DVV / PAL 5.5.2026

Suomi.fi Data Exchange Layer Terms and Conditions of Use

Terms and Conditions of Use

5.5.2026

Version control

version no.	what has been done	date/person
1.0	The Terms and Conditions of Use for Suomi.fi Data Exchange Layer have been updated and the sections concerning the intermediary have been added	4.12.2023/AA
2.0	The Terms and Conditions of Use for Suomi.fi Data Exchange Layer have been updated regarding certificate applications.	5.5.2026/SP

Table of contents

Suomi.fi Data Exchange Layer Terms and Conditions of Use

1 General

These Terms and Conditions of Use shall apply to e-service support services, i.e., the Suomi.fi Data Exchange Layer, provided by the Digital and Population Data Services Agency (DVV). The Suomi.fi Data Exchange Layer offers the Customer Organisation a secure and consistent method of communication that enables the transfer and disclosure of data and provision of E-services. These Terms and Conditions of Use do not apply to the use of content and material available through the service.

The Customer Organisation utilising the Service shall accept these Terms and Conditions of Use as binding upon itself before it can access the Service. The Terms and Conditions of Use shall be accepted on behalf of the Customer Organisation by a named person, who has the authority to sign for the organisation in legal transactions. The Digital and Population Data Services Agency certificate services are utilised in the Service, for which a specific agreement is always required.

A third-party service accessed through the Suomi.fi Data Exchange Layer may only be used where there is a contractual or other similar relationship between the Service Provider and the user. The Digital and Population Data Services Agency does not act as the controller of data transmitted through Security Servers. The service provided by the Digital and Population Data Services Agency is limited to technical implementation. The Digital and Population Data Services Agency does not specify the terms and conditions related to the processing of data transmitted between the E-services connected to the Service, but the Customer Organisations agree on them as necessary. Acceptance of these terms and conditions does not exempt the Customer Organisation from the requirement to apply for a separate data permit or equivalent, or to make a separate agreement or equivalent with the Service Provider. Furthermore, acceptance of the terms and conditions does not exempt the Customer Organisation from their obligation to accept other special terms and conditions, such as the implementation of data security requirements, which may be imposed by a third party as a Service Provider. The Customer Organisation and/or Intermediary must take into account the processing times of these separate processes (if any) that have or may have a direct impact on when the service can actually be used.

2 Definitions

Time Stamping Authority (TSA) refers to a component maintained by a trusted entity that provides a certified time stamping service for the time stamping of messages sent through the Suomi.fi Data Exchange Layer. The Time Stamping Authority is part of the central servers and certificate solutions of the Suomi.fi Data Exchange Layer.

Subsystem refers to services (interfaces) connected to the Customer Organisation's Suomi.fi Data Exchange Layer that are published by the Customer Organisation in the Suomi.fi Data Exchange Layer. The Subsystem is used for the provision and utilisation of services and Information Systems in the Suomi.fi Data Exchange Layer. The Subsystem groups the services provided by the Customer Organisation through

the Suomi.fi Data Exchange Layer and enables the Intermediary to group similar clients.

Customer Organisation refers to an organisation that is connected the Suomi.fi Data Exchange Layer. A Customer Organisation may be a service user, a Service Provider or both. The Customer Organisation can use the Suomi.fi Data Exchange Layer independently or through the Intermediary. A Customer Organisation refers to a Customer Organisation referred to in section 2 of the Act on Common Administrative E-Service Support Services (Support Services Act), which, under the Act, means an *authority or other party performing a public task or a private entity using a support service*.

E-service refers to the e-service or Information System provided by a Customer Organisation to the End User. An E-service enables the use of electronic services by means of information and communications technology delivered by the Suomi.fi Data Exchange Layer.

DVV refers to the Digital and Population Data Services Agency. The Digital and Population Data Services Agency acts as the Service Producer of the Suomi.fi Data Exchange Layer.

Central Server refers to the central component of the Suomi.fi Data Exchange Layer that contains data on all Security Servers connected to the Suomi.fi Data Exchange Layer and the Customer Organisations using them. The functions and operation of the Central Server are the responsibility of the Service Producer or a party designated by it.

User refers to a person representing a Customer Organisation who uses the Suomi.fi Data Exchange Layer or a part of it on behalf of the Customer Organisation. The User may also be a person representing the Customer Organisation’s provider or some other person appointed by the Customer Organisation.

API Catalogue refers to a service directory that contains all organisations that are connected to the Suomi.fi Data Exchange Layer and services available through Subsystems, along with data related to them. Some of the data is automatically updated in the API Catalogue, but the Customer Organisation and/or the Intermediary are responsible for the supplementing of data.

Security Server refers to the Customer Organisation’s or Intermediary’s technical access point to the Suomi.fi Data Exchange Layer. Each system connected to the Suomi.fi Data Exchange Layer must have a Security Server through which all messages are sent to or received from the Suomi.fi Data Exchange Layer. The Security Server is responsible for numerous features, including the transmission of service calls between systems, the certificate handshaking process used for service calls, the encryption of communications and messages, logging, and access control.

