Data processing agreement

Standard contractual provisions

under article 28(3) of the Regulation 2016/679 (The General Data Protection Regulation) for the purpose of the data processors processing of personal data

between

Name	AIAmigo ApS
Address	Gartnervej 130
	9200 Aalborg SV
CVR/VAT	DK45670260
Name	Jan Thomsen
Title	Direktør
Phone	42303980
E-mail	jan@aiamigo.io

hereinafter referred to as the "data processor"

Kunde

hereinafter referred to as the "data controller"

each a "party" and jointly the "parties"

Have agreed the following standard contractual provisions (the "Provisions") for the purpose of complying with the General Data Protection Regulation and ensure protection of privacy and the basic rights and freedom rights of natural persons

Contents

2. Preamble

1. These Provisions lay out the data processor's rights and obligations when the data processor processes personal data on behalf of the data controller.
2. These Provisions have been prepared for the purpose of the parties' observance of article 28(3) of 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 (General Data Protection Regulation).
3. In connection with the delivery of the services agreed in appendix D, the data processor processes personal data on behalf of the data controller in compliance with these Provisions.
4. The Provisions supersede in relation to any similar provisions in other agreements between the parties.
5. These Provisions include four appendices, and the appendices form an integral part of the Provisions.
6. Appendix A contains detailed information about the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing.
7. Appendix B contains the data controller's terms for the data processor's use of sub-processors and a list of sub-processors which the data controller has approved the use of.
8. Appendix C contains the data controller's instructions as regards the data processor's processing of personal data, a description of the security measures which the data processor must implement as a minimum, and how the data processor and any sub-processors are monitored.
9. Appendix D contains the parties' "master agreement", including instructions and terms of delivery.
10. The Provisions with attaching appendices must be stored in writing, including electronically, by both parties.
11. These Provisions do not release the data processor of obligations that the data processor is subject to under the General Data Protection Regulation and any other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data is made in compliance with the General Data Protection Regulation (see article 24 of the regulation), data protection provisions in other Union law or the national law of the EEA member states and these Provisions
2. The data controller has a right and a duty to make decisions as regards for which purpose(s) and by which means processing of personal data may take place.
3. The data controller is responsible for ensuring, among other things, that there is a basis for the processing of personal data, the use of which the data processor receives instructions.

4. The data processor acts according to instructions

1. The data processor may only process personal data according to documented instructions from the data controller, unless required under Union law or the national law of member

states to which the data processor is subject. All of these instructions must be specified in appendix A, C and D. Subsequent instructions may also be given by the data controller, while processing of personal data takes place, but the instructions must always be documented and stored in writing, including electronically, together with these Provisions.

2. The data processor must inform the data controller immediately if in the data processor's opinion any instructions are contrary to this Regulation or data protection provisions in other Union law or the national law of the member states.

5. Confidentiality

1. The data processor may only grant access to personal data which is processed on behalf of the data controller to persons, who are subject to the data processor's powers of direction, who have undertaken a duty of confidentiality or are subject to an appropriate mandatory duty of confidentiality and only to the extent necessary. The list of persons who have been granted access must be reviewed on an ongoing basis. Based on this review, the access to personal data may be closed if the access is no longer necessary, and the personal data must then no longer be accessible to these persons.
2. At the request of the data controller, the data processor must be able to demonstrate that the said persons who are subject to the data processor's powers of direction, are subject to the above duty of confidentiality.

6. Security of processing

1. Article 32 of the General Data Protection Regulation sets out that the data controller and the data processor, with due regard to the state of the art, costs of the implementation and the nature, scope, context and propose of the said processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller will implement appropriate technical and organisational measures to ensure a protection level commensurate with these risks.

   The data controller must assess the risks of the natural persons' rights and freedoms that the processing constitutes and implement measures to address these risks. Depending on their relevance, it may include:

   a. Pseudonymisation and encryption of personal data
   b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. According to article 32 of the Regulation, the data processor must - independently of the data controller - also assess the risks of the natural persons' rights that the processing constitutes and implement measures to address these risks. For the purpose of this assessment, the data controller must make available the necessary information to the data processor which enables the data processor to identify and assess such risks.
3. In addition, the data processor must assist the data controller with its compliance of the data controller's obligations under article 32 of the Regulation, by i.a. making the necessary

information available to the data controller concerning the technical and organisational security measures that the data processor has already implemented under article 32 of the Regulation, and all other information required for the data controller's compliance with its obligation under article 32 of the Regulation.

If - in the assessment of the data controller - the addressing of the identified risks requires implementation of additional measures than the measures already implemented by the data processor, the data controller must state the additional measures that must be implemented, in appendix C.

