@ SMTP

DATA PROCESSING AGREEMENT

SMTP.DK

AND

THE COMPANY

@SMTP

Table of Contents

BILAGSOVERSIGT

DEFINITIONS

"the Agreement"   refers to the main agreement that forms the basis for entering into this Data Processing Agreement.

"General Data Protection Regulation"   refers to Directive 95/46/EC of the European Parliament and of the Council, Act 2000-05-31 no. 429 with latest changes and, after 25 May 2018, Regulation *(EU)* 2016/679 in addition to future legislation that regulates the processing of personal data.

"Data Processing Agreement"   refers to this Data Processing Agreement.

SMTP

This agreement has been entered into between

SMTP.dk ApS
Refshalevej 163A
1432 Copenhagen K
(hereinafter referred to as the "Data Processor")

and

The Customer

(hereinafter referred to as the "Data Controller")

(individually "the Party" and together "the Parties")

1.   BACKGROUND AND SCOPE OF THE AGREEMENT

1.1   This agreement is to ensure that the General Data Protection Regulation is complied with. The purpose of the Data Processor processing personal data on behalf of the Data Controller is stated in Appendix 1.

1.2   If there is a discrepancy between the Data Processing Agreement and the Agreement, this Data Processing Agreement shall take precedence unless otherwise stated directly in the Agreement.

1.3   If there are factors in the Data Processing Agreement and the attached instructions that later prove to be invalid or prove to not be in compliance with the General Data Protection Regulation the Parties may, regardless of Section 1.1, state that this is the case. The Data Processing Agreement shall remain valid in areas not impacted by this and the Parties, if necessary, shall immediately begin negotiations aimed at clarifying, supplementing or revising the factors in question.

2.   RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

2.1   The Data Controller is the data controller of the personal data that the Data Processor processes on behalf of the Data Controller.

2.2   The Data Controller is responsible for ensuring that the Data Processor is entitled to process personal data on behalf of the Data Controller, including that this processing is legal. The Data Controller has the rights and obligations granted to a data controller pursuant to the General Data Protection Regulation.

3. OBLIGATIONS OF THE DATA PROCESSOR

3.1 The Data Processor is only responsible for processing personal data on behalf of the Data Controller on the terms outlined in the Data Processing Agreement or if there is documentation of an instruction from the Data Controller, cf. Section 5.

3.2 The Data Processor will assist and aid the Data Controller upon the request of the Data Controller by delivering relevant information and documentation aimed at allowing the Data Controller to document compliance with the Data Controller's legal obligations, including, for example, the right to gain insight into personal data stored and impact assessments, etc. In return for providing such assistance to the Data Controller, in addition to changes and/or expansions of the instructions, the Data Processor may demand remuneration based on time spent and for extra costs. The hourly rates for this are DKK 650 excluding VAT of 25%.

3.3 If a registered individual contacts the Data Processor with the intention of exercising his/her rights under the General Data Protection Regulation, the Data Processor will pass along this request without undue delay for processing. The Data Processor will assist the Data Controller in accordance with Section 3.2.

4. THE DATA PROCESSOR'S USE OF SUBCONTRACTORS

4.1 The Data Processor uses subcontractors (data subprocessors) for the delivery of services in accordance with the Data Processing Agreement. Upon the signing of this agreement, the Data Controller has approved the use of the data subprocessors listed in Appendix 2.

4.2 The Data Controller shall provide the Data Processor with a general approval to use the data subprocessors if the following conditions are met:

- The Data Processor will always inform the Data Controller about any potential scheduled additions or replacements of data subprocessors and will give the Data Controller a reasonable amount of time to object to such changes. The notification must be accompanied by a description containing similar information as Appendix 2 for already approved data subprocessors which will provide the Data Controller with a basis for assessing the issue.
- The use of data subprocessors takes place on the basis of a written agreement entered into between the Data Processor and the data subprocessor that imposes the same obligations on them as the ones applying to the Data Processor pursuant to the Data Processing Agreement, in addition to the General Data Protection Regulation, so that the rights of the registered individuals are upheld. The Data Processor will actively monitor and ensure that the data subprocessor fulfils such obligations.
- The Data Controller may at any time request documentation for the existence of the data subprocessor agreement and its content, except when this relates to issues that are of a confidential commercial nature between the Data Processor and the data subprocessor.

4.3 Unless otherwise separately agreed, all form of communication with the data subprocessor will be managed by the Data Processor. The Data Controller can refuse the use of data sub-

processors if these do not comply with an instruction. In addition, the Data Processor is directly liable for the data subprocessor's processing of the Data Controller's personal data to the same extent as if the processing was undertaken by the Data Processor itself.

