data processing agreement

Version 2.0 (2020–10)

1. General

1.1 This Data Processing Agreement forms an integral part of the agreement between the Supplier and the Customer (the "**Agreement**").

1.2 Upon performance of the Agreement, the Supplier will process Personal Data on behalf of the Customer in capacity of the Customer's data processor. The Customer is also acting as a data processor on behalf of its customers (the data controllers) with regard to the Processing of the Personal Data.

1.3 Should the Customer be the data controller for the Personal Data, the Customer will inform the Supplier of this fact.

1.4 The purpose of this Data Processing Agreement is for the Customer and the Supplier to comply with from time to time applicable requirements and obligations under Data Protection Law with regard to data processing agreements and to maintain adequate safeguards in respect of personal integrity and fundamental rights of individuals in relation to transfers of Personal Data from the Customer to the Supplier within the scope of the services performed by the Supplier for the Customer under the Agreement.

2. Definitions

"**Customer**"	means the party defined as the Customer in the above and to the extent that the Customer enters into this Data Processing Agreement on behalf of other service recipients pursuant to the Agreement, where appropriate, such service recipients also unless otherwise is expressly set forth in this Data Processing Agreement.
"**Data Protection Law**"	means the from time to time applicable laws and regulations in respect of Processing of Personal Data, including but not limited to 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 (the "GDPR"), replacing the Swedish Personal Data Act (1998:204), as well as Supervisory Authority's binding decisions, regulations and recommendations and supplementary local adaptions and regulations in respect of data protection.
"Data Subject"	means the natural person to whom Personal Data relates to.
"Personal Data"	means any information that the Supplier is Processing on behalf of the Customer under this Data Processing Agreement, relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
"Subprocessor"	means anyone Processing Personal Data as a subcontractor of the Supplier (including, but not limited to, companies within the Supplier group).
"Supervisory Authority"	means the supervisory authority or supervisory authorities authorised to conduct supervision of Processing of Personal Data or considered to be the supervisory authority concerned under Data Protection Law, for example the Swedish Authority for Privacy Protection (Sw. Integritetsskyddsmyndigheten).

”Supplier”	means the party defined as the Supplier in the above.

2.1 Any other terms or concepts used with a capitalized initial letter in this Data Processing Agreement shall, unless otherwise is expressly stated, have the meaning provided for under Data Protection Law and otherwise under the Agreement, unless the circumstances obviously require another order of interpretation.

3. Responsibility and Instructions

3.1 The Customer shall act on behalf of its customers, the data controllers, with regard to all Personal Data processed by the Supplier on behalf of the Customer under the Agreement. The Customer is therefore responsible for ensuring that the Processing of Personal Data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and this Data Processing Agreement. The Customer has the right and obligation to make decisions about the purposes and means of the Processing of Personal Data. The Customer shall be responsible, among other, for ensuring that the Processing of Personal Data, which the Supplier is instructed to perform, has a legal basis. Further, the Customer is obliged to inform the Supplier of any changes in the business conducted by the Customer causing the Supplier to take any measure or change any routing due to the content in Data Protection Law. The Customer shall also regularly inform the Supplier regarding measures taken by third parties, including Supervisory Authority and Data Subject, relating to the Processing.

3.2 The Supplier and the person(s) working under the Supplier’s supervision, shall only process Personal Data in accordance with the Customer’s documented instructions. The Supplier must never process Personal Data for any other purposes than the purposes the Customer has contracted the Supplier for under the Agreement and as set forth in this Data Processing Agreement. Applicable instructions at the conclusion of this Data Processing Agreement are set out in Appendix 1. In addition to the specific instructions set out in Appendix 1, this Data Processing Agreement and the Agreement shall be deemed as the Customer’s full instructions to the Supplier with regard to Processing of Personal Data. Subsequent instructions can also be given by the Customer throughout the duration of the Processing of Personal Data, but such instructions shall always be documented and kept in writing, including electronically, in connection with this Data Processing Agreement.

