# TSPS - Trust Service Practise Statement

Appendices to TSPS:

PS for Remote Electronic Signature

PS for Remote Electronic Seal

PS for Time Stamp Authority

**Version history**

| Version | Date of release | Approved by (Title and name) | Comments |
|---|---|---|---|
| 1.0 | 22.11.2022 | Information Security Manager / Fredrik Lernevall | First release |

# Introduction

Penneo is an innovative company with a diverse organisation, a strong work ethic, and meaningful core values.

At Penneo, the vision is to create a global business network of trust where digital identity, document management, signing processes, and the exchange of information can be made easy, secure and compliant.

Penneo is a Software-as-a-Service company originally founded to help companies digitally sign documents instead of using pen and paper in order to save time, money, paper, and ink. Penneo quickly evolved from that digital signature platform to an eco-system of automation solutions that digitizes companies' workflows related to signing and managing documents in an easy and efficient way as well as staying compliant to regulations such as anti-money laundering legislation.

Penneo strives to provide an easy to use, yet efficient solution that does not only entail digital signatures, but shapes your whole digital document management experience - from e-signature to the automation of signing processes and secure online storage. We aim to build trust between companies and their clients by creating a secure ecosystem of verified and compliant businesses and authorities.

Based on e-signature, Penneo creates several blocks of procedures and documentation that describe Penneo's business:

- Penneo’s Trust Service Practice Statement - with a general description of the all trusted services provided to clients
- Certification Practice Statement (CPS), Practice Statements (PS) for electronic Signature, Seal, Time stamps authorities and Certificate Policies (CPs) for all Public Key Infrastructure (PKI) Services - with information about the services related to root CA and subordinated CAs for Signature, Seal and Time stamp.
- Internal system and technical documentation for particular steps and processes. The technical solution is implemented using an IaaS provider as well as hosting devices at a co-location provider based on legal agreements and service level agreements. Cloud technology for PKI services and time synchronization is used in very high availability and security.

## 1.1. Overview

The hierarchy of the certification authorities and provided services complies with the eIDAS regulation (REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC).

Certification authorities provides the following services defined by eIDAS regulation:

- issuing qualified certificates for remote electronic signatures (physical/legal person)
- issuing qualified certificates for remote electronic seals (legal entity)
- issuing qualified remote electronic time stamps

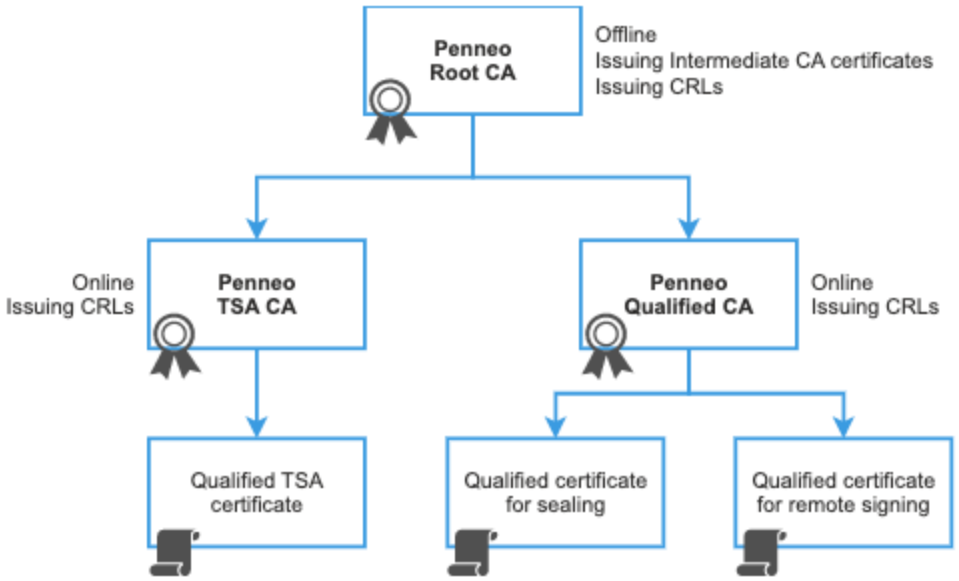
Within Penneo, there are the CPs, Practice Statements and CPS defined for:

- Qualified Root CA

- Issuing qualified certificates for remote electronic signing (Intermediate/subordinate CA)
- Issuing qualified certificates for electronic sealing (Intermediate/subordinate CA)
- Issuing qualified certificates for electronic time stamps (Intermediate/subordinate CA)

## Logical Architecture

This diagram below presents a high-level illustration of the PKI architecture operated by Penneo for subscribers.




## 1.2. Document name and identification

Name and Identification of the document - Trust service practice statement.

No OID allocated for this document.

## 1.3. Trust services participants

> 📌 Please see chapter 1.3 of Appendix A for further information regarding Remote Electronic Signature.

📌 Please see chapter 1.3 of Appendix B for further information regarding Remote Electronic Seal.

📌 Please see chapter 1.3 of Appendix C for further information regarding Time Stamp Authority.

## 1.4. Certificate usage

📌 Please see chapter 1.4 of Appendix A for further information regarding Remote Electronic Signature.

📌 Please see chapter 1.4 of Appendix B for further information regarding Remote Electronic Seal.

📌 Please see chapter 1.4 of Appendix C for further information regarding Time Stamp Authority.

## 1.5. Policy administration

### 1.5.1. Organization administering the document

Penneo administers and manages this document.

### 1.5.2. Contact persons

The contact persons related to this document are:

- VP of Engineering - responsible for the technical implementation of the trust service;
- Information Security Manager - responsible for the policies governing the trust service.

All questions and/or comments concerning this document shall be addressed to: TrustService@penneo.com

### 1.5.3. Person determining suitability for the policy

The pesons determining the suitability of this document are:

- VP of Engineering - responsible for the technical implementation of the trust service;
- Information Security Manager - responsible for the policies governing the trust service.

Results and recommendations from an eIDAS approved auditor are are considered by the responsible persons when determining the suitability of this document.

### 1.5.4. Approval procedures

The approval procedures and processes are managed by Penneo's managers. They determine employees performing the update, modification or changes based on these procedures.

The final version of the performed update/modification is approved according to internal responsibilities by Penneo's manager.

## 1.6. Definition and acronyms

**Definitions**

| | |
|---|---|
| Penneo’s CAs Services | A set of certification authorities which is possible to use during electronic signature an electronic sealing - Root CA, subordinate CA, TimeStamp CA. |
| Penneo’s PKI Services | Penneo’s CA Services and qualified services for remote electronic signature and remote electronic sealing and stamping. |
| Certificate | A data message issued by a certification service provider combines data (code or public cryptographic keys that are used to verify an electronic signature) to verify signatures with the signer and allows to verify his/her identity. |
| Public Certificate registry/repository | An electronic registry where certificates and |

| | |
|---|---|
| | lists of revoked end-user certificates and service certificates are published. It is accessible according to the rules defined in the Certification Practice Statement or Certification Policy (CPS/CP) document. |
| Certificate policy (CP) | A set of rules that assess the applicability of certificates within individual groups and / or classes of applications in accordance with security requirements and is supported by Certification Practice Statement (CPS). It relates to the use of the certificate and to the use of data for the verification of the electronic signature of the holder for which the certificate has been issued. |
| Certificate Practice Statement (CPS) | It forms the framework of the rules set by the CP. They define in their procedures, provisions and regulations the requirements for all services entering the registration and certification process. |
| Certificate Revocation List /repository(CRL) | List of expired certificates published by the Certification Authority to the Public Certificate Registry/repository (LDAP) |
| Electronic Signature | It expresses the general concept of signature, which is applied in an electronic environment. A wide range of means and technologies are used to generate this signature, including digital signatures and biometric methods.These are data in electronic form, which are attached to or logically connected to the data message and which enable the verification of the identity of the signer in relation to the data message. |
| Digital Signature | It is based on the use of cryptography (cryptosystems) with a public key. Currently, this term is used to refer to a special type of electronic signature. This type of electronic signature is used to verify the identity of the sender of the message or the person who signed the message. It is also used to verify |

