POINTSHARP

Data Processing Agreement

PKI as-a-service

Classification:	Public
Publication No.:	PSC-Lg22-05
Document version:	2.1a
Document status:	Final
Date:	20 Mar 2024

Table of Contents

Agreement pursuant to Article 28(3) of the General Data Protection Regulation (EU) 2016/679[1]

1. The General Data Protection Regulation (EU) 2016/679 stipulates that there must be a written agreement on the processing of personal data by the Processor on behalf of the Controller.

1. PARTIES, POSITIONS OF THE PARTIES, CONTACT DETAILS AND CONTACT PERSONS

Data Controller		**Data Processor**	
VAT identification number (or EUID)		**VAT identification number (or EUID)**	
Mailing address		**Mailing address**	
Contact person for the administration of this Data Processing Agreement		**Contact person for the administration of this Data Processing Agreement**	
Name:		Name:	
E-mail:		E-mail:	
Tel:		Tel:	
Contact person for cooperation between the parties about data protection		**Contact person for cooperation between the parties about data protection**	
Name:		Name:	
E-mail:		E-mail:	
Tel:		Tel:	

2. DEFINITIONS

In addition to the concepts defined in the text for the Data Processing Agreement, these definitions shall, regardless of whether they are used in the plural or singular, in definite or indefinite form, have the following meaning when entered with capital letters as the initial letter.

Term	Definition
Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data protection legislation	Refers to all privacy and personal data legislation, along with any other legislation (including regulations and directives) applicable to the Processing carried out in accordance with this Agreement, including national legislation and EU legislation.
Data Subject	Natural person whose Personal Data are Processed.
EUID	Identifier that comprises a country code, the register identifier, the registration number, and possibly a verification digit to enable the identification of companies and their branches in EU member states in the Business Registers Interconnection System.
Instruction	The written instructions that more specifically define the object, duration, type and purpose of Personal Data, as well as the categories of Data Subjects and special requirements that apply to the Processing.
Log	A Log is the result of Logging
Logging	Logging is a continuous collection of information about the Processing of Personal Data that is performed according to this Agreement and which can be associated with an individual natural person.
Personal Data	Any information relating to an identified or identifiable natural person; 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.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed

Term	Definition
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
Subprocessor	A natural or legal person, public authority, agency or other body which, in the capacity of subcontractor to the Processor, Processes Personal Data on behalf of the Controller.
Third Country	A state that is not a member of the European Union (EU) or the European Economic Area (EEA).
VAT identification number	Individual number given to each taxable person intending to make supplies of goods or services, or to make acquisitions of goods for business purposes, each number having a prefix of two letters by which the Member State of issue is identified

3. BACKGROUND AND AIM

3.1 Through this Agreement, the Instructions and a list of possible Subprocessors (hereafter jointly referred to as "the Agreement"), the Controller regulates Processor'sProcessing of Personal Data on behalf of the Controller. The aim of the Agreement is to safeguard the freedoms and rights of the Data Subject during Processing, in accordance with what is stipulated in Article 28(3) of the General Data Protection Regulation (EU) 2016/679 ("GDPR").
3.2 When this Agreement forms one of several contractual documents within the framework of another agreement, the second agreement is referred to as the "Main Agreement" in this Agreement.
3.3 If anything stipulated in item 1, paragraph 3.2, item 15 or 16, paragraph 17.6, items 18–20 or 22 in this Agreement is otherwise regulated in the Main Agreement, the regulation of the Main Agreement shall have precedence.
3.4 References in this Agreement to national or EU legislation refer to applicable regulations at any given time.

4. PROCESSING OF PERSONAL DATA AND SPECIFICATION

4.1 The Controller hereby appoints the Processor to carry out the Processing on behalf of the Controller in accordance with this Agreement.
4.2 The Controller shall give written instructions to the Processor on how the Processing should be carried out.

