the Data Processor's performance of the following:

- Collection, registration, systemisation, storage, use, adaptation/change, disclosure, blocking, deletion, handling etc. of the personal data which the data controller enters and processes by means of the Data Processor's standard SaaS software systems (the Platforms).

C.2 Security of processing

The security level reflects the processing of a large quantity of personal data, for which reason a "high" security level must be established.

Accordingly, the Data Processor is entitled and obliged to make decisions on which technical and organizational security measures should be used to create the necessary (and agreed) security level as regards the information.

The technical and organizational security measures must ensure confidentiality, integrity and accessibility to the data controller's data and compliance with the principles of the General Data Processing Regulation.

In any event, and as a minimum, the Data Processor ensures that the following security measures have been implemented:

Cryptography

The Data Processor has ensured that personal data which is processed in the Data Processor's standard SaaS software system, is encrypted to the extent possible, so that it can only be accessed by use of the Data Controller's passwords which are unknown to the Data Processor. Contact information is further processed in an unencrypted way to the extent necessary for the Data Processor to get in contact with persons. Names, relations to companies and other persons and information about persons' use of parts of the SaaS software system are stored in a way in which both the Data Controller and the Data Processor may access them. All personal data is transmitted in encrypted form from the Data Processor's systems to the end user. The

Data Processor ensures that personal data that is processed in the Data Processor's standard SaaS software system, to the extent possible, is encrypted both "in transit" and "at rest".

Access rights and confidentiality

The Data Processor ensures that the employees' access rights follow the principles "least privilege" and "need to know". The Data Processor ensures that access rights to the production environment of the Platforms are evaluated at least once a year.

Operational security

The Data Processor ensures that logically separated environments are used for development, test and production and that change procedures include roll-back strategies. In addition, the Data Processor has implemented network segmentation.

The Data Processor ensures that backup copies of the data of the Customers of the data controller are stored so that lost data can be restored to the extent possible. All personal data is, however, only stored in accordance with the Data Processor's retention and erasure procedure as prescribed in the Data Processing Agreement and clause C3.

C.3 Retention period/deletion routines

The personal data is stored with the Data Processor until the Data Controller requests to have the information deleted or returned. On termination of the Agreement relationship, information that is kept in the Platform(s) in the form of documents and forms, will be deleted within ninety (90) days unless otherwise agreed with the data controller.

C.4 Location of processing

Processing of the personal data included in the Agreement is made i.a. at the following locations:

- Vesterbrogade 74, 3th floor, 1620 Copenhagen V,
- The locations listed in Appendix B
- The Data Processor's employees' addresses via remote work

C.5 Instructions or approval concerning transfer of personal data to third countries

The Data Controller has given general consent that the Data Processor and its sub-processors may transfer personal data to third countries to the extent that the European Commission has determined that the said third country, area of a third country, a sector in a third country or an international organization located in a third country is secure, and thus has a level of protection that materially corresponds to the protection level applicable to the EU. It further means that the Data Controller has also approved that the Data Processor or its sub-processors may transfer personal data to organizations in third countries that are subject to EU's Standard Contractual Clauses (SCC).

If in this section or by subsequent written notification, the Data Controller has not given instructions or approval concerning the transfer of personal data to a third country, the Data Processor may not make such transfer within the framework of the Data Processing Agreement.

C.6 Further procedures for the Data Controller's supervision of the processing being made with the Data Processor

The Data Controller may, once a year through an auditor or other trusted party that has been approved by the data controller and the Data Processor, control (within usual business hours) that the Data Processor complies with its obligations.

In addition to this potential annual inspection, supervision can be made of the Data Processor when in the Data Controller's reasonable assessment a need for this arises.

Any costs of the Data Controller in connection with a physical inspection are paid by the data controller. However, the Data Processor is obliged to allocate the resources (mainly time) required in order that the Data Controller may carry out its supervision.

C.7 Further procedures for the Data Controller's supervision of the processing being made with any sub-processors

The Data Processor or any representative of the Data Processor may once a year carry out physical inspection concerning the compliance with this Data Processing Agreement with the sub-processor.

In addition to this annual inspection, supervision can be made of the sub-processor when in the Data Processor's (or the Data Controller's) reasonable assessment a need for this arises. Documentation of the inspections made is sent for information to the Data Controller as soon as possible.

The Data Controller may – if it is found necessary – choose to initiate and participate in a physical inspection with the sub-processor. However, this may only become an issue if the Data Controller documents that the Data Processor's supervision of the sub-processor has not provided sufficient security for the Data Controller that the processing with the Data Processor is made in compliance with this Data Processing Agreement.

Any costs of the Data Processor and the sub-processor in connection with the performance of a physical supervision/inspection with the sub-processor, shall not concern the Data Controller.

Version 1.0.1. – Updated 19. February, 2025