Data processor agreement

Engelske kunder
Engelske kunder
Engelske kunder Engelske kunder
United Kingdom
Company registration no.: 00000000
(the "**Data Controller**")

ziik.io (Chainintra ApS)
Nørre Voldgade 18, 1.
1358 København K
Danmark
Company registration no.: 36553081
(the "**Data Processor**")

Date: 5/24/2018 12:29:40 PM

1. Introduction

1.1 This agreement concerning processing of personal data (the "**Data Processor Agreement**") regulates the Data Processor's processing of personal data on behalf of the Data Controller and is attached as an appendix to the Cooperation Agreement (cloud based social intranet), for date, see signed contract (the "**Main Agreement**"), in which the parties have agreed on the terms for the Data Processor's delivery of services to the Data Controller (the "**Main Services**").

1.2 If there are discrepancies between the rights and obligations under the Main Agreement and the Data Processor Agreement, the rights and obligations under the Data Processor Agreement shall prevail.

2. Legislation

2.1 The Data Processor Agreement shall ensure that the Data Processor complies with the applicable data protection and privacy legislation (the "**Applicable Law**"), including in particular:

2.2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as transposed into Danish law with, among others, the Act on Processing of Personal Data (act no. 429 of 31 May 2000).

2.3 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 (General Data Protection Regulation) which entered into force on 25 May 2016 and will apply from 25 May 2018 ("**GDPR**").

3. Processing of personal data

3.1 In connection with the Data Processor's delivery of the Main Services to the Data Controller, the Data Processor will process certain categories and types of personal data on behalf of the Data Controller.

3.2 "Personal data" means "*any information relating to an identified or identifiable natural person*" as defined in GDPR, article 4(1) that is processed under this Data Processor Agreement (the "**Personal Data**"). The categories and types of Personal Data, categories of data subjects, the purposes of the processing and the processing activities performed by the Data Processor as well as the processing locations are listed in **Sub-Appendix A**. The parties shall update Sub-Appendix A whenever changes occur that necessitates an update.

3.3 The Data Processor shall have and maintain records of processing activities in accordance with GDPR, article 30(2).

3.4 The Data Processor possibly processes personal data about the Data Controller's employees in connection with the Data Processor's sale, marketing and product development. Such personal data is not comprised by this Data Processor Agreement, because the Data Processor is data controller for said personal data, and reference is made to the Data Processor's data protection and privacy policy available at the Data

Processor's website.

4. Instruction

4.1 The Data Processor shall only act and process the Personal Data in accordance with the documented instruction from the Data Controller (the "**Instruction**") unless the Data Processor is subject to EU law or national Member State law under which the Data Processor is obliged to process the Personal Data differently; in such a case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Instruction at the time of entering into this Data Processor Agreement is that the Data Processor may only process and store the Personal Data with the purpose of, and to the extent it is necessary for, provision and delivery of the Main Services as described in the Main Agreement and within the specifications described in Sub-Appendix A.

4.2 The Data Controller shall ensure that the Personal Data made available to the Data Processor is processed in accordance with the Applicable Law, including the legislative requirements of lawfulness of processing and information to be provided to the data subject.

4.3 In the event that the Data Processor does not comply with this Data Processor Agreement, the Data Controller may instruct the Data Processor to stop further processing of the Personal Data with immediate effect.

4.4 The Data Processor shall immediately give notice to the Data Controller if the Data Processor considers the Instruction to conflict with the Applicable Law.

5. The Data Processor's obligations

5.1 Confidentiality

5.1.1 The Data Processor shall process the Personal Data as strictly confidential information. The Personal Data shall not be copied, transferred or otherwise processed except from the Instruction, unless the Data Controller in writing has agreed hereto.

5.1.2 The Data Processor's employees that process the Personal Data shall be subject to an obligation of confidentiality that ensures that the employees shall treat the Personal Data with strict confidentiality.

