Data Processing Agreement applicable to IntraManager A/S's customers and other partners, where IntraManager A/S can be considered as the Data Processor

Companies that have a:

Cooperation / customer contract

(Hereafter the "Data Manager")

and

IntraManager A/S

VAT: 33966458

Fjordsgade 11, 1.

5000 Odense C Denmark

(Hereafter the "Data Processor")

2 Background of the Data Processing Agreement

1. This agreement establishes the rights and obligations that apply when the data processor processes personal data on behalf of the data controller.

2. The agreement is designed for the parties to comply with Article 28, pc. 3 in the Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of individuals regarding the processing of personal data and the free movement of such information and repealing Directive 95/46 / EC (the Data Protection Regulation), which sets specific requirements for the content of a Data Processing Agreement.

3. The data processor's processing of personal data is done in order to fulfill the parties' general agreement.

4. The Data Processing Agreement and the general agreement are interdependent and cannot be terminated separately. However, without the termination of the general agreement, the Data Processing Agreement can be replaced by another valid Data Processing Agreement.

5. This Data Processing Agreement takes precedence over any similar provisions in other agreements between the parties, including in the general agreement.

6. There are four annexes to this agreement. The annexes serve as an integral part of the Data Processing Agreement.

7. Annex A of the Data Processing Agreement contains details on 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.

8. Annex B of the Data Processing Agreement contains the data controller's conditions for the data processors use of any sub-processors, as well as a list of any subprocessors that have been approved by the data controller.

9. Annex C of the Data Processing Agreement provides a detailed instruction on what processing the data processor must perform on behalf of the data controller (the subject of the processing), what minimum security measures to observe, and how to monitor the data processor and any sub-processors.

10. The Data Processing Agreement and its annexes are kept in writing, including electronically, by both parties.

11. This Data Processing Agreement does not exempt the data processor from any obligations directly imposed on the data processor under the Data Protection Regulation or any other legislation.

3 Obligations and rights of the data controller

1. As a rule, the data controller is responsible to the outside world (including the data subject) for the processing of personal data within the framework of the Data Protection Regulation and the Data Protection Act.

2. Therefore, the data controller has both the rights and the obligations to make decisions as to what purposes and with which aids the processing must be done.

3. The data controller is responsible, among other things, for the legal basis for the processing that the data processor is instructed to perform.

4 The data processor acts according to instructions

1. The data processor may only process personal data in accordance with documented instructions of the data controller, unless required by EU or national law to which the data processor is subjected; in such case, the data processor shall inform the data controller of this legal requirement prior to processing, unless the court concerned prohibits such notification for the sake of important societal interests, cf. Article 28, pc. 3, point a.

2. The data processor shall immediately inform the data controller if, in the opinion of the data processor, an instruction is in contravention of the Data Protection Regulation or data protection provisions of other EU or national law.

5 Confidence

1. The data processor ensures that only the persons currently authorized to do so have access to the personal data processed on behalf of the data controller. Access to the information must therefore be closed immediately if the authorization is canceled or expires.

2. Only persons for whom it is necessary to have access to the personal data must be authorized in order to fulfill the data processor's obligations to the data controller

3. The data processor ensures that the persons authorized to process personal data on behalf of the data controller have undertaken confidentiality or are subject to an appropriate statutory duty of confidentiality.

4. The data processor must be able to demonstrate, at the request of the data controller, that the relevant employees are subject to confidentiality.

6 Security of processing

1. The data processor shall take all measures required by Article 32 of the Data Protection Regulation, of which it appears that, taking into account the current level, the implementation costs and the nature, scope, context and purpose of the processing in question and the risks of varying probability and severity of the rights and freedoms of natural persons that there must be implemented appropriate technical and organizational measures to ensure a level of security appropriate to these risks.

2. The above obligation entails that the data processor must carry out a risk assessment and then implement measures to address identified risks. Among other things, the following measures may be taken, if they are appropriate:

a. Encryption of personal data

b. Ability to ensure persistent confidentiality, integrity, availability and robustness of processing service systems and services

c. Ability to timely restore availability and access to personal data in the event of a physical or technical incident

d. A procedure for regular testing, assessment and evaluation of the effectiveness of technical and organizational measures to ensure secure processing

3. In relation to the above, the data processor shall, as a minimum, implement at least the level of security and the measures specified in Annex C of this agreement.