| | |
|---|---|
| | that the message to which the digital signature was attached is not altered/modified. |
| Asymmetric cryptography - RSA | The principle of the method is that data encrypted by one of the keys can only be decrypted with knowledge of the other of the key pair and vice versa. One of the keys is called private, the other public. The RSA algorithm is used for asymmetric cryptography. |
| Private key | Data for creating a digital signature. Private part of an asymmetric key pair for cryptographic purposes. Used to sign and decrypt messages. |
| Public Key | Digital signature verification data. Public part of an asymmetric key pair for cryptographic purposes. Used to encrypt messages and verify digital signatures. |
| Registration Authority (RA) | Companies which are responsible for verifying the application for a certificate, identifying and authorizing the subscriber. |
| Electronic Seal | An electronic seal is a piece of data attached to an electronic document or other data, which ensures data origin and integrity. |
| Revoke the certificate | To terminate the certificate based on the responsible user's/manager’s request. The certificate cannot be renewed. |
| Suspension of the certificate | Suspend the certificate based on the responsible user's/manager’s request. Validity can be renewed. |
| Relying Party | An entity that relies on trust in a certificate and an electronic signature verified using that certificate. |
| Root CA | CA issuing certificates to Subordinate CA |
| OCSP responder | A server that provides public key status information in a certificate using OCSP protocol |
| Subordinate CA | CA  issuing certificates to subscribers and relying services |
| TimeStamp CA | CA issuing certificates with time-stamp to subscribers |

| | |
|---|---|
| SmartCard-HSM | The SmartCard-HSM is a lightweight hardware security module in a smart card and form factor. It provides a remote-manageable secure key store for RSA and ECC keys.The SmartCard-HSM is USB Token, which is effectively a chip card interface device (CCID) compliant card reader combined with the smart card chip in a single device. |

### Acronyms

| | |
|---|---|
| eIDAS | The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014 provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. |
| PKI | Public Key Infrastructure - set of services (HW and SW) performing the all activities concerning to certificate life-cycle. |
| EJBCA | PrimeKey’s EJBCA is one of the longest running CA software projects, providing time-proven robustness and reliability. EJBCA is platform independent, and can easily be scaled out to match the needs of your PKI requirements, whether you're setting up a national eID, securing your industrial IOT platform or managing your own internal PKI. EJBCA covers all your needs - from certificate management, registration and enrolment to certificate validation.Software provided by PrimeKey. https://www.primekey.com/ |
| LDAP | Lightweight Di/tablerectory Access Protocol - Public Certificate Registry |
| OID | Object Identifier, number base od object’s identification |
| RA | Registration authority |

| | |
|---|---|
| IP | Identity providers |
| CA | certificate authority |
| TSA | Time stamp authority |
| UTC | Coordinated universal time |
| TSP | Trust service provider |
| HSM | Hardware security modul |
| CRL | Certificate revocation list |
| CCID | Chip card interface device |
| DKEK | Device Key Encryption Key |
| UPS | Uninterruptible Power Supply |

# 2. Publication and Repository Responsibilities

## 2.2. Publication of certificate information

### 2.2.1. Published information

**Address of Company:** Enghavevej 40, 4th floor, 1674 Copenhagen V, Denmark

Internet address: http://www.penneo.com

The publication of root CA certificates, subordinate CAs, certificates for electronic signature, seal and timestamps are available on the Penneo web pages and contain mainly:

- Certificate number;
- Name (contents from common name structure);
- Period of validity of the certificate;
- Object identifier of policy (OID policy);
- CRL address.

Certification policies, Practice statements, Disclosure statements and CPS can be viewed at:

http://www.trust.penneo.com.

Certificate revocation list (CRL) contains information about:

- the date the CRL was issued;
- the CRL number;
- and the link where the CRL is available - included in a certificate.

The list of subscriber certificates are published in the public certificate repository. Details are described in particular CP.

Access to published information is realized via Internet protocols - HTTP and HTTPS.

### 2.2.2. Unpublished information

Penneo reserves the right not to disclose information in accordance with internal security policies, procedures and processes.

## 2.3. Time or frequency of publication

Penneo publishes information on its web pages:

- The frequency of issuing the CRL of the Root CA is twice a year, with validity time one year;
- The frequency of issuing a CRL for the Subordinate CAs once every 12 hours, with validity time 24 hours;
- Certificate policy is published immediately after approval.
- Certificate Practise Statement is published immediately after approval.
- Particular practice statements for signature, seal and time stamp are published immediately after approval.
- Information about revoked certificates of Penneo’s services is published immediatelly.
- Necessary information from applicable law and legal requirements.
- Necessary information from Penneo’s administration, legal and subscribers improvement point of view.

## 2.4. Access controls on repositories

Public published information is accessible on Penneo's web pages in read only format. Access control prevents unauthorized access to modify, delete or add entries into repository.

# 3. Identification and authentication

## 3.1. Naming

The naming scheme of Penneo’s trust services is approved and implemented by responsible Penneo employees or Penneo’s managers.

📌 Please see chapter 3.1 of Appendix A for further information regarding Remote Electronic Signature.

📌 Please see chapter 3.1 of Appendix B for further information regarding Remote Electronic Seal.

📌 Please see chapter 3.1 of Appendix C for further information regarding Time Stamp Authority.

## 3.2. Initial identity validation

Initial identity validation is specified in the relevant CP.

📌 Please see chapter 3.2 of Appendix A for further information regarding Remote Electronic Signature.

📌 Please see chapter 3.2 of Appendix B for further information regarding Remote Electronic Seal.

📌 Please see chapter 3.2 of Appendix C for further information regarding Time Stamp Authority.

## 3.3. Identification and Authentication for re-key request

Identification and Authentication for re-key request is specified in the relevant CP.

## 3.4. Identification and authentication for revocation request

This chapter is specified in the relevant CP.

# 4. Certificate life-cycle operational requirements

📌 Please see chapter 4 of Appendix A for further information regarding Remote Electronic Signature.

📌 Please see chapter 4 of Appendix B for further information regarding Remote Electronic Seal.

📌 Please see chapter 4 of Appendix C for further information regarding Time Stamp Authority.

## 4.1. Certificate application

Certificate application of Penneo's PKI services are performed in secure cryptographic modules. Modules are certified on CC level 5 resp. CC level 4+.

Certificates of subscribers are issued in secure cryptographic modules certified on CC level 4+. Certificates are published and available on public registry.

Minimally once a year secure cryptographic modules are confronted with the status of cryptographic modules on EU (European Commission’s list of Secure Signature Creation Devices) list and possible shortcomings are solved.

## 4.2. Certificate application processing

This chapter is specified in relevant CP.

## 4.3. Certificate issuance

This chapter is specified in relevant CP.

## 4.4. Certificate acceptance

This chapter is specified in relevant CP.

## 4.5. Key pair and certificate usage

This chapter is specified in relevant CP.

## 4.6. Certificate renewal

This chapter is specified in relevant CP.

## 4.7. Certificate re-key

This chapter is specified in relevant CP.

## 4.8. Certificate modification

This chapter is specified in relevant CP.