4.3 The Processor may only carry out the Processing pertaining to this Agreement and the instructions in force at any given time.

5. OBLIGATIONS OF THE CONTROLLER

5.1 The Controller undertakes to ensure that there is a legal basis for the Processing at all times and for compiling correct Instructions with regard to the nature of the Processing so that the Processor and any Subprocessor can fulfil their tasks according to this Agreement and Main Agreement, where applicable.
5.2 The Controller shall, without unnecessary delay, inform the Processor of changes in the Processing which affect the Processor's obligations pursuant to Data Protection Legislation.
5.3 The Controller is responsible for informing Data Subjects about the Processing and protecting the rights of Data Subjects according to Data Protection Legislation as well as taking any other action incumbent on the Controller according to Data Protection Legislation.

6. OBLIGATIONS OF THE PROCESSOR

6.1 The Processor undertakes to only perform the Processing in accordance with this Agreement and for the specific purposes stipulated in the Instructions, as well as to comply with Data Protection Legislation. The Processor also undertakes to continuously remain informed about applicable law in this area.
6.2 The Processor shall take measures to protect the Personal Data against all types of Processing which are incompatible with this Agreement, Instructions and Data Protection Legislation.
6.3 The Processor undertakes to ensure that all natural persons working under its management follow this Agreement and Instructions and that such natural persons are informed of relevant legislation.
6.4 The Processor shall, at the request of the Controller, assist in ensuring that the obligations pertaining to Articles 32-36 in the GDPR are fulfilled and respond to requests for the exercise of a Data Subject's rights pertaining to the GDPR, Chapter III, taking into account the type of Processing and the information which the Processor has access to.
6.5 In the event that the Processor finds the Instructions to be unclear, in violation of the Data Protection Legislation or non-existent, and the Processor is of the opinion that new or supplementary Instructions are necessary in order to fulfil its undertakings, the Processor shall inform the Controller of this without delay, temporarily suspend the Processing and await new Instructions, if the Parties have not agreed otherwise.
6.6 If the Controller provides the Processor with new or revised Instructions, the Processor shall without unnecessary delay from receipt, communicate to the Controller whether the implementation of the new Instructions causes changed costs for the Processor.

7. SECURITY MEASURES

7.1 The Processor shall take all appropriate technical and organisational security measures required pertaining to Data Protection Legislation to prevent Personal Data Breaches, by ensuring that the procedure of Processing meets the requirements of the GDPR and that the rights of the Data Subjects are protected.
7.2 The Processor shall continuously ensure that the technical and organisational security in connection with Processing is executed with an appropriate level of

confidentiality, integrity, accessibility and resilience.
7.3 Any added or revised requirements for protective measures from the Data Controller, after the Parties have signed this Agreement, will be considered as new Instructions pertaining to this Agreement.
7.4 The Processor shall, through its control systems for authority, only grant access to the Personal Data for such natural persons working under the Processor's management and who need access to be able to perform their duties.
7.5 The Processor undertakes to continuously log access to the Personal Data in accordance with this Agreement to the extent required according to the Instructions. Logs may be erased only five (5) years after the logging event, unless otherwise stated in the Instructions. Logs will be subject to the required protection measures pertaining to Data Protection Legislation.
7.6 The Processor shall systematically test, investigate and evaluate the effectiveness of the technical and organisational measures which will ensure the security of the Processing.