End User refers to the end customer utilising the Customer Organisation's E-service, such as a citizen, an organisation, or a representative of an organisation. The Service Producer does not offer the Suomi.fi Data Exchange Layer to End Users.

Service refers to the Suomi.fi Data Exchange Layer, a technical solution produced and maintained by the Digital and Population Data Services Agency for data transfer between organisations. The Suomi.fi Data Exchange Layer is described in more detail as a service on the Service Management website or equivalent. The E-service used in these Terms and Conditions of Use does not refer to the Service or vice versa.

Service Management website refers to Suomi.fi Service Management, which offers the deployment, management, and support of Suomi.fi services to Customer Organisations and Intermediaries.

Service Provider refers to a Customer Organisation that offers its services or provides data to other organisations via the Suomi.fi Data Exchange Layer. An organisation can be a both service user and a Service Provider at the same time.

Service Producer refers to the Digital and Population Data Services Agency, which produces the Suomi.fi Data Exchange Layer.

Data Exchange Layer Operator is the party operating, maintaining, and providing technical support for the Suomi.fi Data Exchange Layer and acts on behalf of the Digital and Population Data Services Agency. In practice a Data Exchange Layer Operator maintains and administers the Service's Central Server environment and performs updating and service work.

Information System refers to the Customer Organisation's E-service or data repository connected to the Suomi.fi Data Exchange Layer. The Security Server is connected to the Information System to establish a connection with the Suomi.fi Data Exchange Layer. The term "Information System" refers to the information systems of both Service Providers and service users.

Intermediary refers to an operator that provides services related to the administrative or technical deployment or maintenance of the Suomi.fi Data Exchange Layer for Customer Organisations in accordance with an agreement between the Intermediary and Customer Organisation.

X-Road® refers to an open source data transmission solution that functions as part of the technical core of the Suomi.fi Data Exchange Layer. X-Road provides a standardised and secure way of transferring data between data resources and the Information Systems that utilise them. X-Road is developed by the Nordic Institute for Interoperability Solutions (NIIS).

3 Description of the Service

3.1 Suomi.fi Data Exchange Layer

The Suomi.fi Data Exchange Layer is a secure communication channel that organisations can use to transfer and disclose data contained in their data repositories to other Customer Organisations using the Suomi.fi Data Exchange Layer. The Data Exchange Layer is a decentralised services entity, in which mutually agreed operating models and data transmission protocols are observed with regard to agreements and message exchanges. The utilisation of services connected to the Suomi.fi Data Exchange Layer always takes place under an agreement or equivalent arrangement between the Service Provider and the service user.

The Service can be utilised by Customer Organisations

- when publishing information,
- when transmitting data and/or
- when receiving data available through the Service from another Customer Organisation.

The Suomi.fi service channel assumes responsibility for identifying organisations and their Information Systems. Traffic between Security Servers is encrypted and timestamped using certificates produced by the Digital and Population Data Services Agency's certificate service. The Security Servers check the authorisation of the Customer Organisation and its Information Systems to invite other services offered in the Suomi.fi Data Exchange Layer.

The Act on Common Administrative E-Service Support Services (571/2016) contains provisions on the Suomi.fi Data Exchange Layer, its development and production, and its provision to Customer Organisations. For a more detailed description of the service, its operating principles and enterprise architecture, see the Service Administration site.

With the link between Finland and Estonia created by the Suomi.fi Data Exchange Layer, it is technically possible to exchange electronic data between organisations that are connected to the countries' service channels. There is a contract between the Digital and Population Data Services Agency and Riigi Infosüsteemi Amet (RIA) regarding the transfer of data between the two countries. RIA (Information System Authority) is the Estonian state information agency that coordinates the development and administration of Estonia's information systems.

3.2 API Catalogue

The services offered through the Suomi.fi Data Exchange Layer and the connected organisations can be found in the API Catalogue, which comprises a centralised service directory. In addition, the API Catalogue contains service descriptions, descriptions of service interfaces, additional technical information, and the contact details of service maintenance providers.

Subsystem and interface information is updated automatically from the Security Servers to the API Catalogue every night. The production of the Subsystem and interface descriptions in the API Catalogue is the responsibility of the owner organisation of each Subsystem. The services presented in the API Catalogue can be implemented after this has been agreed upon with the Service Provider. The API Catalogue also makes it possible to apply for a user permit for services offered through the Suomi.fi Data Exchange Layer, if the Service Provider so separately desires.

4 Modifications in the Service and its terms and conditions

The Service Producer has the right to modify the content, operation and Terms and Conditions of Use of the Service in order to develop the Service or for some other reason that the Service Producer considers justified. For the sake of clarity, it is stated here that methods of agile development are applied to the Service.

The Service Producer is entitled to modify these Terms and Conditions of Use, any terms and conditions drawn up for Service users, and any other special terms of the Service after announcing such modifications on the Service Management site or equivalent. In addition, Customer Organisation contact persons shall be informed of modifications by e-mail.