5.2 Security

5.2.1 The Data Processor shall implement the appropriate technical and organisational security measures as set out in the Data Processor Agreement and in the Applicable Law, including in accordance with GDPR, article 32.

5.2.2 The Data Processor's security measures are further described in **Sub-Appendix B**. .

5.2.3 The Data Processor shall provide documentation for the Data Processor's security measures if requested by the Data Controller in writing.

5.3 Data protection impact assessments and prior consultation

5.3.1 If the Data Processor's assistance is necessary and relevant, the Data Processor shall assist the Data Controller in preparing data protection impact assessments in accordance with GDPR, article 35, along with any prior consultation in accordance with GDPR, article 36.

5.4 Rights of the data subjects

5.4.1 If the Data Controller receives a request for the exercise of a data subject's rights under the Applicable Law and the correct and legitimate reply to such a request necessitates the Data Processor's assistance, the Data Processor shall assist the Data Controller by providing the necessary information and documentation.

5.4.2 If the Data Controller requests the assistance of the Data Processor to respond to a data subject request, the Data Controller shall request so in writing and the Data Processor shall answer such a request with the relevant and necessary information and documentation no later than 7 calendar days after receipt of a request.

5.4.3 If the Data Processor receives a request directly from a data subject for the exercise of a data subjects rights under the Applicable Law and such request is related to the Personal Data, the Data Processor shall immediately forward the request to the Data Controller and must refrain from responding to the person directly.

5.5 Personal Data Breaches

5.5.1 The Data Processor shall give notice to the Data Controller if a personal data breach occurs, that can lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the Personal Data (a "**Personal Data Breach**"). The Data Processor shall notify the Data Controller of a Personal Data Breach immediately and no later than 24 hours after being aware of the Personal Data Breach.

5.5.2 The Data Processor shall have and maintain records of all Personal Data Breaches. The records shall at a minimum include the following for each Personal Data Breach:

5.5.2.1 A description of the nature of the Personal Data Breach, including, if possible, the categories and the approximate number of affected Data Subjects and the categories of affected Personal Data.

5.5.2.2 A description of the likely as well as actually occurred consequences of the Personal Data Breach.

5.5.2.3 A description of the measures that the Data Processor has taken or proposes to take to address the Personal Data Breach, including, where appropriate, measures taken to mitigate its adverse effects.

5.5.3 The records of Personal Data Breaches shall be provided to the Data Controller in copy if so requested in writing by the Data Controller or the supervisory authority.

5.5.4 The Data Processor shall, on request, assist the Data Controller in drafting notification to the supervisory authority and/or the data subjects affected by the Personal Data Breach.

5.6 Documentation of compliance

5.6.1 The Data Processor shall on the Data Controller's written request hereof provide documentation substantiating the following:

5.6.1.1 The Data Processor complies with its obligations under this Data Processor Agreement and the Instruction.

5.6.1.2 The Data Processor complies with the Applicable Law in respect of the processing of the Personal Data.

5.6.2 The Data Processor's documentation in connection with section 5.6.1 shall be provided within reasonable time after the receipt of the request.

5.6.3 The Data Processor is not obligated to undertake an audit of its compliance with the Data Processing Agreement in addition to section 5.6.4.

5.6.4 Notwithstanding section 5.6.3, the Data Processor shall allow for and contribute to audits, inspections, etc., to be conducted by the Data Controller, auditors mandated by the Data controller, or public authorities in Denmark or other competent jurisdictions, insofar such audits, inspections, etc. are necessary to verify the compliance of the Data Processor with this Data Processor Agreement and the Applicable Law. Any auditors performing said audit, inspections, etc. must have undertaken a duty of confidentiality either by written contract or by statutory law. The Data Controller shall notify the Data Processor 14 calendar days before such an audit.

5.7 Location of the Personal Data

5.7.1 The Personal Data shall only be processed by the Data Processor at the locations specified in Sub-Appendix A. The Data Processor shall not transfer the Personal Data to third countries or to international organisations in third countries.