## 4.9. Certificate revocation and suspension

This chapter is specified in relevant CP.

## 4.10. Certificate status services

This chapter is specified in relevant CP.

## 4.11. End of subscription

This chapter is specified in relevant CP.

## 4.12. Key escrow and recovery

### 4.12.1. Key escrow and recovery police and practices

Penneo does not use key escrow services.

### 4.12.2. Session key encapsulation and recovery policy and practices

Penneo uses secure cryptographic modules and defined suppliers procedures for completion of the CAs keys during recovery. Parts of keys are encrypted and is not possible to transfer them in readable forms. The private key after activation never leaves the cryptographic environment.

# 5. Facility, Management, and Operational Controls

Penneo uses hardware and software for the all activities relating to fulfill trust and common trusted PKI services.

Facility, management and operational controls are concentrated on credibility and trustworthy of the all services provided to Penneo’s subscribers.

Security management guidelines are resulting from family of standards ISO/IEC 27001 resp. other standards and procedures required by EU regulations and law.

## 5.1. Physical security controls

Physicals security controls are performed in:

- Data centre rooms operated by third a party provider based on legal contracts and Service Level Agreement (SLA) between Penneo and the data centre provider;

- Public cloud provider where Penneo’s applications are hosted;
- Office locations of Penneo.

Penneo uses physically separated space in rented server rooms to host physical devices specifically designed for PKI infrastructures and data centre operations.

The data centre uses security perimeters and layers to protect areas that contain information and information processing facilities. Secure areas are protected by appropriate entry controls to help ensure that only authorized personnel are granted access.

The all conditions arising from the contract between Penneo and Cloud provider are fulfilled and security controls correspond to the contract.

### 5.1.1. Site location and constructions

Site location and constructions are physically protected and secured. The Computer center is strategically located to ensure they have power availability and connectivity.

Penneo’s office space shall be secured through appropriate measures. Access to Penneo’s office space shall not provide any direct access to internal or confidential information.

Office space does however present an asset that needs to be adequately protected for the access to PKI infrastructure, personnal devices and rooms.

Applications are installed to the cloud solution and use application system from other external company.

Penneo has ensures that appropriate physical  and environmental controls are in place around the devices issuing certificate.

Physical and environmental controls cover physical access control, perimeter security, natural disasters protection, fire safety, redundant power supply, disaster recovery and more.

### 5.1.2. Physical access

Penneo ensures that certificate issuing devices and other devices processing sensitive information are kept within secure areas that are protected by multiple appropriate entry barriers and security measures. This includes the following measures to secure the data centres:

- 24x7 security guards on site;
- Outer perimeter protection (fences, bollards, barriers);
- Outer and inner perimeters surveillance cameras;
- Alarm system (sound and visual) and infrared sensors covering the whole perimeter (in and around the building), which are monitored 24x365 by security personnel;
- Physical access is restricted using mantraps, biometric controls and badge access regulated by role-based access;
- Access control system records any entries or exits in the building, private rooms and other private spaces.

### 5.1.3. Power and air conditioning

Penneo ensures that data centres hosting certificate issuing devices are equipped with sufficient air conditioning and power supply in order to provide suitable conditions for operating devices, as well as reliable and resilient power infrastructure. This includes dual energy access points to the facility, diesel generators with sufficient fuel storage, UPS systems and various redundant elements in the distribution network throughout the premise.

For optimum performance, equipment is maintained and continuously monitored in a climate-controlled environment. The average room temperature and humidity level is controlled at a suitable level. Multiple air conditioning units provide redundant capacity. Down-flow cooling units help ensure maximum cooling of equipment.

### 5.1.4. Water exposures

Penneo ensures that data center facilities include water detection systems installed in areas that may be susceptible to leakage. The water detection alarms are relayed directly to the service center, as well as to the relevant local security and engineering personnel.

### 5.1.5. Fire prevention and protection

Penneo ensures that data centre facilities are protected against damage from fire using fireproof doors and walls and fire suppression systems.

Temperature and smoke/fire alarms, optical smoke detectors (under the raised floor and on the ceiling), connected to main fire panel (dedicated per zone) and smoke detection system under floor and overhead and gaseous fire suppression system.

### 5.1.6. Media Storage

Penneo ensures that devices are handled in accordance to the instructions and protected against theft, damage and unauthorised access.

### 5.1.7. Waste Disposal

Penneo ensures that devices are disposed in a secure way and data is wiped in an appropriate way prior to disposal.

### 5.1.8. Off-Site Backup

Penneo ensures that a backup procedure is in place in order to restore services in case of system failure. Penneo stores backup material at two separate locations in order to ensure that certificate issuing devices can be can become operational in case of a disruption. Other components operated from Penneo's could infrastructure are backed up at a second region.

## 5.2. Procedural controls

### 5.2.1. Trusted roles

Penneo has defined trusted roles to ensure that persons involved in the operations related to certificate issuing devices do so in a trusted capacity. Trusted roles are defined to prevent conflict of interests and that the Penneo's trusted service does not rely on a single person or that one person can single handedly operate the system.

The following trusted roles have been defined:

- Security Officers
- System Administrators
- System Operators
- System Auditors

### 5.2.2. Number of persons required per task

Penneo has implemented internal procedures and controls to ensure that no single trusted person shall be able to perform critical tasks alone. Critical tasks include CA key pair generation and generating a CRL.

### 5.2.3. Identification and authentication for each role

Penneo ensures that persons go through Penneo's hiring process to ensure the suitability and that the person possesses the required qualifications for a given role. Before a person is granted to access to certificate generating systems, the person must be formally appointed to a trusted role by the Security Manager.

The authentication to Penneo's trusted systems follows internal procedures and controls.

### 5.2.4. Roles requiring separation of duties

Penneo applies the need to know and least privilege principles to allocate access rights to users. Certificate generating services and other highly sensitive systems have dual control to ensure that no person can perform changes without the involvement of another trusted person.

## 5.3. Personal controls

### 5.3.1. Qualifications, experience, and clearance requirements

Penneo has defined and implemented a process for hiring that must be followed. The process ensures that the person is identified and fulfills the requirements needed to fill a certain tole. Before access is granted to Penneo's trust service, a person must be formally appointed.

### 5.3.2. Background check procedures

Penneo only appoints personnel who are considered trustworthy to a trusted role. A person must have been through Penneo's hiring process and a check of a persons criminal record must have been performed. When being appointed to a trusted role, the person much acknowledge the responsibility that comes with the trusted role and what requirements apply to the trust service.

### 5.3.3. Training requirements

Penneo ensures that all new employee complete an onboarding awareness training.

Penneo shall provide persons involved in the development, operations and maintenance of Penneo's trusted service with relevant training based on a trusted persons needs.

### 5.3.4. Retraining frequency and sequence

Areas that require a certain basic level of awareness on a continuous basis shall be updated at least annually.

As a minimum, all employees shall complete an annual update concerning Security, Compliance, GDPR and insider training regulations.

Trusted persons shall make sure they maintain skill levels necessary to fulfill the tasks related to trusted role to which they have been appointed.

### 5.3.5. Job rotation frequency and sequence

Penneo does not provide job rotation. Penneo shall ensure that the trust service operations are not affected by personnel changes within Penneo.

### 5.3.6. Sanctions for unauthorized actions

Penneo will evaluate violations of applicable policies and procedures on a case-by-case basis. Penneo's management will determine appropriate disciplinary actions where necessary.

### 5.3.7. Independent contractor requirements

Penneo does not engage independent contractors to operate its trust service components. Penneo may engage independent contractors to perform work related to the trust service. Penneo will at all times maintain the control and oversight of the trusted service.