If the modification made by the Service Producer to the Terms and Conditions of Use is minor, the Customer Organisation accept the modified Terms and Conditions of Use by continuing Service use. However, the Service Producer may also require that the modified Terms and Conditions of Use be approved separately in accordance with the process specified by the Service Producer. If the User does not accept the modified Terms and Conditions of Use, it must notify the Service Producer of this. In this case, the Service must be terminated by no later than when the modified Terms and Conditions of Use enter into force.

If the User does not comply with the current Terms and Conditions of Use and, for example, does not change its implementation to correspond to the modified Terms and Conditions of Use, the Digital and Population Data Services Agency, as a Service Producer, has the right to prevent the use of the service in the manner specified in section *12 Service Producer's right to prevent Service use*.

5 Deployment of the Service

5.1 Registration to the Service and accepting connecting

Use of the Service requires that the Customer Organisation and/or the Intermediary register to the Service Management or equivalent or register in another manner required by the Service Producer and provide the necessary data specified by the Service Producer. In case of modifications, the Customer Organisation and/or Intermediary details can be registered and submitted in the Service or in some other way as required by the Service Producer. The information, descriptions and/or

accounts provided will be passed on to Data Exchange Layer Operators, Service Providers and/or actors responsible for the technical aspects of Service provision.

An organisation with a Finnish business ID or an organisation that does not have a registration obligation under Finnish law (e.g. a private company) or is not otherwise assigned a Finnish business ID (e.g. a foundation or equivalent) may register to the service. Organisations registered in the EU/EEA may also register to the Service. Such organisations must be identified by one of the unique identifiers used by the register that registers organisation data in the EU/EEA. Organisations registered outside the EU/EEA may use the Service if the Service Producer makes an exception and gives its approval.

Organisations' possibilities of using the Service may be limited by legislation. The Act on Common Administrative E-Service Support Services (571/2016) contains provisions on organisations that may user the Service. The Service Producer will assess whether the organisation meets the requirements set in the legislation for connection. If the organisation is approved as a Customer Organisation for the Service, the Customer Organisation can be administratively connected to the Suomi.fi Data Exchange Layer.

Connecting to the Service requires the Customer Organisation to apply for a user permit or equivalent or join the Service administratively in another manner required by the Service Producer. If the Customer Organisation makes use of the Service through the Intermediary, the Intermediary shall assume similar obligations on behalf of the Customer Organisation. However, the Customer Organisation must approve the user permit application itself.

The Customer Organisation must accept these Terms and Conditions of Use. If the Customer Organisation makes use of the Service through an Intermediary, both the Intermediary and the Customer Organisation accept the Terms and Conditions of Use. The Customer Organisation, or an Intermediary representing it, apply for the certificates used on the Security Server. The Customer Organisation, or an Intermediary representing it, conclude an agreement on the use of the certificates with the Digital and Population Data Services Agency. In exceptional cases separately agreed between the Service Producer and the Customer Organisation, the certificates can be applied for on behalf of the Customer Organisation by the Data Exchange Layer Operator. Authorisation related to the certificates of the Data Exchange Layer Operator is granted through the submission of a user permit application or in another manner defined by the Service Producer. The Service Producer requires the applications for certificates at regular intervals or requires other measures be taken or enables the Customer Organisation and/or the Intermediary to employ an operating method by means of which the certificates are updated automatically. More detailed instructions on applying for and renewing certificates are available on the Service Management website or equivalent.

In addition, use of the Service requires registration and supplementing of one's own data in the API Catalogue or other measures required by the Service Producer to deploy the API Catalogue. In this respect, the Service Producer will provide more

detailed instructions in Service Management or equivalent. If the Customer Organisation acts as a Service Provider, the description of data is explained in greater detail in section *6.3 Rights and obligations of the Customer Organisation and the Intermediary*. A Customer Organisation and Intermediary (if any) registered outside the EU/EEA must describe the geographical location of the organisation as required by the Service Producer as well as the procedures related to the processing of data insofar as the processing of data outside the EU/EEA or possible processing of data outside the EU/EEA in connection with the processing of data for services provided or data transmitted through the Data Exchange Layer.

Registration for the Service, approval of joining and the necessary measures are described in more detail in Service Management or equivalent. In addition, the Service Producer may also provide more detailed instructions on its own initiative to the contact persons of the Customer Organisation that it has named by email. If the Customer Organisation makes use of the Service through the Intermediary, the Service Producer shall provide more detailed instructions only to the Intermediary's contact persons, who may then provide them to the Intermediary's own Customer Organisations, taking into account any limitations related to sharing the content of the more detailed instructions.

5.2 Service testing and starting production use of the Service

The Customer Organisation and/or Intermediary shall ensure that the Service is tested in a test environment prior to commencing with the production use of the Service. The testing and production environments are two separate environments used in the Service. Requests to join either are submitted by having the Customer Organisation or Intermediary fill in user permit applications or equivalent.