7. Use of sub-processors

1. The data processor must comply with the conditions that are referred to in article 28(2) and (4) of the General Data Protection Regulation, to make use of another data processor (a sub-processor).
2. Thus, the data processor may not use a sub-processor to meet these Provisions without prior general written approval from the data controller.
3. The data processor has the data controller's general approval to use sub-processors. The data processor must inform the data controller in writing of any planned changes concerning addition or replacement of sub-processors giving at least 45 days' prior written notice and thus give the data controller the possibility of objecting to such changes before the use of the said sub-processor(s). The list of sub-processors already approved by the data controller appears from appendix B.
4. When the data processor uses a sub-processor in connection with the performance of specific processing activities on behalf of the data controller, the data processor must, via a contract or other legal document under the Union law or the national law of the member states, impose on the sub-processor the same data protection obligations as those specified in these Provisions, whereby in particular the required warranties are made that the sub-processor will implement the technical and organisational measures in such a way that the processing complies with the requirements in these Provisions and the General Data Protection Regulation.

   The data processor is therefore responsible for demanding that as a minimum the sub-processor complies with the data processor's obligations under these Provisions and the General Data Protection Regulation.

5. Sub-processing agreement(s) and any later amendments are sent, at the data controller's request to that effect, in copy to the data controller who thus has the possibility of ensuring that similar data protection obligations that follow from these Provisions have been imposed on the sub-processor. Provisions about commercial terms which do not impact the data protection law contents of the sub-processing agreement, should not be sent to the data controller.
6. In its agreement with the sub-processor, the data processor must include the data controller as a beneficiary third party in case of the data processor's bankruptcy, so that the data controller can adopt the data processor's rights and rely on them to sub-processors which e.g. enables the data controller to instruct the sub-processor in erasing or returning the personal data.
7. If the sub-processor fails to fulfil its data protection obligations, the data processor remains fully liable to the data controller for the compliance of the sub-processor's obligations. This will not affect the rights of data subjects which follow from the General Data Protection

Regulation, in particular articles 79 and 82 of the Regulation, vis-à-vis the data controller and the data processor, including the sub-processor.

8. Transfer of information to third countries or international organisations

1. Any transfer of personal data to third parties or international organisations may only be made by the data processor on the basis of documented instructions to that effect from the data controller, and must always be made in compliance with chapter V of the General Data Protection Regulation.
2. If transfer of personal data to third countries or international organisations that the data processor has not been instructed to make by the data controller, is required according to Union law or the national law of the member states to which the data processor is subject, the data processor must inform the data controller of this legal requirement before processing unless the said legislation prohibits such notification for the purpose of important grounds of public interest.
3. Without documented instructions from the data controller, the data processor thus cannot, within the framework of these Provisions:
    a. transfer personal data to a data controller or a data processor in a third country or an international organisation
    b. entrust a sub-processor in a third country with processing personal data
    c. process the personal data in a third country
4. The data controller's instructions concerning transfer of personal data to a third country, including any transfer basis in chapter V of the General Data Protection Regulation, on which the transfer is based, must be specified in appendix C.6.
5. These Provisions should not be confused with the standard contractual clauses mentioned in article 46(2) point (c) and (d) of the General Data Protection Regulation, and these Provisions cannot form a basis for transfer of personal data as mentioned in chapter V of the General Data Protection Regulation.

9. Assistance to the data controller

1. Taking into consideration the nature of the processing, the data processor will assist the data controller to the extent possible by means of appropriate technical and organisational measures to fulfil the data controller's obligations to reply to requests for exercise of the rights of the data subjects as stipulated in chapter III of the General Data Protection Regulation.

    This entails that to the extent possible the data processor must assist the data controller in connection with the data controller's ensuring compliance with:

    a. the information to be provided where personal data is collected from the data subject
    b. the information to be provided where personal data has not been collected from the data subject
    c. the right of insight
    d. the right to rectification
    e. the right to erasure ("the right to be forgotten")
    f. the right to restriction of processing

g. the notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision which is solely based on automatic processing, including profiling

2. In addition to the data processor's obligation to assist the data controller under Provision 6.4, the data processor, taking into account the nature of the processing and the information that is available to the data processor, also assists the data controller with:
    a. the data controller's obligation, without undue delay and where possible no later than 72 hours after having been made aware thereof, to report personal data breaches to the Danish Data Protection Authority at this link https://indberet.virk.dk/myndigheder/stat/ERST/Indberetning_af_brud_paa_sikkerhed, unless it is unlikely that the personal data breach entails a risk to the rights or freedoms of natural persons.
    b. the data controller's obligation, without undue delay, to notify the data subject of the personal data breach, when the breach is likely to entail a high risk of the rights and freedoms of natural persons
    c. the data controller's obligation, prior to the processing, to make an analysis of the consequences of the intended processing activities for protection of personal data (an impact assessment)
    d. the data controller's obligation to consult the Danish Data Protection Agency, before processing, if an impact assessment concerning data protection shows that the processing will lead to a high risk in the absence of measures implemented by the data controller to limit the risk.
3. In appendix C, the parties must set out the required technical and organisational measures with which the data processor must assist the data controller and to which extent. It applies to the obligations that follow from Provisions 9.1 and 9.2.