3.3 Processing may also be performed where Union or Member State law, to which the Supplier or Subprocessor is subject, requires such Processing. Where Processing is required by Union or Member State law to which the Supplier or Subprocessor is subject, the Supplier or the Subprocessor will inform the Customer of the legal requirement before the Processing, unless that law prohibits such information.

3.4 The Supplier shall immediately inform the Customer if instructions given by the Customer, in the opinion of the Supplier, contravene the GDPR or the applicable Union or Member State data protection provisions.

3.5 For the purpose of clarity the Supplier has the right to, during the term if this Data Processing Agreement and thereafter, store and process data derived from the Customer in aggregated or anonymized form i.e. data that does not contain Personal Data.

4. Security etc.

4.1 Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Customer and Supplier shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The Customer shall evaluate the risks to the rights and freedoms of natural persons inherent in the Processing and implement measures to mitigate those risks.

4.2 According to Article 32 GDPR, the Supplier shall also - independently from the Customer - evaluate the risks to the rights and freedoms of natural persons inherent in the Processing and implement measures to mitigate those risks. Furthermore, the Supplier shall assist the Customer in ensuring compliance with the Customer's obligations pursuant to Articles 32 GDPR, by inter alia providing the Customer with information concerning the technical and organisational measures already implemented by the Supplier pursuant to Article 32 GDPR along with all other information necessary for the Customer to comply with the Customer's obligation under Article 32 GDPR.

If subsequently - in the assessment of the Customer - mitigation of the identified risks require further measures to be implemented by the Supplier, than those already implemented by the Supplier pursuant to Article 32 GDPR, the Customer shall specify these additional measures to be implemented in Appendix 1.

5. Disclosure of Personal Data and Information

5.1 The Supplier shall without delay forward to the Customer any request from a Data Subject, Supervisory Authority or any other third party, regarding disclosure of data that the Supplier processes on behalf of the Customer. The Supplier, or anyone working under the Supplier's supervision, may not disclose Personal Data, or information about the Processing of Personal Data, unless expressly instructed otherwise by the Customer, save where such obligation is provided for under applicable Data Protection Law.

6. Assistance to the Customer

6.1 Taking into account the nature of the Processing, the Supplier shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Customer's obligations to respond to requests for exercising the Data Subject's rights laid down in Chapter III GDPR.

6.2 In addition to the Supplier's obligation to assist the Customer pursuant to Section 4.2, the Supplier shall furthermore, taking into account the nature of the Processing and the information available to the Supplier, assist the Customer in ensuring compliance with:

a) the Customer's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data breach to the competent Supervisory Authority, unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b) the Customer's obligation to without undue delay communicate the Personal Data breach to the Data Subject, when the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c) the Customer's obligation to carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data (a data protection impact assessment);

d) the Customer's obligation to consult the competent Supervisory Authority prior to Processing where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Customer to mitigate the risk.

6.3 The parties shall define in Appendix 1 the appropriate technical and organisational measures by which the Supplier is required to assist the Customer as well as the scope and the extent of the assistance required.

6.4 The Customer shall compensate the Supplier for extra work relating to the Supplier's obligation set forth in this section 6 according to the hourly rate applied by the Supplier from time to time.

7. Notification of Personal Data Breach

7.1 In case of any Personal Data breach, the Supplier shall notify the Customer of the Personal Data breach without undue delay after the Supplier has become aware of the Personal Data breach to enable the Customer to comply with the

Customer's obligation to notify the Personal Data breach to the competent supervisory.

7.2 In accordance with Section 6.2 a), the Supplier shall assist the Customer in notifying the Personal Data breach to the competent Supervisory Authority, meaning that the Supplier is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the Customer's notification to the competent Supervisory Authority:

a) The nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

b) the likely consequences of the Personal Data breach;

c) the measures taken or proposed to be taken by the controller to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8. Subprocessor

8.1 The Supplier shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage a Subprocessor. The Customer hereby grants the Supplier a general authorisation to engage Subprocessors.