The two aforementioned Service environments are technically identical, excluding delays between the test and production environments due to version updates. The production environment is the official Service operating environment. After appropriate testing, the Service Producer or the Data Exchange Layer Operator shall grant the Customer Organisation and/or Intermediary approval to move to the production environment. The measures required for testing are described in the Service Management website or equivalent.

A Customer Organisation can bypass the testing phase stipulated in the Terms and Conditions of Use and connect directly to the production environment if an identical connection has previously been tested in accordance with the Terms and Conditions of Use. An identical connection means that a Customer Organisation and its Subsystem are connected to the Data Exchange Layer in exactly the same way as a previous connection, i.e., using the same tested Security Server and interfaces that are currently being used. A separate decision was issued on 29 March 2019 (Reg.no. VRK/1826/2019) regarding situations where bypassing testing is permitted. However, a Service Provider providing services or data through the Data Exchange Layer may also set different requirements for testing that the Customer Organisation and/or Intermediary must consider.

The Customer Organisation may initiate their Service use once the Service Producer has approved the Customer Organisation, granted its approval for use of the Service, and all measures required to start using the Service have been appropriately taken.

6 Parties to the Service and their tasks

6.1 Parties to the Service

The Digital and Population Data Services Agency (DVV) is responsible for providing and developing the Service. For its part, the Digital and Population Data Services Agency is responsible for ensuring the quality of the development work, national dissemination of the results, service provision of the centralised components and customer advice regarding the Data Exchange Layer. The Suomi.fi Data Exchange Layer uses X-Road technology developed by the Nordic Institute for Interoperability Solutions (NIIS). NIIS is responsible for the development of X-Road technology, a core component used by the Data Exchange Layer. The Digital and Population Data Services Agency has contracted the purchase of production services related to the Service from third parties, and with the use agreement outsourced responsibility for the continuity of Service provision and management of disruptions to the Data Exchange Layer Operator.

The Data Exchange Layer enables cross-border data exchange between Security Servers associated with the Estonian X-Tee implementation. This has been agreed upon in a separate agreement between the Digital and Population Data Services Agency and RIA. The Data Exchange Layer can enable the provision of services and the transfer of data between other solutions similar to the Data Exchange Layer.

Customer Organisations and/or Intermediaries utilise the Service for transferring and disclosing data as well as for providing and utilising E-services. Each Customer Organisation and Intermediary (if any) shall act as the controller for its own part with regard to the data they process or act on behalf of the controller as the processor of the data. These data processing activities take place as part of the use of the Service, but the Digital and Population Data Services Agency is not responsible for them as the controller or the data processor. The Digital and Population Data Services Agency acts as the controller as described in section *14.1 Processing of personal and other data and protection of privacy*.

6.2 Rights and obligations of the Service Producer

In addition to what is stipulated in legislation, the rights and obligations of the Service Producer are stipulated in these Terms and Conditions of Use.

The Service Producer is responsible for providing the Service and developing it. The Service Producer shall ensure that the Service meets legislative requirements. The Service Producer has the duty to fulfil its obligations, ensuring that the Service is provided with as little disruption as possible and with a high standard of information security. Requirements for the Service Producer's operations are monitored in

particular by the Act on Common Administrative E-Service Support Services (571/2016).

The Service Producer is responsible for providing Customer Organisations and Intermediaries with the necessary materials and instructions for connecting to the Service on the Service Management website or equivalent. In addition, the Service Producer is responsible for providing support in matters related to joining the test and production environment as well as in faults occurring in the production use of the Service in cases where there is a problem in the Security Server or between the Security Server and the Central Server. The Service Producer shall maintain the test and production environment and receive and process fault reports.

The Service Producer is responsible for procuring and maintaining Central Server and providing certificate services. The Service Producer shall offer the Customer Organisation a Security Server installation package as well as the attendant upgrades and support. The Service Producer shall also maintain the API Catalogue.

The Service Producer is entitled to receive from the Customer Organisation adequate and necessary information required by it in registration, connection, and other Service use phases. The Service Producer is entitled to receive from the Customer Organisation and/or the Intermediary adequate and necessary information required for investigating faults and errors or suspected misuse.

The Service Producer has the right to modify the content, operation and Terms and Conditions of Use of the Service in order to develop the Service or for some other reason that the Service Producer considers justified. For example, the Service Producer has the right to modify the functionalities or interfaces of the Service.

The Service Producer is entitled to freely share the administrative and technical descriptions of the Customer Organisation’s and Intermediary’s Subsystems and E-services stored in the API Catalogue. In addition, the Service Producer has the right to decide and change the open data license used in the publication of the aforementioned data in the API Catalogue.

The Service Producer is entitled to issue orders requiring the Customer Organisation to install updates that the Service Producer considers necessary on the Security Server, including information security updates or version upgrades. The Service Producer shall also set a deadline for installing such upgrades. The Customer Organisation or Intermediary shall be responsible for the costs incurred by installation, and the Intermediary and its Customer Organisations shall also mutually agree on the division of costs.

