POINTSHARP

Data Processing Agreement Instruction

Pointsharp Secure Cloud Net iD

Classification:	Public
Publication No.:	PSC-Lg22-06
Document version:	1.0
Document status:	Final
Date:	11 Feb 2022

Table of Contents

Personal Data Controller's instruction to the Personal Data Processor (Pointsharp) for the processing of personal data within The Service.

Personal Data Controller: Controller as defined in the Data Processing Agreement

In addition to what is already stipulated in the Data Processing Agreement, the Personal Data Processor shall also follow the instructions below:

1 Purposes, object and type

According to agreement with the Personal Data Controller, Pointsharp provides the service Pointsharp Secure Cloud Net iD (The Service). In that assignment, Pointsharp acts as Personal Data Processor and processes personal data for:

- Appointed staff at the Personal Data Controller with roles in the management of the RA domain.
- The subscribers at the Personal Data Controller, that is, the holders of the e-identities, whom are managed in systems related to The Service.

The responsibility as a Personal Data Processor applies to all personal data that Pointsharp may have access to during operation, backup and other maintenance activities, regardless if the personal data is available in unencrypted or encrypted form.

Personal data concerning the Personal Data Controller's staff and subscribers will mainly be stored in encrypted form in databases and backups of these (at rest) as well as in encrypted channels during transport, but may be available in unencrypted form in connection with troubleshooting or other maintenance initiated by the Personal Data Controller.

2 The processing involves the following types of personal data

Subscribers and staff within the Personal Data Controller's RA domain that is managed as part of The Service.

The information is normally encrypted and may contain the following personal data:

- name,
- unique identifier, for example, social security number (in Sweden "personnummer") or employee number,
- email address,
- UPN,
- telephone number,
- serial number of key bearer,
- organization affiliation,
- VAT identification number or EUID,
- RA role,
- photo,

- signature,
- electronic signature,
- office address,
- title,
- certificate with content,
- public key,
- MIFARE number,
- IMEI number, and
- other personal data added by the Personal Data Controller.

3 The processing shall include the following categories of registered persons

The processing of personal data includes the following categories of registered:

- Subscribers at the Personal Data Controller: employees, consultants, or other individuals associated with the Personal Data Controller who use The Service.
- Staff with RA roles at Personal Data Controller: employees, consultants, or other personnel who have the Personal Data Controller's assignment to manage its commitments within The Service.

4 Specify special security processing requirements that will apply to the processing of personal data that is carried out by the Personal Data Processor(s)

The Service shall provide applications with associated system components and databases where personal data is processed and stored. Personal data at rest will consist of personal data and logs that must be encrypted. System administrators at Pointsharp and its subcontractors shall only have access to personal data in encrypted form.

Administrators at Pointsharp will have access to manage personal data in The Service. Such processing of personal data shall only be carried out at the request by an authorized representative of the Personal Data Controller. The Personal Data Controller must be able to review logs of all processing performed.

In the event that trace logging is turned on for troubleshooting, personal data will be temporarily found in log files used during troubleshooting. Log files must be deleted promptly after the troubleshooting has been executed.

A background check must be carried out for all personnel before they are appointed a role that provides access to personal data of the Personal Data Controller. Appointed personnel must have proved to be suitable to hold the role and must have undergone training in the handling of personal data in accordance with the GDPR and this DPA.

Protection of personal data during transfer should not only rely on TLS, but should use an additional encryption method.

4.1 Backup

Backups that contain personal data must be protected to at least the same level as the system or application where the personal data is normally used or stored.

Complete backups of the systems shall be saved for maximum two years before they are rotated in such a way that backups older than two years are destroyed.

5 Specify technical and organizational security measures that apply to the processing of personal data by Personal Data Processor(s)

5.1 Personal data and sensitive data in application databases

All sensitive data in the application databases (including personal data) must be stored encrypted.

Access to hardware and crypto keys must be managed via a process where at least two (2) people in combination are required to handle the keys used for the protection of personal data and sensitive data in databases.

5.2 Personal data and sensitive data during transport

All communication between systems and applications must be protected with technology based on asymmetric and symmetric encryption.

6 Specify special requirements relating to logs that apply to the processing of personal data, as well as who will be having access to these.

Logs must be saved for at least ten (10) years before purging (change from the Data Processor Agreement, section 7.5).

Logs must state which individuals have and have had access to personal data, and in the event of a change in personal data it must be clear what has been changed.

Examples of logs that Pointsharp's staff will handle that contain personal data:

- Authorizations for access to personal data and changes in the authorizations.
- Logical access to The Service.
- All changes of personal data in The Service.
- Troubleshooting logs for applications.

Only personnel at the Personal Data Controller who has been appointed to a role that provides access to personal data shall have access to the logs.

6.1 Trace logging

In connection with troubleshooting there may be a need to turn on trace logging, for the various applications, in order to get information that is more detailed and to facilitate troubleshooting. These trace logs contain personal data and must therefore be handled with the utmost care.

As soon as trace logs have been analyzed, they must be deleted promptly in the systems and at any other temporary storage location or storage media used for the analysis.

7 Localization and transferring of personal data to a third country

Personal data may not be transferred to or processed in third countries.

8 Other instructions regarding the processing of personal data performed by Personal Data Processor(s)

8.1 Deviations and additions to writings in the Data Processing Agreement main document

Section 7.5:

Thinning of logs may only take place after ten (10) years instead of the specified five (5) years.

Section 16.1:

The same notice period applies to the Data Processing Agreement as to the main agreement between the parties, refer to Customer Agreement Terms and Conditions section 18.1.

POINTSHARP

Website
https://www.pointsharp.com

Copyright

Disclaimer
Specifications subject to change without further notice, unless stated otherwise in agreement.

Classification:	Public
Publ. No.:	PSC-Lg22-06
Document version:	1.0
Document status:	Final
Published:	11 Feb 2022