Data Processor agreement

Cloudpoint services

Cloudpoint Oy (hereinafter referred to as “Cloudpoint” or “Data Processor”), and

The Customer (hereinafter referred to as the “Customer” or “Data Controller”)

(jointly referred to as the “Parties”)

have on this day entered into this Data Processing Agreement (“DPA”), based on the current legislation (the Finnish Personal Data Act and the European Data Protection Directive 95/46/EC) and the General Data Protection Regulation (EU 2016/679), which is applicable from May 25, 2018.

This DPA is applicable if and to the extent Cloudpoint during its furnishing of the agreed service to the Customer will process data on behalf of the Customer which according to applicable legislation is defined as “Personal Data”.

Background

Data Controller and Data Processor have entered into an agreement regarding services provided by Cloudpoint from time to time (herein referred to as the “Service Agreement”) to which Cloudpoint’s General Terms and Conditions regarding Service and Software apply.

By entering into this DPA, the Parties wish to ensure that adequate safeguards are in place with respect to the protection of the privacy of data subjects for the duration of the Service Agreement.

Definitions

For the purposes of this DPA, terms that are defined in the Finnish Data Personal Data Act, or other applicable legislation, shall have the same meaning given to them therein.

Scope of the DPA

The Data Processor provides the services ordered by the Data Controller from time to time, and may, for the duration of the Service Agreement, process Personal Data on behalf of the Data Controller. The Data Processor’s main establishment and central administration is in Finland.

The service involves storage and transfer of user details and content provided by the user of the services. Such data may directly or indirectly identify a natural person.

The Data Processor will solely process the Personal Data provided by the Data Controller in order to perform its obligations according to the Service Agreement.

The Personal Data that may be processed by the Data Processor on behalf of the Data Controller is irrevocably and automatically deleted upon the termination of the Service Agreement.

The Parties hereby agree that the processing, the categories of personal data, the data subjects or the purposes of processing may at any time and by mutual agreement be clarified with respect to their specification and/or be enlarged with respect to their volume or scope. Any such changes shall be made in writing in due course after receipt of knowledge of such changes. Unless otherwise agreed by the Parties, the terms and conditions as set forth in this DPA shall apply accordingly.

Obligations of the Data Processor

The Data Controller shall have the full power of disposition regarding the personal data.

The Data Processor agrees that it will:

provide the processing of Personal Data solely in accordance with the instructions of the Data Controller for the purpose set forth in the Service Agreement (“Instructions”), according to the rules and the provisions contained in this DPA and in accordance with the applicable data protection law, and

will implement the security measures specified herein

not acquire any rights in or to the personal data,

not use the personal data for any purpose other than for the performance of its obligations under this DPA and the Service Agreement, or for fault localization in the Data Processor’s system,

not process the personal data for its own purposes without the prior written approval of the Data Controller.

Where the Data Processor believes that any Instruction would result in a violation of the applicable data protection law, Data Processor may suspend the execution of the Instruction until their lawfulness is confirmed by an authorized person of the Data Controller or is changed in writing.

The Data Processor will assist the Data Controller to the extent possible for the fulfilment of the Data Controller’s obligations to respond to requests for exercising the data subject’s rights as stated in applicable law.

The Data Processor will, at the choice of the Data Controller, delete or return all Personal Data in physical or electronic form, if technically possible, after the termination of the Service Agreement, unless applicable law requires storage of the Personal Data.

Notification Obligations of the Data Processor

The Data Processor shall promptly notify the Data Controller of any unauthorized access to personal data and/or any accidental or wilful disclosure of personal data to unauthorized third parties it becomes aware of.

The Data Processor shall promptly notify the Data Controller of any material breach of applicable data protection laws in connection with this DPA it becomes aware of.

Obligations of the Data Controller

The Instructions must be in written form (whether physical or electronic).

The Data Controller has the sole obligation to inform data subjects of the processing of their personal data by the Data Processer, and to ensure that the data subject is aware of its rights according to the applicable legislation.

The Data Controller is obligated to in any other manner perform its obligations in accordance with applicable law. Nothing in this DPA shall be construed as a transfer of the Data Controller's obligations stipulated in applicable law, to the Data Processor.

Transfer of Personal Data Outside the EU/EEA

For the purpose of providing the agreed services, the Data Processor's servers are located in [Finland] and in an additional approximately [number] countries worldwide (within and outside the EU/EEA territory).

The Data Controller is aware and accepts that outside the EU/EEA area, the servers are located under co-location agreement with collaborators. Such parties have no right of access to data on the servers, and limited right of physical access to the servers, when the data is transferred between the Data Processor's Servers, the data in encrypted. The servers are remotely or directly operated by the Data Processor.

The Data Controller commits that the data subjects have been informed or will be informed before the processing by the Data Processor that his or her data could be transmitted to a country outside of the EEA.

Audit Rights

Data Processor shall at Data Controller's request allow the data processing facilities of Processor to be audited with regard to the processing activities covered by this Agreement. Processor will cooperate and provide assistance for such audit as may reasonably be required by Controller and the organization carrying out the audit. The Data Controller is aware that for security reasons, there are limitations and regulations concerning whom may enter the premises where the servers are located.