The Service Producer or the Data Exchange Layer Operator has the right to block Service access or remove the Customer Organisation’s or Intermediary’s Security Server if it is found to be unavailable for at least 60 days and it has not been taken into use within the 60-day deadline set by the Service Producer. If the Service Producer or the Data Exchange Layer Operator finds that the Security Server software is not up to date or the Security Server does not otherwise comply with the requirements stipulated in section *13 Information security and related requirements*,

the Service Producer or the Data Exchange Layer Operator shall have the right to block or remove such a Security Server. Additionally, if the certificates on the Security Server are expired, the Service shall be automatically disconnected. For more information on restricting the use of the Service, see section *12 Service Producer's right to prevent Service use*.

The Service Producer is entitled to collect data for the provision and development of the Service. The Service Producer may collect data on message traffic between Customer Organisation's and Intermediary's Security Servers and the Central Server as well as the traffic volume. However, this never means collecting the actual content processed on the Security Server. In addition, the Service Producer has the right to collect platform monitoring data for all Security Servers connected to the Service in the test and production environments to improve the quality and information security of the Service. The data collected includes the X-Road software version, the version number of the platform server operating system, the periods of validity of the Security Server certificates and energy consumption. The data is used for maintenance purposes and, with the aid of the data collected, Service maintenance can, for example, recommend that the Customer Organisation or Intermediary update the Security Server software to a newer version or notify them if the server certificates are about to expire. Platform monitoring data is not public information. In addition, the developer of X-Road technology, NIIS, has the right to collect operational data, for example, to improve background technology and information security.

The Service Producer may also collect other data necessary for the provision and development of the Service. Statistics can be generated from the collected data. The processing of data is described in more detail in the Service privacy policy on the Service Management website or equivalent.

The Service Producer shall have the right to perform scans between the Security Servers and Information Systems connected to them in order to, for example, improve the provision of the service and detect potential security threats. Based on this data, the Service Producer may recommend, for example, closing certain gates in order to improve the information security or equivalent of the Customer Organisation's and/or the Intermediary's information system entity. The Data Exchange Layer Operator shall provide the Customer Organisation and/or Intermediary with a list of gates that must be opened for the collection of monitoring data. The Service Producer shall also have the right to request that separately specified gates be opened temporarily, such as for the purpose of troubleshooting or incident management.

The Service Producer shall investigate fault situations and suspected misuse for their part and, if necessary, in cooperation with Customer Organisations and/or Intermediaries or other parties. The Service Producer is responsible for the systems, Central Servers, applications and interfaces of the Service as well as for investigating and coordinating fault situations. These tasks may be performed by a Data Exchange Layer Operator on behalf of the Service Producer.

When processing data for which it is responsible, the Service Producer has the obligation to ensure that information security and data protection are not put at risk.

6.3 Rights and obligations of the Customer Organisation and the Intermediary

In addition to what is stipulated in legislation, the rights and obligations of the Customer Organisation and Intermediary are stipulated in these Terms and Conditions of Use.

The Customer Organisation and Intermediary shall meet any obligations that they are responsible for fulfilling. The Customer Organisation and Intermediary shall comply with these Terms and Conditions of Use. The Customer Organisation and Intermediary are responsible for ensuring that the E-service connected to the Service also meets the legal requirements. The Customer Organisation and Intermediary are responsible for the activities of their Users.

The Customer Organisation and Intermediary are entitled to receive from the Service Producer adequate information required to connect to the Service and continue Service use after any modifications. The Customer Organisation and Intermediary are entitled to be informed of any services and interfaces available through the Suomi.fi Data Exchange Layer from the API Catalogue.

Before joining, Customer Organisation and Intermediary must provide the Service Producer with the required information on the organisation as well as the necessary personal and other data on the contact persons, who must be appointed. In addition, the Customer Organisation and Intermediary must implement the technical requirements for joining the Service, which are described on the Service Management website. If the Customer Organisation makes use of the Service through the Intermediary, the Intermediary will take care of similar obligations on behalf of its own Customer Organisation, depending on what has been agreed between the Customer Organisation and the Intermediary.

The Customer Organisation is obligated to describe its E-services and to publish or otherwise make available the necessary interface descriptions of the services provided through the Service to the Security Server it manages. If the confidentiality of the Customer Organisation or another justified reason requires, the data and descriptions of the E-service and its operating principles required by the Service Producer may be delivered directly to the Service Producer.

It is the responsibility of the Customer Organisation and Intermediary to provide a description of the organisation's data to the API Catalogue. The Customer Organisation is also obligated to provide information on their E-service and its operating principles. The Customer Organisation shall itself provide information on the services it provides, its interfaces and their deployment, and the organisation’s contact persons as well as inform users of the organisation’s services of any service outages. If the Customer Organisation makes use of the Service through the Intermediary, the Intermediary will take care of similar obligations on behalf of its own

Customer Organisation, depending on what has been agreed between the Customer Organisation and the Intermediary.

A Customer Organisation and Intermediary (if any) registered outside the EU/EEA must describe the geographical location of the organisation as required by the Service Producer as well as the procedures related to the processing of data insofar as the processing of data outside the EU/EEA or possible processing of data outside the EU/EEA in connection with the processing of data for services provided or data transmitted through the Data Exchange Layer.