8. SECRECY/DUTY OF CONFIDENTIALITY

8.1 The Processor and all natural persons working under its management shall observe both confidentiality and professional secrecy during the Processing. The Personal Data may not be used or disseminated for other purposes, either directly or indirectly, unless otherwise agreed.
8.2 The Processor shall ensure that all natural persons working under its management, participating in the Processing, are bound by a confidentiality agreement pertaining to the Processing. However, this is not a requirement if they are already covered by a legally sanctioned duty of confidentiality. The Processor also undertakes to ensure that there is a nondisclosure agreement with its Subprocessor and confidentiality agreement between the Subprocessor and all natural persons working under its management, participating in the Processing.
8.3 The Processor shall promptly inform the Controller of any contacts with supervisory authorities pertaining to the Processing. The Processor does not have the right to represent the Controller or act on behalf of the Controller towards supervisory authorities in matters relating to the Processing.
8.4 If the Data Subject, supervisory authority or third Party requests information from the Processor pertaining to the Processing, the Processor shall inform the Controller about the matter. Information about the Processing may not be submitted to the Data Subject, supervisory authority or third parties without written consent from the Controller, unless mandatory law so stipulates that such information must be provided. The Processor shall assist with the communication of the information covered by a consent or legal requirement.

9. INSPECTION, SUPERVISION AND AUDITING

9.1 The Processor shall, without unnecessary delay, as part of its guarantees, pursuant to Article 28.1 of the GDPR, be able to report, at the request of the Controller, which technical and organisational security measures are being used for the processing to meet the requirements according to the DPA and Article 28.3.h of the GDPR.
9.2 The Processor shall review the security of the Processing at least once a year by performing a checks to ensure that the Processing complies with this Agreement. Upon request, the results of such checks shall be shared with the Controller.
9.3 The Controller or a third party it appoints (who cannot be a competitor of the

Processor) is entitled to check that the Processor meets the requirements of this Agreement, Instructions and Data Protection Legislation. During such a check, the Controller shall assist the Controller, or the person carrying out the review on behalf of the Controller, with documentation, access to premises, IT systems and other assets needed to be able to check the compliance of the Controller with this Agreement, Instructions and Data Protection Legislation. The Controller shall ensure that staff who carry out the check are subject to confidentiality or non-disclosure obligations pertaining to law or agreement.
9.4 As an alternative to the stipulations of items 9.2–9.3, the Processor is entitled to offer other means of checking the Processing, such as checks carried out by independent third parties. In such a case, the Controller shall have the right, but not the obligation, to apply such alternative means. In the event of such a check, the Processor shall provide the Controller or third party with the assistance needed for performing the check.
9.5 The Processor shall provide the supervisory authority, or other authority which has the legal right to do so, the means to carry out supervision according to the authority's request pertaining to the legislation in force at any time, even if such supervision would otherwise be in conflict with the provisions of this Agreement.
9.6 The Processor shall assure the Controller rights towards any Subprocessor corresponding to all of the rights of the Controller towards the Processor according to section 9 of this Agreement.

10. HANDLING OF CORRECTIONS, DELETIONS, ETC.

10.1 In the case of the Controller requesting correction or deletion due to incorrect processing by the Processor, the Controller shall take appropriate action without unnecessary delay, within thirty (30) days at the latest, from the time the Processor has received the required information from the Controller. When the Controller requests deletion, the Processor may only carry out Processing of the Personal Data in question as part of the process for correction or deletion.
10.2 If technical and organisational measures (e.g., upgrades or troubleshooting) are taken by the Processor in the Processing, which can have an effect on the Processing, the Processor shall inform the Controller in writing pursuant to what is stipulated about notifications in item 18 of this Agreement. The information shall be submitted in good time prior to the measures being taken.

11. PERSONAL DATA BREACHES

11.1 The Processor shall have the capability to restore accessibility and access to Personal Data within a reasonable time in the event of a physical or technical incident pertaining to Article 32.1.c of the GDPR.
11.2 If technical and organisational measures (e.g. upgrades or troubleshooting) are taken by the Processor with regard to the Processing, and these can be expected to affect the Processing, the Processor shall inform the Controller in writing in accordance with the provisions on notifications set out in Section 18 of the Agreement. This information shall be communicated well in advance of the measures being taken.
11.3 In the event of a Personal Data Breach, which the Processor has been made aware of, the Processor shall notify the Controller of the Breach in writing without unnecessary delay. The Processor shall, taking into account the type of Processing and the information available to the Processor, provide the Controller with a written description of the Personal Data Breach.