4. Any regulation / agreement of the parties on remuneration or similar in connection with the subsequent claims of the data controller or data processor whether the establishment of additional security measures will be stated in the parties' general agreement or in Annex D.

7 Use of sub-processors

1. The data processor must comply with the conditions referred to in Article 28 (pc. 2 and 4) of the Data Protection Regulation in order to use another data processor (subprocessor).

2. The detailed conditions for the data processor's use of any sub-processors are set out in Annex B.

3. Once the data processor has informed the controller to use a sub-processor and updated Annex B, the data processor has provided the sub-processor with the same data protection obligations as those set out in this Data Processing Agreement, through a contract or other legal document under EU or national law, providing in particular the necessary guarantees,

that the sub-processor will implement the appropriate technical and organizational measures in such a way that the processing meets the requirements of the Data Protection Regulation. The data processor is thus responsible to - through the conclusion of a sub-processor agreement - impose at least those obligations on any sub-processor that the processor itself is subject to under the data protection rules and this Data Processor Agreement and its annexes.

4. The Sub-Processor Agreement and any subsequent changes thereto will be sent - at the request of the data controller - in copy or as a link to the data controller, who thereby has the opportunity to ensure that a valid agreement has been concluded between the data processor and the sub-processor. Any commercial terms, such as prices that do not affect the data protection content of the Sub-Processor Agreement, should not be sent to the data controller.

5. In its agreement with the sub-processor, the data processor must include that in the event of the data processor's bankruptcy, the sub-processor will be instructed to delete or return information to the data controller.

6. If the sub-processor fails to meet its data protection obligations, the data processor remains fully responsible to the data controller for the fulfillment of the subprocessor's obligations.

8 Transmission of information to third countries or international organizations

1. The data processor may only process personal data following documented instructions from the data controller, including as regards to the transfer (availability, transmission and internal use) of personal data to third countries or international organizations, unless required by EU law or the national law of the Member States to which the data processor is subject; in this case, the data processor shall inform the data controller of this legal requirement prior to processing, unless the court concerned prohibits such notification for the sake of important societal interests, cf. Article 28, pc. 3, point a.

2. Without the data controller's instructions or approval, the data processor - within the framework of the Data Processing Agreement – can therefore not - among other things -

a. disclose the personal data to a data controller in a third country or in an international organization,

b. entrust the processing of personal data to a sub-processor in a third country,

c. have the information processed in another of the data processing departments located in a third country.

3. The data controller's possible instructions or approval for the transfer of personal data to a third country will be set out in Annex C in this agreement.

9 Assistance to the data controller

1. The data processor shall, considering the nature of the processing, assist the data controller, as far as possible, by means of appropriate technical and organizational measures in compliance with the obligation of the data controller to respond to requests for the exercise of the data subjects' rights that are set out in chapter 3 of the Data Protection Regulation.

This means that, as far as possible, the data processor must assist the data controller in ensuring that the data controller ensures compliance with:

a. the obligation to provide information when collecting personal data from the data subject

b. the obligation to provide information if personal data have not been collected from the data subject

c. the data subjects right of access

d. the right to rectification

e. the right to erasure ("the right to be forgotten")

f. the right to restrict the processing g. notification obligation in connection with rectification or deletion of personal data or limitation of processing

h. the right to data portability

i. the right to object

j. the right to object to the outcome of automatic individual decisions, including profiling

2. The data processor assists the data controller to ensure compliance with the data controller's obligations under Articles 32 to 36 of the Data Protection Regulation, considering the nature of the processing and the information available to the data processor, cf. Article 28, pc. 3, point f.

This means that, regarding the nature of the processing, the data processor must assist the data controller in ensuring that the data controller must ensure compliance with:

a. the obligation to take appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with processing

b. the obligation to report breaches of personal data security to the supervisory authority (the Data Inspectorate) without undue delay and, if possible, within 72 hours after the data controller has become aware of the breach, unless the breach of personal data security is unlikely to involve a risk to the rights and freedoms of natural persons.

c. the obligation - without undue delay - to notify the data subject of the breach of personal data security, when such breach is likely to involve a high risk to the rights and freedoms of natural persons

d. the obligation to conduct an impact assessment on data protection if a type of processing is likely to involve a high risk to the rights and freedoms of natural persons

e. the obligation to consult the supervisory authority (Data Inspectorate) before processing, if an impact assessment on data protection shows that the processing will lead to high risk in the absence of measures taken by the data controller to limit the risk

3. The parties' possible regulation/agreement on remuneration or the like in connection with the data processor's assistance to the data controller will be stated in the parties' general agreement or in Annex D of this agreement.