The Customer Organisation and the Intermediary shall contribute to ensuring that the processing of data carried out through the Service on Security Servers is done in accordance with legal requirements. It is the responsibility of the Customer Organisation to ensure the processing of the data under its responsibility in accordance with section *14.1 Processing of personal and other data and protection of privacy* so that data security or data protection are not compromised. The Customer Organisation and Intermediary are also responsible for examining the quality of the data to be processed where necessary.

The Customer Organisation and Intermediary are responsible for the rights and grounds for disclosing data either on their own or under a separate agreement or equivalent arrangement when disclosing data to other Customer Organisations and/or Intermediaries for utilisation, processing or further disclosure through the Service. Data disclosure takes place in compliance with the provisions of the specific and general legislation applicable to the activities of each register authority or other party. Data may be disclosed by different means and for different purposes in compliance with the conditions and requirements set by the controller. A specific data access authorisation or equivalent may be required to disclose data. The Digital and Population Data Services Agency does not comment on the exchange of data between Security Servers.

As the party disclosing or receiving the data, the Customer Organisation must independently take care of the necessary permitting or equivalent as well as any necessary reports, such as on the purpose of the data with regard to the recipient and the party disclosing the data. If the disclosure of data requires a permit, agreement or equivalent, the Customer Organisation must ensure that a description of the process and its requirements for the recipient of the data is included in or linked to the API Catalogue. The Customer Organisation must also ensure that a description of where the permit or equivalent must be applied for or requested is found in the API Catalogue. If the Customer Organisation makes use of the Service through the Intermediary, the Intermediary will take care of similar obligations on behalf of its own Customer Organisation, depending on what has been agreed between the Customer Organisation and the Intermediary.

The Customer Organisation and Intermediary are responsible for ensuring the accuracy of their data. The Customer Organisation shall keep the data submitted to the Service Producer up to date and immediately provide any data that has changed through the Service Management website and API Catalogue or by other means

required by the Service Producer. If the Customer Organisation makes use of the Service through the Intermediary, the Intermediary will take care of similar obligations on behalf of its own Customer Organisation, depending on what has been agreed between the Customer Organisation and the Intermediary.

The Customer Organisation itself or together with the Intermediary defines the services and/or data it wishes to utilise through the Service. The Customer Organisation and/or Intermediary shall ensure that it has made or received the other necessary agreements, permits or equivalent on the basis of which it can utilise the services and/or data available through the Service.

A Customer Organisation that acts as a Service Provider ensures, for its part, that it provides its services and/or discloses its data in accordance with its own terms and conditions. A Customer Organisation that acts as a Service Provider can decide for itself whether an Intermediary can act as a representative of a Customer Organisation that utilises the services, for example, in any permit and contract processes. The Service Providers also decide independently whether services can be provided to a Customer Organisation that utilises an Intermediary or discloses data so that the receiving Security Server or Subsystem is used by multiple organisations.

The Service Producer is not responsible for applying for, granting, or checking the existence or conformity of agreements, permits or equivalent between Customer Organisations or for compliance with them. The Service Producer also refrains from commenting on the role and responsibilities of any Intermediary used in the relationship between Customer Organisations. The Customer Organisation shall comply with the conditions and requirements of any agreements, data access authorisation or equivalent set by third parties.

Each organisation joining the Data Exchange Layer must have either its own Security Server, a Security Server shared with another organisation or a Security Server acquired by other means. The procurement and maintenance of the Security servers and any costs incurred for these shall be the responsibility of the Customer Organisation. The Security server used by the Customer Organisation shall have the installation package offered by the Service Producer installed. The Customer Organisation is responsible for any Security servers, E-services or other Information System connected by them to the Service and any measures related to them. The Customer Organisation shall ensure that the necessary gates are opened and kept open as required by the Service Producer. The Customer Organisation is also obligated to close any gates opened for the purpose of resolving any disruptions and faults. The Customer Organisation shall implement any modifications required in the E-service or other Information System in case of modifications made to the Service. If the Customer Organisation makes use of the Service through the Intermediary, the Intermediary will take care of similar obligations on behalf of its own Customer Organisation, depending on what has been agreed between the Customer Organisation and the Intermediary.

The Customer Organisation shall investigate any faults and suspected misuse for their part and, if necessary, in cooperation with the Service Producer or other parties.

The Customer Organisation is responsible for investigating and coordinating any fault situations in the E-service and related systems. In addition, the Customer Organisation is responsible for the Security Server to the extent that the situation does not involve investigating and coordinating fault situations related to the installation package.

The Customer Organisation has a duty to notify the Service Producer if the Customer Organisation's E-service connection or the Security Server has been removed or is being removed from use completely.

6.4 Rights and obligations of the Intermediary

In addition to what is stated in the previous section, the Intermediary is also bound by the rights and obligations set out in this section. The Service Producer enables the Intermediary to provide its ICT services or platform services to its own Customer Organisations.