### 5.3.8. Documentation supplied to personnel

All new employees go through an onboarding process when joining Penneo. During the onboarding the new Penneo is introduced to the organisation, Penneo's values, code of conduct and applicable policies, standards and legislation.

All existing Penneo’s employees must complete an annual awareness training that includes elements related to information security and data privacy.

## 5.4. Audit logging procedures

Penneo ensures that relevant activities concerning the operations of the trust service are captured via related audit logs. The integrity, availability and confidentiality of the data transmitted and stored are maintained during the collection of audit data to audit logs.

The audit system:

- guarantees the maintenance of audit data and the provision of sufficient space for audit data;
- the automatic non-rewriting of the audit file;
- the presentation of audit records to users in a suitable manner;
- the limited access to audit file for responsible employee only.

### 5.4.1. Types of events recorded

All relevant information concerning data issued and received by the Penneo in role of TSP are recorded for the purpose of ensuring continuity of the service and for the purpose of providing evidence in legal proceedings. Records will be made available as an evidence of the correct operation of the services for the purpose of legal proceedings. Records are maintained for the time period defined in document - Terms and conditions and after this period are archived.

Special events which are recorded are generation of CAs private keys - root CA keys and subordinates CA keys. The process takes place in accordance with the law and in advance prepared initialization process described in internal regulation.

All relevant information concerning data issued and received by Penneo in role of TSP are recorded for the purpose of ensuring continuity of the service and for the purpose of providing evidence in legal proceedings. Records will be made available as evidence of the correct operation of the services for the purpose of legal proceedings.

### 5.4.2. Frequency of processing log

Logs shall be regularly reviewed for the purpose of detecting suspicious activities.

### 5.4.3. Retention period for audit log

Audit logs records shall be kept for at least 10 years from the date of their creation.

Other event logs will not considered audit logs shall be retained based on internal requirements.

Audit logs will be made available to Qualified Auditors upon request.

### 5.4.4. Protection of audit log

The audit system is created and operated on the environment with sufficient capacity, without the possibility to use common access to stored data.

Logs are sent to a dedicated log server. Admins has read only access. Only the root account, which requires the approval from admins can access to logs.

### 5.4.5. Audit log backup procedures

Security Audit Log are logged to two different places, controlled by configuration of used software and hardware.

Backups of the databases used to store production data must be performed at regular intervals - at least every 24h.

Copies of logs are transferred to a secure environment and access is regulated to responsible persons only.

The steps for audit logs backup procedures are the same as during backups of others electronic information and medias.

### 5.4.6. Audit collection system (internal vs.external)

Audit log collection system is operated by Penneo and does not depend on external sources.

### 5.4.7. Notification to event-causing subject

No one who caused the incident is informed.

### 5.4.8. Vulnerability assessment

Penneo shall perform a risk assessment at least on an annual basis. Risk assessments shall follow the methodology as defined by the ISO 27005 standard.

Penneo shall performed vulnerability scans and penetration testing covering the trusted services including CAs.

The tests shall focus on internal and external threats towards the trust service and the information processes therein.

## 5.5. Records archival

Penneo shall archive records to establish the events that have taken place in relation to the issuance or certificates.

### 5.5.1. Types of records archived

Penneo archives especially:

- records from Root CA and subordinate CA’s initialization, including video recording;
- signed protocol from initializations ceremony;
- audit reports;
- evaluation of Penneo based on legal and law requirements;
- information from business contracts, initialization, cancellation, content of contracts;
- particular version of Platform programs;
- product and technical documentation, application software, version of applications and documents.

### 5.5.2. Retention period for archive

Root CA records and subordinates CA records are archived for the all time of PKI trust services which Penneo uses for business activities.

Audit logs are archived minimally for 10 years.

### 5.5.3. Protection of archive

Archive records are protected against modifications.

### 5.5.4 Archive backup procedures

Archive records are protected based on technical and object security. Inside internal documentation are described requirements for protection of archive records.

### 5.5.5 Requirements for time-stamping of records

In the cases of time stamp usage, Penneo uses electronic qualified time stamps for subscribers.

### 5.5.6 Archive collection system (internal or external)

Archiving system is Penneo internal.

### 5.5.7 Procedures to obtain and verify archive information

The information is kept and is located in the locations designated for this purpose and is accessible to:

- Penneo's employees, if required for their activities,
- authorized supervisory and control bodies and bodies active in criminal matters, if it is required by other standards.

## 5.6 Key changeover

Penneo distinguishes between several types of actions:

- common change of root CA keys - before expiration of valid certificate, minimally a year in advance has to be new ceremony of keys generation and issuing of the new root CA certificate (self-signed certificate).
- common change of subordinates CA keys - before expiration of valid certificate, minimally a year in advance has to be sent new certification application for subordinates CA;
- common keys change of electronic seal and time stamp certificate - before expiration of common and valid certificate - minimally 1 year before, is issued the new key pair and the new certificate;
- after suspicion of abuse of the private key - immediately after suspicion, is issued the new key pair and the new certificate,
- after possible technical problems - based on:
    - lower security of cryptographic algorithms,
    - length of keys,

    - new methods and improving of security,

is issued the new key pair and new certificate.

Upon expiration of CAs certificates the old ones has to be deleted and written protocol created. The back up and cryptographic environment has to be initialized.

Information about changes of CAs certificates has to published on Penneo's web pages in advance.

# 5.7. Compromise and disaster recovery

## 5.7.1 Incident and compromise handling procedures

Penneo established business continuity procedures and disaster recovery plans, which includes:

- procedures that solve incidents and compromise problems;
- business continuity management and disaster recovery policy;
- risk management policy.

Risk management is performed regularly and must be performed at least on an annual basis but should be updated whenever new relevant threats and vulnerabilities are identified. Hence, the risk management process is continuous.

The risk identification shall only take relevant risks into account. Risks considered negligible due to an extremely low probability of occurrence or extremely low potential impact will not be included for further analysis in as part of the risk assessment.

Special internal procedures addresses problems with:

- misusing of CA private key. Immediately actions have to be performed, as described in internal procedures;
- lost of necessary and needed data or misuse of private information;
- breach of security with impact on business of Penneo's;
- lost of documentation and detailed description of processes;
- breach of Penneo Platform or outages of used SW and HW.

Analysis and recovery processes have to be started.

### 5.7.2 Computing resources, software, and/or data are corrupted

Corruption of computing resources, software and data security are managed by internal procedures and resources. Service level agreements are concluded to agreement with suppliers.

### 5.7.3 Entity private key compromise procedures

In the case a root CA private key is compromised Penneo will:

- disconnect usage of automated Platform and cooperating PKI services for remote electronic signature, seal and time-stamp;
- revocation of the root CA certificate;
- revocation of subordinates CA certificates;
- revocation of all valid certificates issued by those CAs.

Immediately publish information on Penneo's web pages and revoked certificates are published in relating CRLs. Information about revocation activities has to send to all subscribers (based on agreements between Penneo's and subscribers).

All private key (including seal private key) and back-ups will be deleted and secure encryption environment initialised. About initialisation and private key destroying is written protocol signed and published.

In the case a subordinate CA private key is compromised Penneo will:

- immediately stop usage of the particular CA certificates and disconnect usage of automated Platform and cooperating particular CA service;
- revocation of the particular CA certificate by the Root CA and issuing of the new CRL;
- all subscribers will be informed about private key compromising and will be notified of the particular CA termination;
- revocation of  all certificates issued by the particular CA and issuing of the new CRL.

The particular CA private key and back-ups will be deleted and secure encryption environment initialized. About initialization and private key destroying is written protocol signed and published.

