Certificate services

20.9.2024

Terms and conditions for the Validation service

General

The Digital and Population Data Services Agency (DVV) is an authority that maintains the personal data register and provides support services for electronic services, notary and legal recognition services, and guardianship services. Its task under the Act on the Population Information System and Certificate Services of the Digital and Population Data Services Agency (661/2009) is also to provide certified electronic services. The Agency was previously known as Population Register Centre until 31 December 2019. As of 1 December 2010, the Agency has also operated as the statutory certification authority for healthcare services and as of 1 April 2015, as the statutory certification authority for social welfare (Act on the Processing of Client Data in Healthcare and Social Welfare (703/2023), Act on Electronic Prescriptions (61/2007) and Act on the Population Information System and Certificate Services of the Digital and Population Data Services Agency (661/2009).

The Digital and Population Data Services Agency's operations as a provider of electronic identification service and qualified trust service provider are regulated by the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the "eIDAS Regulation").

The authenticity of electronic signatures, electronic seals and possible time stamps can be validated using the document Validation service by the Digital and Population Data Services Agency. The service currently allows you to validate PDF documents and ASiC files (e.g. Estonia's DigiDoc).

The service validates

- the technical validity and the legal status of the electronic signature or seal
- the validity and time of the time stamp
- whether the correct person or organisation has signed the document.

The service does not validate the accuracy of the document's content or, for example, whether the person or organisation that has signed it is eligible to use services.

The user of the Validation service may be a natural person or a proprietary system of the Digital and Population Data Services Agency's client. Natural persons will use the online interface of the Validation service manually. Electronically signed or sealed documents can be validated on the service page: https://dvv.fineid.fi/en/validation under *Validate document*. Clients' proprietary systems can be integrated with the Validation service, in which case the client's system automatically sends signed documents for validation.

Responsibilities of the Validation service user

The user is obligated to use the Validation service in accordance with these terms and the Digital and Population Data Services Agency's technical instructions.

The Validation service user is obliged to ensure that the user is entitled to submit the document in a third-party service that validates the electronic signature or seal and the time stamp. The Validation service user is responsible for any personal data in the document. The Digital and Population Data Services Agency cannot control the content of the user's document in the Validation service.

The Validation service can be used to validate the electronic signature or seal and the possible time stamp of predefined document types. The Validation service has not been audited for the processing of classified information.

Digital and Population Data Services Agency's liability

The Digital and Population Data Services Agency's liability for the provision of certificate services is determined under the valid cooperation contracts and pursuant to the provisions in the Tort Liability Act (412/1974). In addition, the requirements laid down in the Act on Strong Electronic Identification and Electronic Trust Services (617/2009) apply to the Digital and Population Data Services Agency.

The Digital and Population Data Services Agency is responsible for the security of the Validation service. The Digital and Population Data Services Agency is liable for the services that it has commissioned as if for its own.

Limitations of the Digital and Population Data Services Agency's liability

The maximum extent of the Digital and Population Data Services Agency's liability to the party relying on the Validation service is for the direct damage incurred if the damage is the result of the Digital and Population Data Service Agency's direct actions. The Digital and Population Data Services Agency shall not be liable for any indirect or consequential damage.

The Digital and Population Data Services Agency is not responsible for the functioning of public telecommunications or information networks, such as the internet, and it shall not be liable for situations in which the execution of an act is prevented due to the failure of a device or software used by the user or in cases where the Validation service is used in violation of its intended use.

The Digital and Population Data Services Agency is not responsible for damage caused by force majeure. Such an impediment may include strike, fire, war, rebellion, seizure, currency restrictions, action by an authority, legal provisions and official regulations, disturbances in public telecommunications, or other equally significant and unusual causes beyond the control of the Digital and Population Data Services Agency.