The Intermediary may act as an administrative Intermediary, i.e., apply for and manage, on behalf of the Customer Organisations, the user permits, or equivalent required by the Service Producer or Suomi.fi Data Exchange Layer. The Intermediary may also act as a technical Intermediary, in which case it may carry out the technical connection process of the Customer Organisation and the management of the Security Server as well as provide technical solutions for implementing or connecting the services. The technical Intermediary is required to apply for a user permit or equivalent, or to join the Service in another manner required by the Service Producer. The Intermediary may simultaneously act as a Service Provider or service user in the Service.

The Intermediary is entitled to agree on the role it will play on behalf of the Customer Organisation related to the Service as well as how the responsibilities concerning the Customer Organisation shall be divided between the Intermediary and Customer Organisation. The Service Producer does not comment on the type of agreement between the Intermediary and Customer Organisation.

Regardless of the role, the Intermediary must register for the Service Management or equivalent and provide the Service Producer with the required information on the organisation as well as the necessary personal and other data on the contact persons, who must be appointed. The technical Intermediary shall also submit a description of its organisation and the ICT services or equivalent it provides to the API Catalogue as required by the Service Producer. If the Intermediary acts as a Service Provider, it must submit a description of the E-services it offers to the API Catalogue as required by the Service Producer. The Intermediary shall keep the information required by the Service Producer up to date. If the Intermediary makes use of the Services or data provided through the Service itself, it shall be responsible for applying for the necessary user permits or equivalent.

More detailed instructions on Intermediaries are provided on the Service Management website or equivalent.

7 Ownership and other intellectual property rights to the Service

Unless otherwise stated, ownership and other intellectual property rights shall remain the property of their original owners.

The ownership and other intellectual property rights of the data in the registers they maintain and the services they provide shall belong to the Service Producer and the Customer Organisations, respectively.

These Terms and Conditions of Use do not alter the ownership and other intellectual property rights of the Service Producer or the Customer Organisation to computer programs and applications created and/or procured by them as well as the source codes, descriptions and instructions of such programs.

All material that the Service Producer or the Customer Organisation hand over to each other before or after Service use begins shall remain the property of the party that handed it over. However, the stipulations of this section shall not apply to nor prevent the handing over of log or other data related to the functioning of the Service to the Service Producer or Data Exchange Layer Operator, nor prevent the disclosure of material and data required for investigations. Provisions on the disclosure of information are also laid down in law.

The obligations and terms related to ownership and other intellectual property rights shall also remain valid after Service use or provision has been terminated.

Application component licenses are described in connection with Security Server distribution packages.

8 Right of the Customer Organisation and Intermediary to use the Service and the material contained in it

The Customer Organisation and the Intermediary are granted the right to use the Service in compliance with these Terms and Conditions of Use and any other special conditions, including requirements set by third parties, in their own internal use, and to utilise the Service when providing its E-services to End Users.

A Customer Organisation and the Intermediary are neither entitled to hand over material received through the Service to third parties if the material is not public, nor to provide the general public access to its content or any part thereof by distributing, transmitting, presenting or displaying it publicly, without the prior written consent of the Service Producer or other rightsholders.

9 Fees charged for the Service and distribution of costs

No fees or other payments are charged for the Service. The Service Producer shall not comment on the fees for E-services or data provided through the Service. For the time being, the certificates required to use the Service are provided free of charge. The prices of the certificates and the possibility of charging a fee for them will be reviewed annually.

The Service Producer shall be responsible for the general administration and technical support of the Service as well as bear the costs incurred for providing instructions and support for the deployment of the Service and for any other obligations.

The Customer Organisation and/or the Intermediary shall be responsible for setting up the required and appropriate connections, making any modifications required in their own systems, any other costs that may be incurred for connecting to the Service, and any other costs that may be incurred for obligations they may have.

10 Availability of the Service

While the Service Producer does not guarantee that the Service will be available continuously, every effort will be made to ensure its uninterrupted availability. For more details on availability of the Service, visit the Service Management website or equivalent.

For the sake of clarity, it is stated here that the Service Producer shall at all times have the right to interrupt Service provision because of a modification, an upgrade or a technical reason related to the Service, or due to repairs, installation or servicing of the telecommunications network or some other similar reason, or as a result of an information security threat or incident, or when this is required by legislation or an order issued by an authority.

11 Notification of outages and fault situations in Service provision

Outages and faults are reported on the Suomi.fi website or equivalent as well as to the contact persons of the Customer Organisation and/or Intermediary as soon as possible after the fault has been detected if this is possible technically or due to data protection and information security reasons.

This notification shall indicate the estimated duration of the outage or fault and, where possible, any protection measures that can be taken by the Customer Organisation, Intermediary and End User. In addition, the Service Producer shall notify the Customer Organisations, Intermediaries and End Users when the outage or fault has been rectified.

12 Service Producer's right to prevent Service use

The Service Producer shall reserve the right to refuse approval of a Customer Organisation or a User as a user of the Service with just cause. By its decision, the Service Producer may prohibit Service use or prevent it in full or in part from a private organisation, foundation, or trader pursuant to more detailed provisions in the Act on Common Administrative E-Service Support Services.