### 5.7.5 Business continuity capabilities after a disaster

Penneo uses hosting providers that have necessary measures in place to deal with unexpected events. Penneo manages business continuity capabilities and has internal procedures for reactions different scenarios.

## 5.8 CA or RA termination

### 5.8.1. CA termination

As a listed company, Penneo must be compliant with the danish “Traded Securities Act” (Værdipapirhandelsloven), which, under § 27, states that any information significant for the business' operations must be announced as quickly as possible. The Qualified Trust Service provided by Penneo through Penneo Signing is a significant asset to the company, meaning any significant changes must be announced to all shareholder and thus the public via a company announcement as soon as the information fulfils the requirements according to the Traded Securities Act. Adherence to the eIDAS requirement is ensured through Penneo’s status as a publicly listed company.

In addition, the CEO informs the supervisory board that has granted the right to act as a QTSP in addition to the announcement made in accordance to the Traded Securities Act.

Penneo has a documented process for company announcements and guidelines for information that is considered insider information and therefore must be announced to the market.

In case management decides on a new strategic direction, which leads to either Penneo choosing to terminate/cease operations or transferring the ownership of the operations to a third party, detailed plans is prepared to ensure successful execution.

The process of CA’s termination is managed based on internal termination documentations and internal plans.

Penneo ensures that the process of issuing of CRL is functional to the last valid certificate issued by Penneo’s PKI services.

All activities have to be time managed and user friendly to fulfil as much as possible every requests from subscribers.

### 5.8.2. RA termination

Process of RA termination is described within internal RA/IP documentation and the agreement between Penneo company and companies performing activities in roles of identity providers/Registration authorities.

# 6. Technical Security Controls

Penneo uses algorithms, method, length and all certificate life cycle’s best practices for creation of cryptographic keys.

## 6.1 Key pair generation and installation

Penneo uses algorithms, method, length and all certificate life cycle’s best practices for creation of cryptographic keys. Before modification of trusted modules testing and verification has to be performed and verified if capability and efficiency is not broken and declaration of cryptographic modules status is not changed.

The complex steps and procedures are part of internal documentation under Risk Management and Key management documentation.

> 📌 Please see chapter 6.1 of Appendix C for further information regarding Time Stamp Authority.

### 6.1.1 Key pair generation

Generating of the Root and the Subordinates CAs is performed in a secure area to prevent access to unauthorised persons and in accordance to pre-prepared internal detail procedures.

Several independent role are present during generation including:

- Information Security Manager
- External auditor (for Root CA)
- Internal Witness
- Root administrator of Penneo's PKI solution.
- Key Custodians

Keys generated for root CA are saved in the secure cryptographic module evaluated by Common Criteria certified level 5 (CC EAL 5).

Keys generated for subordinates CAs are saved in the secure cryptographic modules evaluated by Common Criteria certified level 4+ (CC EAL 4+).

The generation of key pairs for creating a remote electronic signature, electronic seal and electronic time stamp is performed in secure cryptographic modules, which are under the control of Penneo and fulfills the requirements of standards EN 419 221-5. Process is specified in corresponding Certificate policy.

A protocol/report is signed about generation of CAs key pairs by participating people after secure cryptographic modules initialization and keys generation. This protocol contains:

- name lists of participants - roles and responsibilities;
- date and time of the beginning and end of the keys generation - an accuracy of at least minutes;
- the place where it was generated;
- a description of the cryptographic modules, allowing unambiguous identification of this module;
- the date of the report;
- the handwritten signatures of all employees who generated the keys.

Penneo informs all relying parties to become aware of key changeover and publishes new the Certificate on their web pages. Common name of the Penneo's CAs certificates always contains the date of certificates generation.

Access to private keys is managed by responsible Penneo's employees. Activation of private keys which are stored in the secure cryptographic module is performed with the direct personal participation of at least two responsible Penneo's persons authorized by Penneo’s management and with smart card usage.

### 6.1.2 Private key delivery to subscriber

The chapter is specified in relevant CP.

📌 Please see chapter 6.1.2 of Appendix A for further information regarding Remote Electronic Signature.

### 6.1.3 Public key delivery to certificate issuer

The chapter is specified in relevant CP.

📌 Please see chapter 6.1.3 of Appendix A for further information regarding Remote Electronic Signature.

### 6.1.4 CA public key delivery to relying parties

CA’s public keys are part of CA certificates. Moreover it is possible to download from Penneo's web pages.

📌 Please see chapter 6.1.4 of Appendix A for further information regarding Remote Electronic Signature.

### 6.1.5 Key sizes

Key size of root CA is 4096 bits (RSA). The size of subordinate CA and TSA certificate is 2048 bits (RSA algorithm).

The size of subscribers keys is 2048 bits.

### 6.1.6 Public key parameters generation and quality checking

Parameters of keys are relevant to legal requests for eIDAS or EU and standards. Keys pair are generated based on the supplier’s delivered software and hardware generation tool and use mechanisms from the secure cryptographic modules.

Parameters for subscribers are defined in advance and implemented to the hardware cryptographic module which is responsible for the key pair generation.

### 6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Key usage purposes are defined in the certificate extension.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private keys are saved to secure cryptographic modules under Penneo's controls.

Subscribers use secure cryptographic modules that are implemented to infrastructure for automated Penneo’s Platform services.

### 6.2.1 Cryptographic module standards and controls

Standard for root CA cryptographic module is Common Criteria EAL 5 (CC-18-98209). A trusted channel and public key attestation allow remote key generation and certificate issuance. Advanced key management functions provide for key backup and escrow.

Generation of remote key pairs for subordinate CAs (for remote electronic signature, seal and time stamps) are performed in the secure cryptographic modules which are certified by Common Criteria as well (Common criteria level 4+).

Before initialisation procedure Penneo verifies if all secure cryptographic modules are sent in the original packaging and delivery is without complication or problems.

### 6.2.2 Private key (n out of m) multi-person control

The primary purpose of the key management is to maintain the assurance of confidentiality and integrity for any cryptographic key. It requires an efficient and secure key management process (key distribution, key exchange, key storage, key archive), which must be documented including its adhering roles and responsibilities. The secure and proper management of cryptographic keys is critical to the effective and proper use of encryption techniques.

The control over the private key is split using a n-of-m scheme for the private credentials. In such a scheme m defined and responsible employee are given a private credentials and n defined and responsible employee must come together to activate the private key.

Responsible employees do not perform a key life cycle operations without cooperation with other defined employee.

The subscriber’s private key is available to the subscriber during remote and automated remote signing process only.

### 6.2.3 Private key escrow

No escrow is used for private keys.

### 6.2.4 Private key backup

The secure cryptographic environment supports encrypted key backup and restore using mechanisms that can be set during cryptographic modules initialisation.

The mechanisms ensure that cryptographic material is never exposed in plain. Any media containing private key components used for loading cryptographic keys must be maintained in a secure location and accessible only to authorized employees. When removed from the secure storage location devices containing key components are for the minimum practical time necessary to complete the key-loading process.

The media upon which a component resides must be physically safeguarded at all times when removed from secure storage.

📌 Please see chapter 6.2.4 of Appendix A for further information regarding Remote Electronic Signature.

### 6.2.5 Private key archival

After the expiration of the private keys of the root certification authority or after Penneo’s PKI termination keys are destroyed, including the backups and the cryptographic module is initialised.

### 6.2.6 Private key transfer into or from a cryptographic module

Transferring of the keys should be minimised.

Transfer of the private key from back-up into cryptographic module is possible during recovery process. The private key leaves the cryptographic module in encrypted form based on backup and recovery processes specified in internal documentation only.