5.7.2 Any transfer of the Personal Data shall only be done in accordance with this Data Processor Agreement, including the Instruction and the Applicable Law.

6. Sub-Processors

6.1 The following shall apply for the Data Processor's engagement of third parties to process the Personal Data ("**Sub-Processors**"): The Data Processor has general authorisation to engage Sub-Processors without further written consent from the Data Controller provided that the Data Processor informs the Data Controller in writing of the identity of the potential Sub-Processor (and of any data processor of the Sub-

Processor) at least 7 calendar days prior to entering into an agreement with the concerned Sub-Processor, thereby giving the Data Controller the opportunity to object to such changes. If the Data Controller has not objected to the named Sub-Processor within 7 calendar days of the Data Processors notification, the non-objection shall be deemed a tacit consent.

6.2 The Data Processor shall conclude a written sub-processor agreement with any Sub-Processor. Such an agreement shall at minimum provide the same data protection obligations as the ones applicable to the Data Processor in accordance with this Data Processor Agreement and the Main Agreement. The Data Processor shall on an ongoing basis monitor and control its Sub-Processors' compliance with such data protection obligations, and the documentation hereof shall be provided to the Data Controller if so requested in writing.

6.3 The Data Processor is accountable to the Data Controller for any Sub-Processor's processing of the Personal Data in the same way as for its own actions and omissions.

6.4 The Data Processor is at the time of entering into this Data Processor Agreement using the Sub-Processors listed in **Sub-Appendix C**. If the Data Processor initiates sub-processing with a new Sub-Processor, such new Sub-Processor shall be added to the list in Sub-Appendix C under paragraph 2.

7. Remuneration and costs

7.1 The Data Controller shall pay the Data Processor for time spend in accordance with the Data Processor's applicable hourly rates to comply with the following items in the Data Processing Agreement: 5.3, 5.4, 5.6.1 and 5.6.2, 5.6.4 (the expenses of the data processor in connection with audit), 5.6.3.

7.2 The Data Processor is entitled to payment for the time and materials used to comply with any changes to the Instruction, when those changes are made by the Data Controller. This includes implementation costs and increased costs for delivery of the Main Services.

7.3 Each party shall bear the costs of changes to the Applicable Law, including the interpretations and guidelines hereof.

8. Breach and liability

8.1 The Data Processor is not liable for non-delivery or delay of the Main Services in so as its delivery will be in violation of the modified Instruction or delivery in accordance with the modified Instruction is impossible. This may, for example, be the case, (i) where the modifications cannot be technically, practically or legally implemented, or (ii) where the Data Controller explicitly states that the modifications must apply before implementation is possible.

8.2 Breach and liability shall be governed by the Cooperation Agreement and the Data Processor Agreement, but the liability shall be limited by the payment to the Data Processor for the last 12 months

9. Duration

9.1 The Data Processor Agreement shall remain in force for as long time as the Data Processor processes the Personal Data.

10. Termination

10.1 The Data Processor's authorisation to process Personal Data on behalf of the Data Controller shall expire at the termination of this Data Processor Agreement.

10.2 The Data Processor may continue to process the Personal Data for up to three months after the termination of the Data Processor Agreement to the extent it is necessary and required under the Applicable Law. In the same period, the Data Processor is entitled to include the Personal Data in the Data Processor's backup. The Data Processor's processing of the Data Controller's Personal Data in the three months after the termination of this Data Processor Agreement shall be considered as being in accordance with the Instruction.

10.3 At the termination of this Data Processor Agreement, the Data Processor and its Sub-Processors shall, at the Data Controller's choice, return or delete the Personal Data processed under this Data Processor Agreement, provided that the Data Controller is not already in possession of the Personal Data. At the Data Controllers' written request, the Data Processor shall delete all the Personal Data, except when EU-Member State legislation or national legislation stipulate otherwise. The Data Processor shall provide documentation for such deletion to the Data Controller upon request.