4.4   The Data Processor is not currently transferring the Data Controller's personal data to countries outside of the EU/EEA. The Data Processor is, regardless of Section 4.2, not entitled to use subcontractors in unsafe non-member countries without prior written consent from the Data Controller. The use of subcontractors based in unsafe non-member countries must take place in accordance with the General Data Protection Regulation's legitimate reasons for transfers. In its written consent, the Data Controller will in addition take into consideration whether the Data Processor, with written authority, is to ensure that there is signed standard contracts directly between the Data Controller and the data subprocessor or if the Data Controller wishes to undertake this on its own.

5.   INSTRUCTIONS

5.1   The Data Processor only processes personal data pursuant to and in accordance with the Data Controller's instructions in effect at any given time. The instructions from the Data Controller encompass any processing which is necessary for the Data Processor's delivery of services to the Data Controller.

5.2   The Data Processor shall notify the Data Controller if an instruction, in the opinion of the Data Processor, is not in accordance with the General Data Protection Regulation.

5.3   It is not permitted for the Data Processor to refuse to comply with the Data Controller's instructions as a result of missing payments, etc., and the Data Processor has no right of retention or the like when it comes to the Data Controller's personal data.

5.4   The Data Processor can only process personal data outside of the given instructions if it is required by an EU or national court that the Data Processor is subject to. The Data Processor shall notify the Data Controller of the reason for this unless such a notification would be in violation of EU or national law/court order.

6.   TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Data Processor shall, taking into consideration the current technical capabilities, implementation costs and the nature of the processing in question, its scope, content, and purpose, in addition to the likelihood of risks materialising and their impact on the rights of physical individuals and their rights to freedom, implement appropriate technical and organisational measures to, among other things, prevent the occurrence of:

- accidental or illegal destruction, loss, or change

- unauthorised transfer, access or misuse
- other illegal processing, cf. Security Annex attached as Appendix 3

6.1   The Data Processor must be able to demonstrate to the Data Controller that the Data Processor has the necessary technical and organisational security measures in place. The Parties

agree that the guarantees stated in Appendix 3 are sufficient at the moment of entering into this Data Processing Agreement.

6.2   Without undue delay and no later than 24 hours after the Data Processor has become aware of a security breach, the Data Processor shall notify the Data Controller in writing of this. This notification shall, at a minimum, and to the extent possible in light of the nature of the incident, include the following: 1) information on the nature of the found security breach, 2) what categories of registered individuals is affected by it, and 3) an approximate number of the affected registered individuals, including categories of comprehensive personal data and the number of these in addition to what preventive or mitigating measures the Data Processor has implemented as a result of the found security breach.

6.3   Upon written request, the records must be made available to the Data Controller or the supervising authorities.

7.   TRANSFERS TO OTHER COUNTRIES

7.1   Personal data may not be transferred to non-member countries on the basis of the Data Processor's acceptance or consent unless the Data Controller has approved such a transfer. The Data Processor shall beforehand ensure that the transfer of the personal data in question can legally take place in accordance with the provisions of the General Data Protection Regulation.

7.2   If personal data is transferred to an EU member state it is the responsibility of the Data Processor to ensure that the provisions on security measures in effect at any given time and as stated in the legislation of the member state in question are complied with.

8.   DUTY OF CONFIDENTIALITY

8.1   The processing of personal data shall take place under full confidentiality between the Data Processor and the Data Controller. Employees of the Data Processor, third parties (for example repairmen) and also data subprocessors who are working with the processing of personal data under the framework of this Data Processing Agreement shall accept a duty of confidentiality. Only employees of the Data Processor who are authorised to do so may access the personal data that is processed under the Data Processing Agreement. The Data Processor shall ensure that employees who are processing personal data have committed to a duty of non-disclosure or are subject to an appropriate legal confidentiality

8.2   Regardless of Section 13, the provisions on the duty of confidentiality shall have no time limit.

9. CONTROLS AND DECLARATIONS

9.1 The Data Controller is entitled to, at own expense, submit the Data Processor's processing of personal data on behalf of the Data Controller to an inspection and/or audit by an independent third party. The Data Processor is entitled to remuneration for time spent and the costs associated with this. The hourly rate for this is DKK 650 excluding VAT of 25%.

10. CHANGES TO THE DATA PROCESSING AGREEMENT

10.1 If changes to legislation or practice results in changes to the Data Processing Agreement, the Data Controller is entitled to make these changes at no cost with a notice of 7 days.