Authentication minimally two responsible Penneo's employees is necessary for recovery purposes based on internal processes. Written protocol is created and approved by Penneo's manager.

📌 Please see chapter 6.2.6 of Appendix A for further information regarding Remote Electronic Signature.

### 6.2.7 Private key storage on cryptographic module

Private keys of Penneo's PKI Services in unencrypted state are stored in activated and initialized hardware cryptographic modules that meet the requirements of the legislation for trust-building services.

For cryptographic module activation and initialization minimally two Penneo's responsible employees have to cooperate.

Subscribers private key is stored in the secure cryptographic module and after signature is the private key deleted.

### 6.2.8 Method of activating private key

The chapter is specified in relevant CP.

📌 Please see chapter 6.2.8 of Appendix A for further information regarding Remote Electronic Signature.

📌 Please see chapter 6.2.8 of Appendix C for further information regarding Time Stamp Authority.

### 6.2.9 Method of deactivating private key

The chapter is specified in relevant CP.

📌 Please see chapter 6.2.9 of Appendix A for further information regarding Remote Electronic Signature.

📌 Please see chapter 6.2.9 of Appendix C for further information regarding Time Stamp Authority.

### 6.2.10 Method of destroying private key

The chapter is specified in relevant CP.

📌 Please see chapter 6.2.10 of Appendix A for further information regarding Remote Electronic Signature.

📌 Please see chapter 6.2.10 of Appendix C for further information regarding Time Stamp Authority.

### 6.2.11 Cryptographic Module Rating

Penneo uses cryptographic modules for key pairs generation and storage of CAs private keys cryptograhic modules that meet the requirements of the legislation for trust-building services (The Common Criteria EAL 5 and 4+).

The cryptographic modules are implemented to Penneo's application and are certified for qualified remote electronic signature, seal and time stamp. The implementation and security is regularly monitored and checked.

## 6.3 Other aspects of key pair management

### 6.3.1 Public key archival

Penneo archives all issued certificates.

Retention period is a minimum of 10 years.

### 6.3.2 Certificate operational periods and key pair usage periods

The chapter is specified in relevant CP.

📌 Please see chapter 6.3.2. of Appendix A for further information regarding Remote Electronic Signature.

# 6.4 Activation data

## 6.4.1 Activation data generation and installation

Activation data is generated during initialisations processes of a particular secure cryptographic module and key pairs generation of the particular CA.

Activation data fulfils requirements of implemented and initialised secure cryptographic module (data length, data composition, data distribution).

## 6.4.2 Activation data protection

Activation data is distributed among responsible Penneo's employees in specified form only and are saved in secure places. Protection of activation data is described in internal documentation.

## 6.4.3 Other aspects of activation data

Activation data of CAs must not be transmitted or kept in an open form.

# 6.5 Computer security controls

## 6.5.1 Specific computer security technical requirements

The strategic goal of Penneo is to make information security as the integral part of the company culture.

The key strategic goals for the Penneo's business:

- Keep subscriber’s data confidential and safe;
- Deliver signed documents with the following verifiable properties:
  - The identity of the signer(s) can be uniquely established (Authenticity);
  - The signer(s) cannot deny having signed the document (non-repudiation);
  - The document can not be modified undetected (Integrity).

- Keep product reliability and availability as close to 100% as possible.

Penneo shall implement necessary technical and organizational security measures against sensitive data being accidentally or unlawfully destroyed, lost or impaired and against any unauthorized persons receiving the personal data, the personal data being abused or otherwise processed contrary to the legislation.

### 6.5.2 Computer security rating

- Family ITU-T
  - 501, X.509, X.520
- RFC
  - 2560, 3647, 5280, 6962
- ISO/IEC
  - 17021, 17065, 3166-1
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ETSI TS 119 495 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;  Part 1: Overview and common data structures.
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;  Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;  Part 3: Certificate profile for certificates issued to legal persons.
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;  Part 5: QC Statements.
- CEN/TS 419 261 Security requirements for trustworthy systems managing certificates and time-stamps.
- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.
- The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA),

# 6.6 Life cycle technical controls

## 6.6.1 System development controls

Penneo’s software is built from the ground up to be easy and painless to deploy and maintain.

Hardware used to operate to issue certificates are from trusted sources and checked and used according to manufacturing specifications.

All releases are done according to Penneo’s software development policy, which includes testing and reviews prior to release.

## 6.6.2 Security management controls

Verification of controls is performed regularly base on ISO/IEC 2700X principles and standards. In order to ensure compliance to policies and working instructions as defined within this ISMS continuous monitoring and auditing shall be implemented and tracked. The responsibility for the monitoring and auditing lies with the Information Security Manager who is the head of the Risk & Compliance department.

### 6.6.3 Life cycle security controls

Penneo uses during the all phases of development and implementation independent life-cycle security controls defined in internal documentation /and others standards.

Penneo performs clearly defined process for development of software from the storage and management of source code to deployment of releases and hot fixes.

## 6.7 Network security controls

Penneo uses layered security of its networks that operate the trust service.

Network segmentation is implemented to ensure that Penneo’s applications are logically separated and no access to other resources is permitted.

Penneo’s production environment is not directly accessible from the internet.

Penneo's root CA is not accessible to subscribers, the status is off-line. It is not connected to a network.

📌 Please see chapter 6.7 of Appendix A for further information regarding Remote Electronic Signature.

📌 Please see chapter 6.7 of Appendix B for further information regarding Remote Electronic Seal.

## 6.8 Time-stamping

Time-stamping is used during remote electronic signature and seal and the all data is verified and transferred by secure channel.

# 7. CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1. Certificate profiles

Certificate profile is specified in relevant CP.

## 7.2. CRL profiles

CRL profile is specified in relevant CP.

## 7.3. OCSP profiles

Not supported.

# 8. Compliance Audit and other Assessments

To ensure that Penneo's subscribers can trust Penneo and Penneo’s Trust Service is audited by a Qualified Auditor against the eIDAS regulation and applicable standards.

Penneo's trusted services requires implementation of corresponding legislation, standards and procedures to fulfil eIDAS regulation.

Penneo completes an ISAE 3000 audit on an annual basis to ensure internal controls designed and effective.

## 8.1 Frequency or circumstances of assessment

Compliance to eIDAS requirements is audited every two years by a Qualified Auditor.

An ISAE 3000 audit of internal processes and controls is completed every year by a Certified Public Accountant with Information Security expertise.

The Penneo is obliged to allow authorities who in accordance with the legislation in force at any time have access to the facilities of the subscribers and the Penneo or representatives who act on behalf of the authority access to the physical facilities of the Penneo against due identification and the prior signing of a non-disclosure declaration.

Penneo also performs internal audits.

## 8.2 Identity/qualifications of assessor

Penneo's Trust Service must be audited by a Qualified Auditor. The Qualified Auditor must be trained for auditing such services and be independent of from the audit subject. The Qualified Auditor must free from conflicts of interest.

Other auditors must be independent of Penneo and able to demonstrate the required expertise and experience in performing audit activities.

## 8.3 Assessor's relationship to assessed entity

External audits must be performed by a person/legal entity independent of Penneo.

Internal audits are performed by Penneo employees.

## 8.4 Topics covered by assessment

Audits must be completed in accordance to the standards applicable for the given audit and meet the requirements of the audit scheme applicable to the defined scope.

## 8.5 Actions taken as a result of deficiency

Should any deficiencies be identified through any audit activities, appropriate risk treatments must be initiated to remediate the deficiency.

The risk treatment plan is managed as part of the risk management process.