10. Communication of a personal data breach

1. The data processor must notify, without undue delay, the data controller after becoming aware of a personal data breach.
2. The data processor's notification to the data controller must, where possible, be made no later than 24 hours after having become aware of the breach, so that the data controller can comply with its obligation to report the personal data breach to the Danish Data Protection Agency within 72 hours, see article 33 of the General Data Protection Regulation.
3. In compliance with Provision 9.2.a, the data processor must assist the data controller with reporting the breach to the competent supervisory authority. This means that the data processor must assist in providing the information below, which according to article 33(3) must be specified in the data controller's reporting of the breach to the competent supervisory authority:
    a. 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
    b. the likely consequences of the personal data breach
    c. the measures made by the data controller or suggested to be made to handle the personal data breach, including where relevant, measures to mitigate potential adverse effects.

4. In appendix D, the parties must state the information which the data processor must obtain in connection with its assistance to the data controller with the controller's obligation to report personal data breaches to the competent supervisory authority.

11. Erasure and return of information

1. On expiry of the services concerning processing of personal data, the data processor is obliged to erase all personal data which has been processed on behalf of the data controller and confirm to the data controller that the information has been erased, unless the Union law or the national law of the member states prescribes storage of the personal data.

   The data processor undertakes to only process the personal data for the purpose(s), in the period and under the conditions that these rules prescribe.

12. Review, including inspection

1. The data processor makes available all information required to prove compliance with article 28 of the General Data Protection Regulation and these Provisions to the data controller and provides the possibility of and contributes to reviews, including inspections which are made by the data controller or another auditor authorised by the data controller.
2. The procedures for the reviews of the data controller, including inspections, with the data processor and sub-processors are specified in Appendix C.7 and C.8.
3. The data processor is obliged to give supervisory authorities which according to applicable law have access to the facilities of the data controller or the data processor, or representatives who act on behalf of the supervisory authority, access to the physical facilities of the data processor against appropriate identification.

13. The parties' agreements on other matters

1. The parties may agree on other provisions concerning the service and processing of personal data about e.g. liability in damages as long as these other provisions are not directly or indirectly contrary to the Provisions or impedes the basic rights and freedoms of the data subject that follow from the General Data Protection Regulation.

14. Commencement and expiry

1. The Provisions enter into force on the date of both parties' acceptance.
2. Both parties may require that the Provisions be re-negotiated if law amendments or inappropriateness of the Provisions give rise to that.
3. The Provisions are valid for as long as the service concerning processing of personal data lasts. In this period, the Provisions cannot be terminated unless other provisions regulating the delivery of the service concerning processing of personal data are agreed between the parties.
4. If the delivery of the services concerning processing of personal data ceases, and the personal data has been erased or returned to the data controller in compliance with the Provisions 11.1 and Appendix C.4, the Provisions can be terminated at written notice by both parties.

Appendix A. Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller

Category of data subject	Purpose
Customers	To manage customer users and their access to the AIAmigo platform. To process and organize the information registered by the customer within the system. To support the functions and workflows used by the customer within the platform. To provide support, maintenance, and ensure the stable operation of the service.

A.2. The data processor's processing of personal data on behalf of the data controller is primarily about the services (nature of the processing) described in Appendix D or the master agreement

A.3. The processing includes the following types of personal data about the data subjects

General personal data (such as name, address, email, telephone number etc.).

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

Category of data subject	Description
Customers	Customers and authorized users of the AIAmigo platform.

A.5. The data processor's processing of personal data on behalf of the data controller can be commenced once these Provisions have entered into force. The processing has the duration specified in Appendix D or the master agreement

Appendix B. Sub-processors

B.1. Approved sub-processors

Supplier	Country	Legal basis for processing outside the EU	Function
Supabase Pte. Ltd.	Singapore	SCC (Standard Contractual Clauses) *Supplier's sub-processors:* SCC (Standard Contractual Clauses)	Database – storage of application data. Server location: Paris (AWS eu-west-3)
Netlify Inc.	United States	EU-U.S. Data Privacy Framework *Supplier's sub-processors:* EU-U.S. Data Privacy Framework	Frontend hosting and CDN. The provider is incorporated in the United States.

On commencement of the Provision, the data controller has approved the use of the above sub-processors for the described processing activity. The data processor may not - without the data controller's written approval - make use of a sub-processor for another processing activity than the one described or agreed, or use another sub-processor for this processing activity.

Appendix C. Instructions concerning 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 is made by the data processor of the processing described in the master agreement/contract or in Appendix D

C.2. Security of processing

Technical Security Measures

All communication between the client and the server is secured using TLS-encrypted connections.