10 Notification of personal data breach

1. The data processor notifies the data controller without undue delay after becoming aware that the data processor's personal data have been breached or any subprocesser has been breached. If possible, the data processor's notification to the data controller must be made within 48 hours of being informed of the breach, so the data controller has the opportunity to fulfill his possible obligation to report the breach to the regulator within 72 hours.

2. In accordance with Section 10.2, point b of this agreement, the data processor - considering the nature of the processing and the information available to it - shall assist the data controller in reporting the breach to the regulator.

This means that the data processor, among other things, shall help to provide the following information which, in accordance with Article 33, pc. 3 of the Data Protection Regulation, shall be stated in the data controller's notification to the supervisory authority:

a. the nature of the breach of personal data security, including, where possible, the categories and the approximate number of data subjects affected, as well as the categories and the approximate number of personal data records concerned

b. likely consequences of the breach of personal data security

c. measures taken or proposed to deal with the breach of personal data security, including, where appropriate, measures to mitigate its potential adverse effects

11 Deletion and return of information

1. Upon termination of the processing services, the data processor is obliged, at the discretion of the data controller, to delete or return all personal data to the data controller, and to delete existing copies, unless EU or national law provides the storage of personal data.

12 The parties' agreements on other matters

1. Any (special) regulation of the consequences of the parties' breach of the Data Processing Agreement will be stated in the parties' general agreement.

2. Any adjustment of other relationships between the parties will be stated in the parties' general agreement.

13 Entry into force and termination

1. This agreement comes into force upon both parties signing the general agreement and where no other DPA has been entered.

2. The agreement may be required to be renegotiated by either party if legislative changes or inconsistencies in the agreement give rise to this.

3. The parties 'possible regulation / agreement on remuneration, conditions or similar in connection with amendments to this agreement will be stated in the parties' general agreement or in Annex D.

4. Termination of the Data Processing Agreement can be done according to the termination terms, incl. notice of termination, as stated in the general agreement.

5. The agreement is valid if the processing is in progress. Notwithstanding the termination of the general agreement and / or the Data Processing Agreement, the Data Processing Agreement will remain in effect until the termination of the processing and the deletion of the information by the data processor and any subprocessors.

14 Contacts / contact points of the data controller and data processor

1. The parties may contact each other via the following contacts / contact points, as mentioned in the general agreement between the parties.

2. The parties are obliged to continuously inform each other of any changes regarding the contact person / contact point.

15 Signature

On behalf of the data processor:

Odense, November 5, 2021

Lars Klausen

CEO

Annex A: Information about the processing

The purpose of the data processor's processing of personal data on behalf of the data controller is:

That the data controller can use the "IntraManager" system, which is owned and managed by the data processor, to collect and process information about the data controller's customers and / or members.

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 the system "IntraManager" available to the data controller and thereby stores personal data about the data controller's members and/or on the company's servers.

The processing includes the following types of personal data about the data subjects:
Name, email address, telephone number, address, social security number, payment information, membership and / or customer number, type of membership / purchase / subscription

The processing includes the following categories of data subjects:
Persons who have or have had a membership and/or customer relationship with the data controller. The data processor's processing of personal data on behalf of the data controller may commence after the entry into force of this agreement.

The processing has the following duration:
The processing is not limited in time and will last until the agreement is terminated or terminated by one of the parties.

Annex B: Conditions for the data processor's use of sub-processors and list of approved sub-processors

B.1.: Conditions for the data processor's use of any sub-processors: The data processor has the general authorization of the data controller to make use of subprocessors.

However, the data processor must notify the data controller of any planned changes regarding the addition or replacement of other data processors, thereby allowing the data controller to object to such changes.
Such notification must reach the data controller at least 2 months before the application or change is to take effect. If the data controller objects to the changes, the data controller must notify the data processor within 14 days of receipt of the notification. The data controller can only object if the data controller has reasonable, concrete reasons for this.