8.2 Where the Supplier engages a Subprocessor for carrying out specific Processing activities on behalf of the Customer, the same data protection obligations as set out in the Data Processing Agreement shall be imposed on that Subprocessor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of this Data Processing Agreement and the GDPR.

8.3 The Supplier will inform the Customer of any intended changes concerning the addition or replacement of Subprocessors. The Customer is entitled to object to such changes. Such objections may only be attributable to objective grounds, such as the security of the Processing under the Data Processing Agreement. Should the Customer make such objection and the Supplier does not accept to replace the Subprocessor in question, the Supplier shall be entitled to additional compensation from the Customer for the costs incurred due to the fact that the Subprocessor in question cannot be used by the Supplier. The Supplier also has the right to terminate the Agreement and / or this Data Processing Agreement in whole or in part (e.g. insofar as they pertain to a particular add-on service) with thirty (30) days' prior notice.

8.4 The Supplier shall upon request of the Customer provide the Customer (and if requested, Customer's customers that are controllers) with an accurate and

up-to-date record regarding the Subprocessors engaged by the Supplier for the Processing of Personal Data, contact information to the Subprocessors as well as the geographic location of such Processing.

8.5 A list of the Subprocessors engaged by the Supplier at the date of the Agreement is attached to this Data Processing Agreement as Appendix 2.

9. Audits

9.1 The Supplier shall within reasonable time following the Customer's request to the Supplier thereof make available to the Customer all information necessary to demonstrate that the obligations laid down in Article 28 of the GDPR have been complied with. This means e.g. that the Customer has, in the capacity of controller, the right to take necessary measures to verify that the Supplier can fulfil its obligations under this Data Processing Agreement and that the Supplier actually has taken measures to ensure this.

9.2 The Supplier shall also assist and contribute to audits, including inspections, conducted by the Customer or an independent auditor.

10. Transfers of Personal Data outside the EU/EEA

10.1 The Supplier and Subprocessors may only transfer Personal Data to a location outside of the EU/EEA (a so-called third country) provided that from time to time applicable requirements under Data Protection Law are observed. The Supplier shall upon such transfers to Subprocessors in third countries, on the behalf of the Customer enter into an agreement where the Subprocessor is obliged to apply the EU standard contractual clauses (2010/87/EU) or any standard clauses that replace these following decision by the EU Commission and / or by the CJEU.

10.2 In the event that the EU standard contract clauses (2010/87/EU) or other applicable third country transfer mechanism under the GDPR (whichever used for the transfer) are no longer sufficient to satisfy the requirements of applicable data protection provisions applicable to the Processing of Personal Data under this Data Processing Agreement to legalize the transfer of Personal Data to third countries, the Supplier shall use its reasonable efforts to implement either an alternative transfer mechanism which satisfies the requirements of data protection provisions applicable to the Processing of Personal Data under this Data Processing Agreement – in order to legalize the transfer to third countries – or cease with such transfer.

11. Confidentiality

11.1 The Supplier only grants access to the Personal Data Processed on behalf of the Customer to persons under the Supplier's authority who have committed themselves to confidentiality by contract or are under an appropriate statutory obligation of confidentiality. The duty of confidentiality applies during and after the term of this Data Processing Agreement. Access to Personal Data shall be

limited to such persons requiring the Personal Data in order to conduct their job assignment. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to Personal Data can be withdrawn, if access is no longer necessary, and Personal Data shall consequently not be accessible anymore to those persons.

11.2 The Supplier shall at the request of the Customer demonstrate that the concerned persons under the Supplier's authority are subject to the abovementioned confidentiality.

11.3 The obligation under section 11.1 above does not apply to information that the Supplier is ordered to disclose to an authority according to Data Protection Law or other statutory requirement.