11. Contact

11.1 The contact information for the Data Processor and the Data Controller is provided in the Main Agreement.

12. Accept

12.1 Both parties agree and guarantee that this Data Processor Agreement is entered into and accepted by persons that are authorised and have the necessary mandate to do so.

Sub-Appendix A

1. Personal Data

1.1 The Data Processor processes the following types of Personal Data in connection with its delivery of the Main Services:

Name, telephone number, email, profile picture, Varying personal information that the customer or customers customer issues or registers without the company's active processing and identification thereof, working hours

2. Purpose

2.1 The Data Processor processes Personal Data with the following purposes:

that the Data Controller (Customer) can use Ziik's platform, which is owned and administered by the Data Controller (the Customer), to streamline internal communication and knowledge sharing. Ziik only provides the platform and the Customer owns all data.

3. Data subjects

3.1 The Data Processor processes Personal Data on the following categories of data subjects on behalf of the Data Controller:

customers, employees of the customer, customer's customer and their employees, suppliers (when supplier is an individual or a sole proprietor), Supplier's employees (when supplier is a company), business partner (when business partner is an individual or a sole proprietor), employees of the business partner (when the business partner is a company)

4. Processing activities

4.1 The Data Processor processes the Personal Data by performing the following processing activities:

Delivering the company's service (a cloud based social intranet)

5. Locations

5.1 The Data Processor shall process the Personal Data at the following locations:

Copenhagen, Denmark (Main office)

Sub-Appendix B

1. Introduction

1.1 This description of the technical and organisational security measures (the "Description of Security Measures") is prepared to demonstrate the Data Processor's established security measures, implemented in accordance with GDPR, article 32, or security measures to be established before the processing of the Personal Data.

2. Organisational security

2.1 The Data Processor has implemented the following organisational security measures:

2.1.1
a) All employees of the Data Processor are subject to confidentiality obligations that apply to all processing of Personal Data.
b) The employee access to Personal Data is limited, so that only the relevant employees have access to the necessary Personal Data.
c) The employees of the Data Processor that have access to special categories of personal data or critical IT systems have undergone a security clearance before they were employed.
d) The Data Processor has documentable process descriptions for the processing of Personal Data.
e) The Data Processor has an IT security policy.
f) The Data Processor has established procedures that ensure proper deletion or continuous confidentiality when hardware is repaired, serviced or disposed.

2.1.2 2-factor authentication

3. Technical and logical security

3.1 The Data Processor has implemented the following technical and logic security measures:
a) Logical access control with username and password or other unique authorisation
b) Regular backup
c) Firewall that is updated regularly
d) Antivirus programs that are updated regularly
e) The webistes and web forms of the Data Processor uses SSL Certificates/HTTPS (Hyper Text Transfer Protocol Secure)
f) Logging and checking unauthorised or repeated failed login attempts

4. Physical security

4.1 The Data Processor have implemented the following physical security measures:
a) The Data Processor's devices (including PCs, servers, etc.) are secured behind locked doors
b) Fire alarms and smoke detectors

Sub-Appendix C

1. Approved Sub-Processors

1.1 The following Sub-Processors shall be considered approved by the Data Controller at the time of entering into this Data Processor Agreement on the terms of this Data Processing Agreement and the Applicable Law:

Linode, Servers, disclosure@linode.com
Close.io, CRM tool, support@close.io
E-conomic, Accounting tool, info@e-conomic.dk
Stripe, Billing service, info@stripe.com
Campaign Monitor, Newsletters, support@campaignmonitor.com
Zapier, Integration tool, contact@zapier.com

2. New Sub-Processors

2.1 New Sub-Processors may be used by the Data Processor by adding and updating these in a separate document in continuation of this Sub-Appendix C, which shall be sent for information or approval by the Data Controller before a new Sub-Processor is used.