Parties shall mutually agree which organization will carry out the audit.

Data Controller will pay all costs, fees and expenses of the organization carrying out the audit.

Sub-processors

Data Controller acknowledges and agrees that (a) Data Processor's affiliates may be retained as sub-processors; and (b) Data Processor's affiliates respectively may engage third-party sub-processors in connection with the provision of the services. Data Processor has or shall enter into a written agreement with each sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of the Data Controller's Personal Data to the extent applicable to the nature of the services provided by such sub-processor.

Data Processor shall make available to Data Controller the current list of sub-processors for the services provided by Data Processor. Such sub-processor lists shall include the identities of those sub-processors and their country of location. Data Processor shall provide notification of a new sub-processor(s) before authorizing any new sub-processor(s) to process Personal Data in connection with the provision of the applicable services.

Data Controller may object to Data Processor's use of a new sub-processor by notifying Data Processor promptly in writing within ten (10) business days after receipt of Data Processor's notice. In the event Customer objects to a new sub-processor, Data Processor will use reasonable efforts to make available to Data Controller a change in the services or recommend a commercially reasonable change to Data Controllerr's configuration or use of the Services to avoid processing of Personal Data by the objected-to new sub-processor without unreasonably burdening the Data Controller. If Data Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Data Controller may terminate the agreement with respect only to those services which cannot be provided by Data Processor without the use of the objected-to new sub-processor by providing written notice to Data Processor. Data Processor will refund Data Controller any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated services, without imposing a penalty for such termination on Data Controller.

Data Processor shall be liable for the acts and omissions of its sub-processors to the same extent Data Processor would be liable if performing the services of each sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

Data Processor Security Obligations

Data processor is responsible for implementing and maintaining the technical and organisational measures for service provided according to the Service Agreement as described herein.

Data processor has implemented and will maintain measures to maintain the security of the service as set forth in Exhibit 1.

Controller and Processor agree that the security measures specified in Exhibit 1 to this Agreement are appropriate technical and organisational measures to ensure a level of security appropriate to the risk, such as the protection of Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access to Personal Data transmitted, stored or otherwise processed, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposing as well as the risk for the rights and freedoms of natural persons.

In the event that the Data Processor is legally obliged to disclose to third parties or to a relevant supervisory authority, personal data to satisfy legal requirements, comply with law or respond to lawful requests or binding decisions by relevant authority the Data Processor shall, unless prohibited by law, notify Data Controller without undue delay in writing or email of the reason and the form of the disclosure after it becomes aware of the obligation to disclose. The Data Processor shall wait, unless prohibited by law, for further Instructions concerning the requested disclosure.

Miscellaneous

The provisions of Cloudpoint's General Terms and Conditions regarding Service and Software regarding term and termination, liability, jurisdiction and competent court apply accordingly to this Agreement.

Amendments and supplements to this DPA must be in writing. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will take precedence.

Exhibit 1 Technical and Organisational Security Measures

Cloudpoint will implement not less than the controls listed below, or their equivalent, during the term of this DPA:

Access control to premises

The Data Processor will implement suitable measures for the purpose of preventing unauthorized persons from gaining access to the data processing equipment by the following means:

Access authorizations for employees and third parties

Protection and restriction of entrances and exits (restricted keycards and/or passes)

Logging of the persons having access

Security of relevant premises (alarms and/or security guards)

Access control to data and user control

The Data Processor commits that any and all personnel with access to the Personal Data has this authority on a need-to-know-basis, for the purpose of providing the services in the Service Agreement, by means of:

IP-address restriction to database to ensure that only the service and allowed locations can be used to access the data.

Requirements for user authorization and strict access control

Confidentiality obligations

Differentiated access policies (e. g. partial blocking)

Controlling destruction of data media

Logging of events and activities (monitoring of break-in attempts, or attempts of unauthorised access)

Issuing and safeguarding the identification codes

Use of encryption where deemed appropriate by Data Processor

Automatic log-off of user IDs that have not been used for a substantial period of time

Controlling the removal of data media

Ensuring that Customers only have access to their own Data

Transfer of data

The Data Processor will secure the Personal Data transferred and/or otherwise processed in accordance with the Service Agreement and Instructions by means of:

Policies controlling the production of backup copies

Documentation of the transfer, retrieval, and transmission programs

Authorization policy

Encrypting external online transmission

Deleting remaining data before changing data media

The traffic between the user and the service is encrypted SSL EV (extended validation) certificates.

Personal Data is not transferred to a third Party without the Data Controller’s prior written consent, unless legally obliged.

Organizational control

The Data Processor will maintain its internal organization in a manner that meets the requirements of data protection law, by means of:

Binding internal policies for personnel and/or consultants regarding security and the process of personal data, and/or instructions

Internal emergency plan for recovery and safeguard of Personal Data

Authority to access data for personnel based on a strictly need-to-know-basis

No customer data will be copied to external devices (USB sticks, CD i.e) without taking the necessary security measurements, such as encryption or password protection