12. Compensation

12.1 The Supplier shall be entitled to full compensation from the Customer for all work and all costs incurred as a consequence of fulfilling section 9, and 15.1 due to instructions on Processing of Personal Data provided by the Customer to the Supplier, which go beyond what is set forth in Appendix 1 or the functions and level of security that the Supplier normally offers its customer, e.g. as regards the Supplier's server services and if the Supplier is required to make customizations specifically for the Customer. The Supplier shall also be entitled to compensation from the Customer for work incurred as a consequence of fulfilling the obligation according to section6. All work for which the Supplier is entitled to compensation according to this section shall be compensated in accordance with the Supplier's hourly rates applicable from time to time. The compensation shall cover the actual cost of the Supplier.

13. Liability

13.1 If the Supplier, anyone working under the Supplier's supervision, or the Supplier's Subprocessor, processes Personal Data in violation of this Data Processing Agreement or contrary to the lawful instructions provided by the Customer, the Supplier shall, taking into account the limitation of liability under the Agreement, compensate the Customer for any direct damage caused by the Supplier due to incorrect Processing, including damages and any administrative fines paid by the Customer to a third party. Without prejudice to the limitation of liability under the Agreement, the Supplier's liability under this section 13.1 shall never exceed an amount equal to the fees paid by the Customer to the Supplier under the Agreement during the twelve (12) months period preceding the event that caused the damage.

13.2 If the Customer or anyone working under the Customer's supervision, or any third party engaged by the Customer cause the Supplier damage due to vague, inadequate or wrongful instructions, inadequate information from the Customer as to the nature of the data processed (e.g. if sensitive Personal Data is processed without the Customer having informed the Supplier thereof) or if the damage is due to a breach of this Data Processing Agreement, the shall

Customer compensate the Supplier for such damage, including damages and any administrative fines paid by the Supplier to a third party.

13.3 The Supplier's liability for claims and damages pursuant to this section 13 is subject to: (i) the Customer informing the Supplier in writing of any claims made against the Customer without undue delay; and ii) the Customer allowing the Supplier to control the defence of the claim and to alone decide on any settlement.

14. Term and Termination

14.1 This Data Processing Agreement enters into force when duly signed by both Parties and remains in force as long as the Supplier processes Personal Data on behalf of the Customer.

14.2 Upon termination of this Data Processing Agreement and subject to section 3.5 above the Supplier shall, as determined by the Customer in its sole discretion, delete or return all the Personal Data to the Customer without undue delay but in any event no later than within ninety (90) days and delete existing copies, unless Union or Member State law requires storage of the Personal Data. Upon request by the Customer, the Supplier shall provide a written notice of the measures taken regarding the Personal Data upon the termination of the Processing of Personal Data.

15. Changes to the Data Processing Agreement

15.1 If Data Protection Law changes during the term of this Data Processing Agreement, or if the Supervisory Authority issues guidelines, decisions or regulations concerning the application of Data Protection Law that result in this Data Processing Agreement no longer meeting the requirements for a data processing agreement pursuant to Data Protection Law, the Parties shall in good faith discuss necessary changes of this Data Processing Agreement in order to meet such new or additional requirements. Such changes shall come into effect in accordance with the Parties' written agreement thereof or otherwise no later than within such time set forth in Data Protection Law or a Supervisory Authority's guidelines, decisions or regulations. The Supplier shall be entitled to reasonable compensation for any work, costs and expenses due to such changes.

15.2 Other changes and addendums to this Data Processing Agreement must be made in writing and duly signed by both Parties in order to be binding.

16. Miscellaneous

16.1 The provisions of the Agreement shall apply also in respect of the Supplier's Processing of Personal Data and the obligations under this Data Processing Agreement. In case of inconsistency between the provisions of the Agreement and this Data Processing Agreement, the provisions of this Data Processing Agreement shall take precedence in relation to all Processing of Personal Data and nothing in the Agreement shall be deemed to limit or change obligations

under this Data Processing Agreement insofar that this would mean that either Party does not comply with the requirements under Data Protection Law.