10.2 If instead the changes are based on the Data Controller's circumstances, including the Data Controller's desire for a personal data protection level that exceeds what is required by law and/or the relevant security-related level, the Data Processor can request remuneration based on time spent and extra costs incurred.

10.3 The Data Processor is to ensure that the data sub processors are obliged to comply with the changes pursuant to Section 10.1 and 10.2 without undue delay.

11. DELETION OR DESTRUCTION OF PERSONAL DATA

11.1 Upon the expiry or termination of the Agreement, this Data Processing Agreement shall also cease to be in effect. The Parties shall agree on the deletion, handing back or destruction of all personal data that is processed by the Data Processor on behalf of the Data Controller. The Data Processor shall furthermore delete all copies of data, including from backups, in accordance with the Data Processor's scheduled and systematic overwriting of backups.

11.2 Regardless of 11.1, the Data Processor is entitled to – at the extent necessary to be able to document delivery of services as per the Agreement or to defend itself against legal claims – save a copy of the Data Controller's personal data. In such a case, the Data Controller's personal data may then only exclusively be processed for those stated purposes and the processing shall cease as soon as these purposes are no longer valid.

11.3 The Data Processor shall also ensure that any potential data sub processors do not process personal data after the cessation of the Agreement unless Section 11.2 is applicable.

12. BREACH OF CONTRACT AND LIABILITY

12.1 The Agreement's provisions on breach of contract and liability also apply to the Data Processing Agreement.

13. COMMENCEMENT AND DURATION

13.1   This data processing agreement shall commence upon the signing of it by both parties and shall continue until the cessation of the Agreement.

13.2   Regardless of 13.1, this Data Processing Agreement shall last as long as the Data Processor is in possession of any of the Data Controller's personal data.

13.3   The Data Controller is entitled to, at own expense and with the assistance of third parties, to ascertain that deletion, etc. has taken place as stated by the Data Processor. The Data Processor is entitled to remuneration for time spend and costs associated with this.

14. APPLICABLE LAW AND JURISDICTION

14.1   The Data Processing Agreement is governed by Danish law.

14.2   It is agreed that all claims and any disputes that may arise from the Data Processing Agreement shall be settled by the Copenhagen District Court.

15. SIGNATURES

15.1   This Data Processing Agreement is signed in writing or electronically and in 2 original copies, one for each of the Parties.

[place, date]:   [place, date]::

Name: Name:

Title:
                                                            Title:

SMTP.dk   Company

SMTP

Appendix 1

The processed information

The personal data that the Data Processor processes on behalf of the Data Controller is related to the categories of personal data that have been handed over by the Data Controller to the Data Processor in the document:

- The object of and duration of the processing
  - The data uploaded by the Data Controller is used for all forms of email communication for third parties. The data is stored in the system for 30 days.
- The nature and purpose of the processing
  - Sending of all the Data Controller's emails for all types of communication that takes place via the Data Processor's sending protocol.
- The type of personal data
  - Common data that the Data Processor shall process on behalf of the Data Controller
    - Email addresses, subject headings and receiver's name
- Categories of registered individuals
  - The sender of emails and the email addresses of these sender's customers
- The physical location (of servers, etc.) where personal data is being processed

  ADEODC Herstedvang 8 1606 2620 Albertslund

SMTP

Appendix 2

Data processing subcontractors

ADEODC Herstedvang 8 1606 2620 Albertslund

- The object of and duration of the processing
  - o Hosting of the email sending system. Live transmission. Emails are stored for 30 days.
- The nature and purpose of the processing
  - o Sending emails
- The type of personal data
  - o Common data that the Data Processor shall process on behalf of the Data Controller
    - ▪ Email addresses, subject headings and receiver's name
- Categories of registered individuals
  - o The sender of emails and the email addresses of these sender's customers

(Full listing data sub processors will show on final DPA)

@ SMTP

Appendix 3

Security annex

- Sensitive data is encrypted in transit via a secure file transfer solution in accordance with industry standards
- The Data Processor makes use of anti-virus programs
- The Data Processor has set up firewalls
- The Data Processor shall secure critical network access points and ensure that systems are tested for weaknesses on an ongoing basis
- All employees of the Data Processor or those who work for the Data Processor have been assigned a unique account that may not be shared, and which must be kept confidential
- All customers will be assigned an automatically generated code when they first log in
- The password configurations are enforced so as to ensure a minimum configuration of:
  - At least 8 characters
  - Must contain 2 numbers
- New users must be authorised for access by users with higher levels of system rights before access is granted to systems
- All access and key events are logged, and these logs are accessible to the Data Processor if necessary
- Remote access takes place via an encrypted connection