## 8.6 Communication of results

Results of audits must be reported to Penneo's Information Security Manager in writing for analysis. Deficiencies will be deal with as specified under 8.5.

Audit results will be shared with relevant stakeholders.

# 9. Other Business and Legal Matters

## 9.1 Fees

Fees are determined on a case by case basis to match the need of a person or organisation.

It is necessary to differ between a price list of identity provider functioning as registration authority and Services of Penneo.

In the case of cooperation agreement between Penneo and the Customers, fees can be defined in an attachment of the agreement.

### 9.1.1 Certificate issuance or renewal fees

Penneo issues Certificates as part of its Trust Service and may charge a fee for either issuance of Certificates or Subscription for use of service.

Applicable fees will be stated in the Terms of the contract between Penneo and Subscriber.

### 9.1.2 Certificate access fees

Certificates access is provided by Penneo free of charge.

### 9.1.3 Revocation or status information access fees

Revocation or status information access is free of charge.

### 9.1.4 Fees for other services

Fees for other services are defined in subscriber’s agreement.

### 9.1.5 Refund policy

It is not relevant for this document.

## 9.2 Financial responsibility

Penneo actively manages its finances through regular budget rounds in order to secure sufficient resources to keep operations running, as well as further develop the trust service. As a listed company, Penneo releases quarterly financial reports in addition to the annual report. Released financial reports are found on Penneo’s homepage.

### 9.2.1 Insurance coverage

Penneo has insurance coverage of its civil liability, with an insurance of professional civil liability that complies with the current regulation applicable and to maintain the customary and sound insurance level, including as a minimum product liability

insurance and general liability insurance to cover Penneo's liability in accordance with our customer agreements. In addition to this, Penneo is liable for product liability in accordance with the general rules of damages of Danish law. Penneo's liability for damages in each case, is limited to the amount which is paid out in accordance with Penneo's product liability insurance in force at any time.

Penneo declares that it has valid business risk insurance in such a way as to cover possible financial damages.

Penneo has arranged liability insurance for all employees for damages caused by the employer to the extent determined by the Danish Employment Insurance Law and the insurance company.

### 9.2.2 Other insurance and assets

Penneo declares that it has sufficient financial resources and other financial security for the provision of the Services with regard to the risk of liability for damage.

Detailed information on the assets of Penneo can be obtained from the Annual Report of Penneo published in the Commercial Register.

### 9.2.3 Insurance or warranty coverage for end-entities

Penneo does not provide this service.

## 9.3 Confidentiality of business information

### 9.3.1 Scope of confidential information

Confidential information is everything what is nor accessible on web pages of Penneo or available on print papers or is included inside contract between Penneo and subscribers.

Sensitive and confidential information include:

- private keys
- internal documents, rules and procedures
- personal data:
    - In order for the Platform to function in accordance with the Agreement the following personal data will be processed each time:

    - Name,
    - IP-address,
    - e-mail address,
    - Electronic ID informations, and
    - social security number, if this is chosen by the Data Controller for each document send for signing to a third party.
- Penneo’s business information;
- Subscriber’s business information.

Internal and confidential documents can be shared with external parties if an non-disclosure agreement (NDA) has been signed by wither the individually or with the company engaged by Penneo.

### 9.3.2 Information not within the scope of confidential information

Information outside of scope of confidential information are marked as Public and are available on contact places of Penneo.

### 9.3.3 Responsibility to protect confidential information

Every employee in the Penneo has a duty to maintain confidential information. It is exactly defined in internal documents.

## 9.4 Privacy of personal information

### 9.4.1 Privacy plan

Penneo ensures the protection of personal data for subscribers Penneo provides PKI trust services.

### 9.4.2 Information treated as private

Penneo provides personal information based on contract between Penneo and subscribers (regulated by the certification policies to subscribers, relying parties, as well as external auditors) for the purpose of a compliance audits, and for legal point of view in cases of criminal activities.

The Data Protection Officer is responsible for ensuring that operational processes within Penneo are in compliance to GDPR.

### 9.4.3 Information not deemed private

Information not deemed private is everything what is not marked as a private and content is not under protection based on legal acts.

A Data Privacy Statement outlining how Penneo handles personally identifiable information (PII) shall be written and made available to external stakeholders.

### 9.4.4 Responsibility to protect private information

The Data Protection Officer is responsible for ensuring that operational processes within Penneo are compliance to GDPR.

### 9.4.5 Notice and consent to use private information

Process is managed by legal acts and regulation. Data Processing Agreement (DPA), which forms part of the contract between Penneo and each respective customer shall be available. The DPA shall be available on Penneo's website.

### 9.4.6 Disclosure pursuant to judicial or administrative process

Compliance in regards to the EU regulation General Data Protection Regulation 2016/679 (GDPR). All processed information is accessible to authorities entitled by law in case when it is legally required.

### 9.4.7 Other information disclosure circumstances

All Penneo's employees shall ensure that his/her behaviour does not result in violations to the privacy of subscribers of Penneo and shall report any incidents including incidents involving PII.

## 9.5 Intellectual property rights

The Certificate Practice Statement, Certificate Policy, particular Practice Statements and other related documents are protected by the copyright of Penneo company and represent its significant know-how.

Penneo is also owner and holder of rights to the web based application (the structure, the content and particular steps) fulfilling procedures of the certification authorities and

trust services for electronic signature, time-stamp and electronic seal.

Penneo has intellectual property rights on issued certificates and used exclusively for electronic signature, time-stamp and seal. Key pairs are the property of the subscribers (legal or natural).

Penneo has a European trademark to the word Penneo, in relation to the function and services the Penneo Sign product provides.

## 9.6 Representations and warranties

Penneo guarantees that all requirements are met concerning to contracts, certificate policies and CPS, internal documents and procedures.

### 9.6.1 CA representations and warranties

Penneo manages all PKI trust services and provides qualified services in accordance with:

- relevant certification policy;
- certificate practices statement;
- relevant Practice statement,
- PKI, TSA disclosure agreement,
- internal operational documentation,
- applicable national and EU legislation and legal acts.

#### 9.6.1.1. Penneo’s Qualified Root CA

Penneo’s Root Certification Authority guarantees:

- that use CA's private keys only for issuing certificates to subordinate CAs;
- that issues a certificate conforming to the X.509 standard, internal documentation and procedures;
- that publishes the CP on Penneo’s web pages;
- that publishes Root CA’s certificate on Penneo’s web pages;
- that publishes CRLs regularly on Penneo’s web pages;

- in the case of Root CA’s certificate revocation informs subscribers and relying parties and publishes information about the certificate revocation.

#### 9.6.1.2. Penneo’s qualified Subordinate CA for electronic signature, seal and time-stamp.

Penneo’s qualified subordinates CAs (for electronic signature, seal and time-stamp) guarantees:

- that certificates issued to subscribers and for theirs needs meet the requirements required by the legislation for trust services and the relevant technical standards and norms
- publish the certification policies under which it issues certificates on its website
- in the case of Root CA’s certificate revocation informs subscribers and relying parties and publishes information about the certificate revocation;
- The Platform and technical infrastructure are in accordance with EU technical standards and EU legislative;
- that all needed information about issued certificates, CRL, CP and CPS are available on the Penneo’s web pages
- in the case of Subordinate CA’s certificate revocation informs subscribers and relying parties and publishes information about the certificate revocation.

All guarantees can be managed and fulfilled if the certificate holder and relying parties fulfil all conditions and obligations concerning to the CP and contract between Penneo and subscribers.