Notifying users of the processing of their data

The handling of private information in the certification authority's systems is subject to the provisions of the law on the handling of private information and the protection of privacy, including Act on the Population Information System and Certificate Services of the Digital and Population Data Services Agency (661/2009), EU's General Data Protection Regulation (679/2016) and the Data Protection Act (1050/2018). The handling of public information in the certification authority's systems is subject to the provisions of the Act on the Openness of Government Activities (621/1999). The certification authority ensures that

private information handled in its systems is protected against unauthorised access. Information can be disclosed to authorities on the basis of acts, decrees and associated regulations.

The processing of personal data in the Validation service is based on Article 6 section 1 e of the EU's General Data Protection Regulation: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The Validation service provided by the Digital and Population Data Services Agency supports electronic transactions and supplements electronic signatures and the seal service, provisions on which are laid down in Section 61 of the Act on the Population Information System and Certificate Services of the Digital and Population Data Services Agency (661/2009).

The certification authority has published specific policy rules under the Data Protection Act with regard to the certificate services.

Processing signed documents

The validation of electronic signatures and electronic seals shall be subject to temporary automatic processing of the signed document in plain text in a protected environment. The document will be deleted from the Validation service immediately after validation. Once the document has been deleted, the processing of personal data will also end.

General obligations and responsibilities of the processor

The user of the Validation service is the controller of the personal data contained in the documents. The Digital and Population Data Services Agency is the processor of personal data. Personal data are processed to validate electronic signatures in documents submitted to the Validation service. The processor shall process personal data in accordance with the terms and conditions for the Validation service.

The processor undertakes to ensure that all its personnel with the right to process personal data are committed to secrecy obligation or they are bound by an appropriate statutory secrecy obligation.

The processor of personal data agrees to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and to follow the controller's instructions and any updates to the controller's instructions.

The processor shall also implement measures to ensure that any natural person under the authority of the processor who has access to personal data only processes them in accordance with the terms of use.

The processor undertakes, without undue delay, to notify the controller, in accordance with these instructions, of all requests made by data subjects concerning the exercise of the data subject's rights under the applicable legislation.

The processor undertakes to assist the controller with appropriate technical and organisational measures to enable the controller to fulfil its obligation to respond to requests concerning the exercise of the data subject's rights. The processor understands that requests for the exercise of these rights may require its assistance in, for example, informing and communicating with the data subject, implementing the data subject's right of access, rectification or deleting personal data.

If necessary, the processor undertakes to assist the controller in carrying out a data protection impact assessment under the EU's General Data Protection Regulation, in any prior consultation and in obtaining a potential data protection certification. The controller has the right to charge reasonable labour costs in a manner agreed upon separately by the parties.

In principle, a processor may not transfer personal data outside the EU or EEA.

The processor shall make available to the controller all the information and material necessary to demonstrate compliance with the obligations described in these terms and conditions and shall allow and participate in audits, such as inspections, carried out by an auditor authorised by the controller.

Storing data and event log

An event log is kept of all events that take place in the Validation service. The Validation service logs the date of the validation request, the size of the document, a hash of the document, the results (TOTAL_PASSED, TOTAL_FAILED or INDETERMINE), the signature policy, the signature ID and the format.

The Validation service will not store the validated document after the validation. The event log does not contain the user's IP address or other personal data.

The Digital and Population Data Services Agency is responsible for the Validation service's event log and the disclosure of the data contained within. The log data can be used to retrospectively investigate the events that have taken place in the Validation service, if necessary.

The Digital and Population Data Services Agency will retain the event log for two (2) years after the validation conducted in the Validation service.

Privacy statement

The privacy statements related to the Digital and Population Data Services Agency's services and registers detail how, where and why personal data is processed. The certificate information system's statement referred to in the Data Protection Act is available at https://dvv.fi/en/privacy-statements.

Settling of disputes

Any disputes arising from the use of the Validation service that cannot be settled in negotiations between the Parties will be handled in the Helsinki District Court in Finnish. Within the central government, disputes are resolved through negotiations.