Access to the platform requires authentication and, where enabled, supports two-factor authentication (2FA).

Passwords are stored as secure hash values and cannot be recovered in plain text.

Personal data is encrypted at rest in the database.

Regular backups and logging are performed to ensure data integrity and recovery.

Access to personal data is role-based and restricted to authorized personnel with a legitimate business need.

Development, testing, and production environments are separated.

Organizational Security Measures

All employees are trained in the handling of personal data and are bound by confidentiality obligations.

Management is responsible for information security and compliance with applicable data protection legislation.

Personal data is treated confidentially and is only accessible to authorized personnel.

User access rights are reviewed regularly and revoked when no longer required.

Operational Security

Development, testing, and production environments are kept separate.

Operating systems, applications, and dependencies are updated regularly with relevant security patches.

Administrative accounts are protected by strong passwords and, where possible, two-factor authentication.

Login attempts and security-related events are logged for troubleshooting and security monitoring purposes.

Administrative endpoints are protected by up-to-date antivirus software and firewalls.

Note

AIAmigo processes only the personal data necessary to provide the agreed services to the customer.

AIAmigo does not maintain physical archives containing personal data.

Personal data is processed and stored in accordance with the data controller's instructions and the approved sub-processors.

C.3. Assistance to the data controller

To the extent possible, the data processor must assist the data controller in compliance with the Provisions 9.1 and 9.2 by implementing the technical and organisational measures specified in Appendix C.2.

C.4. Storage period/deletion routines

Personal data is kept with the data processor until the data controller requests to have the data erased or returned, unless otherwise agreed in Appendix D/the master agreement.

On expiry of the service concerning processing of personal data, the data processor must either erase or surrender the personal data in compliance with provision 11.1, unless the data controller has changed its initial choice, after having signed these Provisions. Such changes must be documented and be stored in writing, including electronically, in connection with the Provisions.

C.5. Place of processing

Processing of the personal data included in the Provisions cannot take place without the data controller's prior written approval in other places than the premises of the data processor or sub-processor.

C.6. Instructions concerning transfer of personal data to third countries

The data processor does not transfer personal data to third countries unless to the generally approved sub-processors listed in Appendix B.

If the data controller fails in these Provisions or subsequently to give documented instructions about transfer of personal data to a third country, the data processor is not entitled to make such transfers within the framework of these Provisions.

C.7. Procedures for the data controller's reviews, including inspections, of the processing of personal data which has been left to the data processor

The data processor shall, upon request, make available the information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and this Data Processing Agreement.

The data controller may, once per year or where there are reasonable grounds to suspect non-compliance, request documentation of the data processor's technical and organizational security measures.

If the documentation provided is not considered sufficient, the data controller may, by prior written agreement, carry out an audit or inspection of the data processor.

Any audit or inspection shall:

be notified in writing at least 30 days in advance,

be carried out during normal business hours,

take reasonable account of the data processor's operations and the security and confidentiality of other customers,

be limited to matters relevant to the processing of personal data carried out on behalf of the data controller.

The data controller shall bear its own costs in connection with any audit or inspection. The data processor shall make available the resources reasonably required to facilitate the audit. If an audit identifies material non-compliance with this Data Processing Agreement or applicable data protection legislation, the data processor shall bear its own costs of remedying the identified deficiencies.

C.8. Procedures for reviews, including inspections, of the processing of personal data which has been left to sub-processors

The data processor shall ensure that all approved sub-processors are contractually required to implement appropriate technical and organizational security measures in accordance with Article 28 of the General Data Protection Regulation.

The data processor shall monitor its sub-processors on an ongoing basis by obtaining and reviewing relevant documentation, including data processing agreements, security statements, certifications, or other documentation demonstrating compliance with applicable data protection and security requirements, where relevant.

Upon request, the data controller may be provided with the documentation that the data processor is legally permitted to disclose regarding the sub-processors' compliance with their data protection obligations.

Appendix D. The parties' regulation of other matters, including instructions concerning the processing of personal data

This Data Processing Agreement forms part of the agreement between the parties regarding the provision of the AIAmigo software platform (SaaS).

The data processor shall process personal data only on documented instructions from the data controller and only to the extent necessary to provide the agreed services.

The data processor may only:

process personal data for the purpose of providing, operating, maintaining, and supporting the platform,

process personal data in accordance with this Data Processing Agreement and the documented instructions of the data controller,

use the approved sub-processors listed in Appendix B.

Personal Data Breaches

In the event of a personal data breach, the data processor shall notify the data controller without undue delay and provide the information reasonably required by the data controller, including:

a description of the nature of the breach,

the categories of personal data affected, where known,

the likely consequences of the breach,

the measures taken or planned to contain and remediate the breach.