### 9.6.2 RA representations and warranties

Relation between Penneo and registration authorithies (identity providers) are managed via agreement. Registration authorities (IP) fulfil own business model which guarantees that identity of subscribers is verified and valid based on related legal conditions.

### 9.6.3 Subscriber representations and warranties

All information about representation and warranties are included to the agreement between Penneo and the subscriber.

Penneo rejects any other guarantee that is not enforceable under the laws, except the ones covered in section 9.6.2

Penneo rejects guarantees and applicable disclaimers in the documentation that connects the subscribers and relying third parties in certificates.

Penneo guarantees the subscriber, at least:

- Not factual errors in the information in the certificates, known or made by the Certification Authority.
- No factual errors in the information in the certificates, due to lack of due diligence of the certificate request or to its creation.
- The certificates comply with all the material requirements established in the Certification Practice Statement.

### 9.6.4 Relying party representations and warranties

Relying parties follow the CP according to which the Certificate was issued.

### 9.6.5 Representations and warranties of other participants

The Cloud provider and Computer centre are subjects directly involved in the operations of Penneo's PKI and The Platform services based on a contract concluded between providers and Penneo. They must fulfil conditions for continuous services of Penneo's Platform services.

Penneo uses Infrastructure as a service (IaaS) and Time synchronisation from Cloud provider. It provides access to networking features, computers, and data storage space. IaaS gives Penneo the highest level of flexibility and management control over your IT resources. Time synchronisation is described in particular CP for time-stamp. Relationship is managed through AWS Service terms contains chapters Penneo uses during providing trustworthy and qualified services.

Relationship between The computer centre and Penneo is managed through Service agreement containing SLA.

## 9.7 Disclaimers of warranties

Penneo provides guarantees in accordance with chapter 9.6.

## 9.8 Limitations of liability

Penneo uses qualified PKI services based on this CP and CPS. Penneo is not responsible for damages if subscribers and relying parties have not fulfilled the obligations required by the legal regulation.

Under contract with a customer, the Parties are liable for damages in accordance with the general rules of Danish Law with the limitations set out below, always provided that the limitations apply only if the loss is not attributable to gross negligence or willful intent on the part of the Party committing the tort.

Penneo disclaims liability for any indirect loss or consequential loss including, but not limited to, business interruption, loss of profits, loss of the Customer's Data and goodwill with the Customer.

Apart from product liability, the total amount of damages that the Customer can claim from Penneo in accordance with a customer agreement is limited to the smaller of the following:

- the total payment that Penneo has received from the Customer in accordance with their agreement at the time of the claim, or
- DKK 25,000 per claim per year.

## 9.9 Indemnities

Penneo only provides indemnity, in relation to possible data breaches. Herein either party is obligated to indemnify the other Party for expenses and use of resources in connection with the fulfilment of the obligations of a Party in relation to a supervisory authority or the data subject, as well as fines imposed by a supervisory authority or a court in so far as these are caused by a breach of the other Party.

## 9.10 Term and termination

The Agreement takes effect on the date on which the subscriber accepts this Agreement.

There is a period of commitment for access to the Platform (subscription) of 12 months as from the Time of Agreement.

Either Party may terminate the Agreement at a written notice of 3 months to expire at the end of the subscription period. If the Agreement is not terminated at the latest 3

months before the expiry of the subscription period, this gives rise to a new subscription period of 12 months.

The all conditions are described in document - Terms and Conditions - and are the part of the Agreement between Penneo and subscribers.

### 9.10.1 Term

This CP is valid based on information of CP publication and approval by Penneo’s manager. This document can be replaced by a new version of CP.

The Agreement between Penneo and subscribers takes effect on the date on which the subscriber accepts the Penneo Order Confirmation or otherwise accepts this Agreement ("Time of Commencement").

There is a period of commitment for access to the Platform (subscription) of 12 months as from the Time of Commencement.

More detail is possible to find out in document - Terms and Conditions.

### 9.10.2 Termination

Termination of this documentC can be made by Penneo’s manager decision in the case:

- of new version of trust services
- termination of PKI services

### 9.10.3 Effect of termination and survival

This document is valid to the end of validity of last issued certificates based on the CP.

## 9.11 Individual notices and communications with participants

The types of personal data and categories of data subjects that Penneo is to process for a subscriber as part of the service delivered is according to the Terms and  the Data Processing Agreement.

It is only the subscriber who decides which personal data is to be processed by Penneo and for which purposes this personal data may be processed.

Penneo processes the personal data only in accordance with documented instruction from the subscriber and in accordance with the Legislation in force at any time.

## 9.12 Amendments

Each Party may at any time with a reasonable prior written and reasoned notice demand amendments to the Data processing agreement if the amendment is necessary to observe the Legislation in force at any time.

The Data processing agreement may furthermore at any time be adjusted in accordance to the terms applicable for the service.

### 9.12.1 Procedure for amendment

See chapter of 1.5 of this document.

### 9.12.2 Notification mechanism and period

New version of this document will be published on Penneo's web pages.

### 9.12.3 Circumstances under which OID must be changed

OID's are published in this CP. OID's are based on international standard and are assigned to Penneo.

All OID's are mentioned in the certification policy and CPS issued by Penneo. The OID is included in related the certificate.

Circumstances for changing are based on Penneo's business changes, new version of certification policy which have some influence on certificate guarantees.

## 9.13 Dispute resolution provisions

The Parties (Penneo and subscribers) agree that the Agreement has been concluded in accordance with Danish law and that any dispute between the Parties must be settled in accordance with Danish law.

The Parties shall endeavour to settle disputes amicably through negotiation. If a dispute cannot be settled amicably, both Parties are entitled to bring the matter before the Copenhagen City Court in the first instance.

## 9.14 Governing law

Processes and activities are managed by Danish law.

## 9.15 Compliance with applicable law

Processes of Penneo's PKI services are in line with valid Danish regulations. Relationship between Penneo and the subscribers are signed and based on the agreement.

If a provision in the Agreement is declared illegal, invalid or unenforceable, the provision must in spite of this be enforced to the greatest extent possible in accordance with current legislation so that the subscribers original intention reflected. Such a provision does not affect the lawfulness or validity of other provisions.

Any provision in the agreement which according to its nature extends beyond the time when the Agreement ends in full or in part shall continue to apply and be binding on the subscribers.

## 9.16 Miscellaneous provisions

If a provision in the Agreement is declared illegal, invalid or unenforceable, the provision must in spite of this be enforced to the greatest extent possible in accordance with current legislation so that the subscribers original intention reflected. Such a provision does not affect the lawfulness or validity of other provisions.

Any provision in the agreement which according to its nature extends beyond the time when the Agreement ends in full or in part shall continue to apply and be binding on the subscribers.

### 9.16.1 Entire agreement

This document applies the trust service provided by Penneo where CAs under this document are being used.

### 9.16.2 Assignment

Not supported.

### 9.16.3 Severability

Not supported.

### 9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not supported.

### 9.16.5 Force Majeure

If Penneo cannot provide its services in accordance with the Agreement as a result of force majeure, Penneo cannot be held liable for losses on account of that and the Customer cannot terminate the Agreement with immediate effect. If the accessibility to the Service is essentially impossible due to force majeure and this lasts for more than 30 days, either Party may terminate the Agreement in writing with immediate effect but cannot in that connection advance any claims against the other Party.

Penneo must inform the Subscriber without undue delay if a force majeure situation arises. Force majeure is a matter on which Penneo has no influence and which Penneo cannot bypass with reasonable financial and practical measures. Force majeure is for example war, mobilisation, terrorist attack, failure/breakdown of public electricity supply, strike, fire, flood etc.

## 9.17 Other provisions

Chapter is not relevant for this document.