16.2 Swedish law shall under all circumstances be applied to this Data Processing Agreement.

16.3 Disputes arising in connection with this Data Processing Agreement shall be settled in accordance with the dispute resolution procedure set out in the Agreement.

appendix 1 – processing of personal data

These instructions apply for Processing of Personal Data in accordance with the Data Processing Agreement (DPA). In addition to what already is stated in the DPA, the Supplier should also follow these instructions.

Purpose	The Supplier's Processing of Personal Data is done as the data processor, and with regards to customer data which a customers choose to store within the Customer's services, as the personal data Subprocessor for the purpose of to deliver, develop, manage, debug, maintain and administer the Customer's services to its customers and partners. As the supplier of the hosting service provided to the Customer, the Supplier processes data by hosting, organizing, receiving, forwarding, structuring, implementing, searching, processing, storing, transferring, recovering, deleting, limiting, maintaining, logging, supporting, troubleshooting, and other services related to providing the hosting service, the personal data added by the customer
Categories of personal data	As data processor, the Supplier Process data such as name, e-mail, national identification number, address, telephone number and similar contact information to the Customer's customers. The Supplier also Processes usernames and IP addresses. As a Subprocessor, the Supplier Processes Personal Data such as e-mail and web-data as well as identifiable meta-data such as customer number, technical database identifiers, invoice numbers and other types of specialized local serial numbers. Additional categories may occur depending on what categories of personal data the customers choose to store within the Customer's services (this is then regulated by the Customer as the personal data processor and the customer as the data controller).
Categories of registrants	As a data processor, the Supplier will Process Personal Data for employees, customer contact persons, supplier contact persons and partner contact persons. As a Subprocessor, additional categories may occur depending on what categories of Personal Data the customers choose to store within the Customer's services (this is then regulated by the Customer as the data processor and the customer as the data controller).

Retention	The Supplier (as personal data processor) shall Process Personal Data during the term Agreement (as defined in the Data Processing Agreement). Information stored indirectly on the Supplier's services, such as backups of customer data, logs or similar, are specified on the Supplier's and / or in agreement / terms and are in general stored between 7 days and 3 months depending on service type.
Practical handling	IP addresses and usernames are also Processed in the form of logging, monitoring and backup. If the Customer or any of its customer should order third party services such as domains or SSL-certificates, the required information is sent to third parties. This is also clarified in separate contract terms for domain names. Processing performed by the Supplier as the Subprocessor usually consist of, for example, logging, troubleshooting, monitoring, backup and customer support.

Technical and organizational security measures

Below, some of the actions taken by the Supplier as a data processor to ensure that Personal Data is Processed safely is listed.

Instruction of employees etc.

The Supplier makes sure that the employees and possible business partners at all time are familiar with and has received proper education and instruction about the cause of the data processing, politics, working methods, and about their obligation of professional secrecy.

There should be an information safety policy available that the management has processed and approved within the last year. The information safety policy is communicated to the relevant stakeholders, including the Supplier's employees.

Overall, the information safety policy meets the requirements concerning safety measure and the security of processing according to the data processing agreements.

New employees have signed a confidentiality agreement. New employees have been introduced to:

- The information safety policy
- The procedures concerning data processing and other relevant information

There are procedures available that make sure that the right to access personal data of the Customer of resigned employees are inactivated or ended, and that assets with access to personal data of the Customer are withdrawn.

There are formalised procedures available that make sure the resigned employees are made aware of their obligation to sustain the agreement of confidentiality and the obligations of secrecy. The contract of employment contains guidelines to make sure that the employee is subject to obligations of secrecy after the end of provision.