11.4 The description shall give an account of:

a. The nature of the Personal Data Breach and, if possible, the categories and number of Data Subjects affected and the categories and number of Personal Data records affected,

b. the likely impact of the Personal Data Breach, and

c. measures taken or proposed and measures to mitigate the potential negative effects of the Personal Data Breach.

11.5 If it is not possible for the Processor to provide the full description at the same time, according to item 11.3 of this Agreement, the description may be provided in instalments without unnecessary further delay.

12. SUBPROCESSOR

12.1 The Processor is entitled to hire the Subprocessor(s) listed in the Subprocessor appendix. 2.

12.2 The Processor undertakes to enter a written agreement with the Subprocessor to regulate the Processing that the Subprocessor carries out on behalf of the Controller and to only hire Subprocessors who provide adequate guarantees. The Subprocessor shall carry out appropriate technical and organisational measures to ensure that the Processing fulfils the requirements of GDPR. When it comes to data protection, such an agreement shall entail the same obligations for the Subprocessor as are set out for the Processor in this Agreement.

12.3 The Processor shall ensure in its agreement with the Subprocessor that the Controller is entitled to terminate the Subprocessor and instruct the Subprocessor to, for instance, erase or return the Personal Data if the Processor has ceased to exist in the actual or legal sense, or has entered into insolvency.

12.4 The Processor shall be fully responsible for the Subprocessor’s Processing on behalf of the Controller. The Processor shall promptly inform the Controller if the Subprocessor fails to fulfil its undertakings under the Agreement.

12.5 The Processor is entitled to hire new subprocessors and to replace existing subprocessors unless otherwise stated in the Instructions.

12.6 When the Processor intends to hire a new subprocessor or replace an existing one, the Processor shall verify the Subprocessor’s capacity and ability to meet their obligations in accordance with the Data Protection Legislation. The Processor shall notify the Controller in writing of

a. the Subprocessor’s name, corporate identity number and head office (address and country),

b. which type of data and categories of Data Subjects are being processed, and

c. where the Personal Data will be processed.

12.7 The Controller is entitled within thirty (30) days of the notice pursuant to item 12.6 to object to the Processor’s hiring of a new subprocessor and, due to such an objection, to cancel this Agreement to be terminated in accordance with the provisions of item 16.4 of this Agreement.

12.8 The data processor shall at all times keep a correct and updated list of the Subprocessors hired for tte Processing of Personal Data on behalf of the Controller and make the list accessible to the Controller. The list shall specifically state in which country the Subprocessor Processes Personal Data and types of Processing the Subprocessor carries out.

12.9 When the Processor ends its collaboration with a Subprocessor, the Processor shall notify the Controller in writing. When an agreement terminates, the Processor

shall ensure that the Subprocessor erases or returns the Personal Data.
12.10 At the Controller's request, the Processor shall send a copy of the agreement regulating the Subprocessor's Processing of Personal Data in accordance with item 12.1.

13. LOCALISATION AND TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

13.1 The Processor shall ensure that the Personal Data shall be handled and stored within the EU/EEA by a natural or legal person who is established in the EU/EEA, unless the parties to this Agreement agree otherwise.
13.2 The Processor is only entitled to transfer Personal Data to a Third Country for Processing (e.g. for service, support, maintenance, development, operations or other similar handling) if the Controller has given advance written approval of such transfer and has issued Instructions to this end.
13.3 Transfer to a Third Country for Processing in accordance with item 13.2 of the Agreement may be carried out only if it complies with the Data Protection Legislation and fulfils the requirements for the Processing set out in this Agreement and the Instructions