B.2.: Approved sub-processors At the entry into force of the Data Processing Agreement, the data controller has approved the use of the following sub-processors:

Company	Amazon Web Services EMEA SARL (AWS Europe)
Registration number	352 2789 0057
Adress	38 Avenue John F. Kennedy L-1855 Luxembourg
Processing	Datacenter hosting of servers

Company	OVH Ireland
Registration number	468585
Adress	The Courtyard Building Carmanhall Road Sandyford Dublin 18 Ireland
Processing	Datacenter hosting of servers

Company	inMobile ApS
Registration number	31426472
Adress	Axel Kiers Vej 18 L 8270 Højbjerg Denmark
Processing	SMS Gateway

Company	Hubspot Ireland Limited
Registration number	IE515723
Adress	One Dockland Central Guild Street 1 662880 Dublin Ireland
Processing	Support tickets
Special circumstances	Hubspot has committed itself to complying with the EU Data Regulation by preparing a DPA (https://legal.hubspot.com/dpa).

Company	Microsoft Ireland Operations Ltd.
Registration number	IE8256796U
Adress	One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521 Irland
Processing	Email, Web meetings, Documents etc.
Special circumstances	Microsoft has committed itself to complying with the EU Data Regulation by preparing a DPA ((MicrosoftOnlineServicesDPA) that applies to all customers in the EU.

Company	CPR-Administrationen
Registration number	DK29136815
Adress	Holmens Kanal 22 1060 Copenhagen K Denmark
Processing	CPR lockup

At the entry into force of the Data Processing Agreement, the data controller has specifically approved the use of the above-mentioned sub-processors for precisely the processing described next to the party. The data processor cannot - without the specific and written approval of the data controller - use the individual sub-processor for a "different" processing than agreed or allow another sub-processor to perform the described processing.

Annex C Instructions regarding the processing of personal data

C.1.: The subject / instruction of the processing The data processor's processing of personal data on behalf of the data controller takes place by the data processor performing the following:

C.1.1: Personal information
The data processor stores the data controller’s information via the system "IntraManager". This includes names, addresses, social security numbers, payroll information, etc. The information is used to manage the staff.

C.1.2: Customer information
The data processor can store parts of the data controller's customer information via the system "IntraManager". This includes names, addresses, social security numbers, and so on. The information is used for management and statistics of the customers.

C.2.: Security of processing The level of security must reflect the processing of a large amount of personal data covered by Article 9 of the Data Protection Regulation on "special categories of personal data", which is why a "high" level of security must be established.

The data processor is then justified and obliged to make decisions about the technical and organizational security measures to be used to create the necessary (and agreed upon) level of security around the information.
However, the data processor must - in all cases and at least - implement the following measures agreed with the data controller (based on the risk assessment carried out by the data controller):

- Hashing of all passwords so that these cannot be decrypted and used elsewhere. If a password is to be validated, a comparison of the two hash values must take place
- Encryption of all personal data before storing it
- Only send data on encrypted connections
- Close all unnecessary server access

C.3: Storage Period / routine erasure
The personal data is stored with the data processor until the data controller requests that the data be erased or returned.

C.4: Location of processing The personal data covered by the agreement cannot be processed without the prior written consent of the data controller at sites other than the following:

- AWS Europe's Data Centers located in Ireland
- OVH, Route de la Ferme Masson, 59820 Gravelines, France
- OVH, 9 Rue du Bassin de l'Industrie, 67000 Strasbourg, France
- The data processor's offices (always), as long as they meet the access security requirements

C.5.: Instruction or approval regarding the transfer of personal data to third countries The data processor must never transfer to a third country, implied a country outside the EU or the EEA, unless instructed to do so by the data controller.

C.6.: Detailed procedures for the data controller's supervision of the processing performed at the data processor The data controller or a representative of the data controller can conduct an annual audit of compliance with this Data Processing Agreement with the data processor. In addition to the possible supervision, the data processor can be monitored when a need arises in the opinion of the data controller.

C.7.: Detailed procedures for the supervision of the processing performed by any subprocessors The data processor or a representative of the data processor has the option of conducting an annual audit of compliance with this Data Processing Agreement with the sub-processor.

In addition to the possible oversight, the sub-processor can be monitored when, in the opinion of the data processor (or the data controller), a need arises.
Documentation of the audits held is sent as soon as possible for information to the data controller. Any expenses incurred by the data controller and sub-processor in connection with a physical supervision / inspection at the sub-processor shall be the responsibility of the data controller - except if the data controller has initiated and possibly participated in such supervision.