The supplier provides awareness training for the employees including general it-safety in relation to personal data. It is documented that all employees that either has access to or process personal data has completed the offered awareness training.

Communication links and encryption

The supplier has appropriate technical measures to protect systems and networks, including data protection under transmission and access through the internet and to limit the risk of unauthorized access and/or instalment of damaging code.

The supplier applies appropriate encryption technologies and other equally measures in accordance with the requirements listed in the law, approved standards for encryption of classified information and good data processing practice.

The transmission of sensitive and confidential information through the internet is protected by encryption. Technological solutions are available and archived. Firewall only allow encrypted data traffic. Formalised procedures are available which secure that the transmission of sensitive and confidential information through the internet are protected by a strong encryption based on a recognised algorithm.

Conditional access and administration of user access

Procedures concerning the restriction of user's access to personal data is available. There are formalised procedures for follow-up to make sure that the user's access to personal data is in accordance with their occupational needs. The agreed technical measures support the maintenance of the restrictions in the user's occupational access to personal data. The user's access to systems and databases are restricted to the employees' occupational needs.

There are procedures available for allocation and interruption of the users' access to systems and databases that are used to process personal data. Consistently, assessments and approvals of assigned user access should be made.

A list of authorised employees shall be kept with identification of which type of access the authentication covers. The list of authorised employees needs to be updated on an ongoing basis in regard to good data processing practice.

By the end of the service the employee's access shall be closed.

In addition, the data processor uses secure identification and authentication technologies, for instance, passwords, biometrics, or similar. The authentication mechanisms follow the latest guidelines of good practice in this regard.

Downtime, including operating processes

The supplier needs to have documented emergency procedure that secures the restoration of services without undue delay in case of downtime.

Furthermore, there needs to be operational documentation and operating processes available for all the systems where customer data is processed. This should as a minimum contain:

- Description of installation
- Description of configuration
- Description of backup, job-scheduling
- Description of security configurations and audit/monitoring
- Description of recovery and re-establishment procedures
- Description of procedures for error handling
- Description of operational monitoring
- Description of change management and roll-back plans

Operational documentation and operating processes need to be kept up to date and made accessible for relevant personnel.

Backup

Backup of configuration files and data needs to take place in a continuous process, so relevant data can be re-stored. The backups need to be stored so they are not accidental or illegal (for instance in case of fire, flood, accidents, theft, or similar) destroyed, lost, deteriorates, comes to the knowledge of unauthorised persons, misused or processed in contravention of the existing regulations for treatment of personal data.
The backups need to be physical stored separate from the primary data and in a security approved data centre.

Change management

The supplier has the formal procedure for change management to secure that each change is authorised, tested, and approved before it is implemented. The procedure needs to be supported by an effective separation of the functions and/or management follow-up to make sure, that no individuals can control a change by them self.

Physical and environmental protection

The supplier needs to sustain physical safety measures to secure locations that are used to process personal data, including storage of personal data included by the data processing agreement against unauthorized access and manipulation.

Disposal of equipment

The supplier needs to have formal procedures to secure effective deletion of personal data before disposal of electronic equipment.

Logging

1. Secure logging in all environments where personal data is processed.
2. Secure that the logs as minimum needs to include information about:
    a. All attempts for logs – both if they succeed or not
    b. Time
3. Secure that the logs extent is defined from the supplier's risk assessment
4. Secure that there is enough space for the logs to be saved and stored for the period
5. Weighing up the logs' deadline of deletion between the option to analyse cyber-attacks, support investigation and the consideration to protection of physical persons' rights and freedom.
6. Secure gathered information about user activity in logs and make sure they are protected against deletion and manipulation.

appendix 2 – data processors

As personal data controller for your personal data as a customer, the following providers may be used as data processors for different scenarios.

Provider	Reason	Data	Country	Legal basis
SMTP.dk ApS	SMTP Relay	Name, e-mail, and any info in communication.	DK	Delivery of service according to agreement