14. LIABILITY FOR DAMAGES IN CONNECTION WITH THE PROCESSING

14.1 In the event of a compensation for damage in connection with Processing, through a judgment given or settlement, to be paid to a Data Subject due to an infringement of a provision in the Agreement, Instructions and/or applicable provision in Data Protection Legislation, Article 82 of the GDPR shall apply.
14.2 Fines pursuant to Article 83 of the GDPR, or Chapter 6, Section 2 of the Data Protection Act (2018:218) with supplementary provisions to the EU's data protection regulation shall be borne by the Party to the Agreement named as recipient of such sanctions.
14.3 If either party becomes aware of circumstances that could be detrimental to the other party, the first party shall immediately inform the other party of this and work actively with the other party to prevent and minimise the damage or loss.
14.4 Regardless of the content of the Main Agreement, items 14.1 and 14.2 of this Agreement take precedence to other rules on the distribution between the Parties of claims among themselves as far as the processing is concerned.

15. CONCLUSION, TERM AND TERMINATION OF THE AGREEMENT

15.1 This Agreement shall enter into force from the time the Agreement is signed by both Parties and until further notice. Either party has the right to terminate the Agreement with thirty (30) days' notice.

16. AMENDMENTS, TERMINATION WITH IMMEDIATE EFFECT, ETC.

16.1 Each party to the Agreement shall be entitled to invoke a renegotiation of the Agreement if there is a major change of the ownership of the other party or if applicable legislation or interpretation thereof changes in a way that significantly affects the Processing. The invoking of a renegotiation pursuant to the first sentence does not mean that any part of the Agreement will cease to be in effect, but only means that a renegotiation of the Agreement will commence.
16.2 Additions and amendments to the Agreement must be made in writing and signed by both parties.

16.3 If either party becomes aware that the other party is acting in violation of the Agreement and/or Instructions, the first party shall inform the other party without delay of the actions in question. The party is then entitled to suspend the performance of its obligations pursuant to the Agreement until such time as the other party has declared that the actions have ceased, and the explanation has been accepted by the party that made the complaint.
16.4 If the Controller objects to the Processor using a new Subprocessor, pursuant to item 12.6 of this Agreement, the Controller is entitled to terminate the Agreement with immediate effect.

17. MEASURES IN THE EVENT OF TERMINATION OF THE AGREEMENT

17.1 Upon termination of the Agreement, the Processor shall, without unnecessary delay, depending on what the Controller chooses, either delete and certify to the Controller that it has been carried out, or return

a. all Personal Data Processed on behalf of the Controller and
b. all associated information such as Logs, Instructions, system solutions, descriptions and other documents which the Processor has obtained through information exchange in pursuance of the Agreement.

1.2 In connection with the return of data, the Processor shall also delete existing copies of Personal Data and associated information.
1.3 The obligation to delete or return Personal Data or/and associated information does not apply if storage of the Personal Data or information is required under EU law or relevant national law where Processing may be carried out pursuant to the Agreement.
1.4 If Personal Data or associated information is returned, it must be in a commonly used and standardised format, unless the Parties have agreed to another format.
1.5 Until the data is deleted or returned, the Processor shall ensure compliance with the Agreement.
1.6 Return or deletion pertaining to the Agreement shall be carried out no later than thirty (30) calendar days counting from the time of termination of the Agreement, unless otherwise stated in the Instructions. Processing of Personal Data which the Processor subsequently carried out shall be regarded as unauthorised Processing.
1.7 Confidentiality/professional secrecy in item 8 shall continue to apply even if the Agreement otherwise ceases to apply.

18. NOTIFICATIONS WITHIN THE PURVIEW OF THIS AGREEMENT AND THE INSTRUCTIONS

18.1 Notifications about the Agreement and its administration, including termination, shall be submitted via email or in any other manner agreed by the Parties to each Party's contact person for the Agreement.
18.2 Notifications about the collaboration of the Parties regarding the data protection shall be submitted via email or in any other manner agreed by the Parties to each Party's contact for the Parties' cooperation on data protection.
18.3 A notification shall be deemed to have reached the recipient no later than one (1) business day after the notification has been sent.

19. CONTACT PERSONS

19.1 Each Party shall appoint their contact person for the Agreement.
19.2 Each Party shall appoint their contact person for the Parties' cooperation on data protection.

20. RESPONSIBILITY FOR INFORMATION REGARDING PARTIES, CONTACT PERSONS, AND CONTACT INFORMATION

20.1 Each Party is responsible for the information entered in item 1 of the Agreement always being current and correct.
20.2 Change of information in item 1 shall be communicated to the other Party pursuant to item 18.1 of the Agreement.

21. CHOICE OF LAW AND DISPUTE RESOLUTION

21.1 When interpreting and applying the Agreement, Swedish law shall apply with the exception of the choice of law rules. Disputes regarding the Agreement shall be settled by a competent Swedish court.

22. THE PARTIES' SIGNATURES ON THE AGREEMENT

22.1 The Agreement can be produced either in digital format for electronic signature or in paper format for manual signature. In the latter case, the Agreement is drawn up in two identical copies, whereof each Party receives one.

Data controller	
Place	
Date	
Name in print	
Signature	

Data processor	
Pointsharp AB	
Place	
Date	
Name in print	
Signature	

Version management

This document is based on the Data Processing Agreement developed and maintained by Sveriges Kommuner och Landsting (SKR). For more information and the original document, consult the website https://skr.se/skr/ekonomijuridik/juridik/offentlighetsekretessarkivdataskyddsforordningengdpr/dataskyddsforordningengdpr/avtalpersonuppgiftsbitrade.12704.html.

Version	Datum	Förändringar	Ansvarig
1.1	2018-12-19	10.1, 14.1, 18.2,	PR
1.2	2019-12-17	2, 3.1, 3.3, 5.1, 6.3, 6.4, 7.1, 8.2, 9.1, 9.2, 9.6, 10.1, 10.2, 11.4, 12, 13.3, 14.2, 14.3, 17.3, 17.4, 18.2, 18.3, 18.4, 21.1, 22.1	NE
1.2.1	2020-01-02	17.4	PR
1.2.1a	2022-02-07	1 (changed Corporate ID No. to VAT identification number), 2 (added VAT identification number and EUID to the term list, changed list to alphabetic order)	Pointsharp
2.1 (inkl. 2.0)	2023-04-06	1, 2, 3.1, 3.3, 5.1, 6.1, 6.5, 10.2, 12.2, 12.3, 12.4, 12.5, 12.7, 12.8, 12.9, 12.10, 14.3, 15, 16, 17, 18, 19, 20, 21, 22	HA, EW, FS, PR
2.1a	2024-02-29	Removed 22.2	Pointsharp

Data Processing Agreement Instruction

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. The purposes, object and nature

1 a. The object of the Processing of Personal Data by the Processor for the Controller is to:

Provide a service for issuing and life-cycle management of e-identities to be used by the user for various purposes, such as logging in to IT infrastructure/web applications and signing electronic documents

1 b. The objective of the Processing of Personal Data by the Processor for the Controller is to:

According to agreement with the Personal Data Controller, Pointsharp provides the service PKI as a Service (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.

1 c. The Processing of Personal Data by the Processor on behalf of the Controller refers mainly to the following measure of Processing (type or nature of the Processing):

- Collection
- Logging
- Processing
- Reading
- Storage
- Transfer

2. The processing involves the following types of Personal Data

The Processor has the right to Process the following types of Personal Data on behalf of the Controller:

- name,
- unique identifier, for example, social security number (in Sweden "personnummer") or employee number,
- email address,
- upn,
- telephone number,
- serial number and model of key bearer,
- OS on device there key bearer is used,
- organization affiliation,
- VAT identification number or EUID,
- Microsoft SID (Microsoft security identifier)
- RA role,
- photo,
- signature,
- electronic signature,
- office address,
- title,
- certificate with content,
- public key, and
- MIFARE number.

3. Processing covers certain categories of Data Subject

The Processor has the right to process Personal Data regarding the following categories of Data Subjects:

- 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 requirements when it comes to Processing of Personal Data carried out by the Processor

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.

4.1. Backups

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 the special technical and organizational security measures which apply to the Processing of Personal Data by Processor

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

6. Specify special requirements for logging with regard to the Processing of Personal Data and who should have access to them.

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 staff at the Personal Data Processor 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.
- Events related to issuing and managing certificates.

Only staff at the Personal Data Processor 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. Duration of Processing

During the duration of the Data Protection Agreement.

Personal data in logs that Pointsharp must retain after the termination of the Data Processor Agreement, due to traceability requirements, will be processed in accordance with the personal data processor agreement until the logs are deleted after 10 years

9. Other instructions regarding the Processing of Personal Data performed by the Processor

9.1. 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

Section 17:1:
Logs will not be deleted in connection with the termination of the agreement, it will happen after 10 years, see section 8 of this instruction.

List of Processor's Subcontractors

Pointsharp AB, as Personal Data Processor, has the following subcontractors for parts of the PKI as a Service .

Company/ organisation	Address and contact details	Location of Personal Data (address, country)	Types of Personal Data Processed by the Subprocessor	Purpose of processing by the Subprocessor	Processing time	Additional information about the Subprocessor's Processing of Personal Data
Orange Business Digital Sweden AB 556638-0639	Gårdsvägen 6, 169 70 Solna Telephone: +46 8 501 126 00	Solna and Upplands Väsby Sweden	See the Data Processing Agreement Instruction section 2 for information on which Personal Data it could be.	Operational supplier (Supplier of IT services) Provides server operation for all the components that are part of the Service and are necessary for issuing and checking the validity of the e-identification.	During the validity of the main agreement and thereafter handling of personal data that is necessary to fulfill requirements in regulatory documentation (based on requirements from DIGG, CP/CPS and trust framework)	All data is encrypted in transit and at rest in databases. Orange's operation of IT services is ISO/IEC 27001 certified and the data centers are PCI-DSS certified.

Company/ organisation	Address and contact details	Location of Personal Data (address, country)	Types of Personal Data Processed by the Subprocessor	Purpose of processing by the Subprocessor	Processing time	Additional information about the Subprocessor's Processing of Personal Data
Thales DIS Sweden AB 556343-7218	Glasfibergatan 12, 125 45 Älvsjö Telephone: +46 8 517 95700	Stockholm Sweden	Personal data that appears physically on the card, is stored in the card's chip or is otherwise linked to the card • name, • unique identifier, • title, • e-mail address, • upn, • card serial number • organisation, • Microsoft SID (Microsoft security identifier), • photo, • certificate with public key (containing the above-mentioned personal data), • signature, • MIFARE-nuber, • office address,	Ordering, issuing and delivery of ordinary cards in cases where the customer uses personalized smart cards ordered from factory.	During the validity of the main agreement and thereafter handling of personal data that is necessary to fulfill requirements in regulatory documentation (based on requirements from DIGG, CP/CPS and trust framework)	Thales' security infrastructure is based on ISO/IEC 27001. The largest part of production is certified according to ISO/IEC 27001, which includes the part of the business where raw materials for smart cards are manufactured, i.e. where the personalization of passports and national identity cards (NID) takes place.

Company/ organisation	Address and contact details	Location of Personal Data (address, country)	Types of Personal Data Processed by the Subprocessor	Purpose of processing by the Subprocessor	Processing time	Additional information about the Subprocessor’s Processing of Personal Data
			• security code (PUK), • private key			

POINTSHARP

Website
https://www.pointsharp.com

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

Classification:	Public
Publ. No.:	PSC-Lg22-05
Document version:	2.1a
Document status:	Final
OID:	
Published:	20 Mar 2024