The Service Producer has the right to limit Service use for a justified reason, such as if the data protection or information security of the Service could be at risk without such limits in place, or if the data protection or information security of another service or register connected to the Service could be put at risk. In addition, the Service

Producer has the right to prevent a Customer Organisation, Intermediary or User from using the Service:

- if the Customer Organisation, Intermediary or User violates, or there is just cause to suspect that the Customer Organisation or Intermediary is in violation of these Terms and Conditions of Use, conditions related to utilising the Service set by other parties, good practices or the law
- if the Customer Organisation or Intermediary does not provide the required data or accounts
- if the Customer Organisation or Intermediary fails to comply with other legislation in its activities, or
- if the Customer Organisation, Intermediary or User utilises the Service in a manner that jeopardises the data protection or information security of the Service, or the data protection or information security of another service or register connected to the Service.

Additionally, if a Customer Organisation fails to take measures required by modifications made to the Service, the Service Producer has the right to prevent the Customer Organisation from using the Service until these measures have been appropriately completed. If a Customer Organisation fails to install Security Server updates by the given deadline, the Service Producer has the right to prevent the Customer Organisation from using the Service until these updates have been appropriately installed. Other consequences of failing to complete the required modifications by the set deadline may include the technical inability of the Customer Organisation to use the Service. If the Customer Organisation makes use of the Service through the Intermediary, the Intermediary will take care of similar obligations on behalf of its own Customer Organisation, depending on what has been agreed between the Customer Organisation and the Intermediary.

13 Information security and related requirements

In accordance with the Support Services Act (571/2016), managing and ensuring information security is an essential part of the Service. Providing for information security is the responsibility of both the Service Producer and Customer Organisations and Intermediaries.

Data of the lowest protection level (protection class IV) may be transferred through the Service without special arrangements. The requirements of the Finnish Transport and Communications Agency Traficom regarding the transfer of protection class IV data in data networks have been implemented and taken into consideration in the use of the Service. With regard to this, the Service Producer will define, for example, the length of encryption keys and certificates to be used in the Security Servers. In other cases, the Customer Organisation and the Service Provider shall agree upon the fulfilment of more stringent contractual and technical information security requirements and the transfer of, for example, protection level III data through the Service.

13.1 Service Producer's rights and obligations

The Service Producer is responsible for the information security of the Service in compliance with the valid legislation. With regard to the tasks that are the responsibility of the Service Producer, the valid information security practices of the Service Producer shall be observed.

The Service Producer may make Service use conditional on fulfilment of specific information security requirements applicable to the Customer Organisation, Intermediary and the E-service. The Service Producer has the right to tighten information security requirements. More stringent forms of the requirements also may have been imposed in agreements, data access authorisations or equivalent between a third party and the Customer Organisation.

The Service Producer or the Data Exchange Layer Operator appointed by them may perform remote administration actions and port scanning on a Security Server. The Service Producer has the right to require that the Customer Organisation and/or the Intermediary allow access for remote monitoring of Security Servers connected to the Service by the Service Producer or the Data Exchange Layer Operator appointed by them. To obtain a situational picture and for the purposes of vulnerability management, the Service Producer or the Data Exchange Layer Operator appointed by them will need, among other things, information on the Security Server's software version, packages installed in the Security Server operating system, and the services that are in use. The Service Producer or the Data Exchange Layer Operator appointed by them may carry out port scanning to verify that the Security Server environment has been hardened according to instructions and to check the status of information security updates for the purposes of vulnerability management.

If the Service Producer decides to implement vulnerability scans on the public interfaces of the Customer Organisation's E-service, the date of the vulnerability scans will be jointly agreed upon in order to ensure that they can be implemented without causing any harm to the use of the E-service.

The Service Producer has the right to publish information on the undisrupted operation of the Security Server in the API Catalogue or elsewhere on the basis of the Customer Organisations's or Intermediary's Security Server monitoring data.

If an Information System of the Service Producer used to provide the Service or an Information System of the Customer Organisation or Intermediary connected to the Service disrupts the functioning or information security of an Information System used to provide the Service or connected to the Service, the party responsible for the Information System causing disruption shall immediately take action to rectify the situation. If necessary, the Service Producer, Customer Organisation or Intermediary may disconnect their Information System from a system maintained by the other party.

The Service Producer shall immediately notify the Customer Organisations, Intermediaries and Users if the Service is targeted or threatened by a significant information security violation or other incident that prevents the functioning of the

Service, essentially interferes with it, or jeopardises information security. The Customer Organisations, Intermediaries and Users shall be notified of any information security incidents and threats observed as stated in section *11 Notification of outages and fault situations in Service provision*.

If the Service Producer finds this possible and necessary in individual cases, the Service Producer or Data Exchange Layer Operator shall notify the Customer Organisations and Intermediaries of any observed vulnerabilities, potential corrective measures and information security updates which are associated with the Service, or which otherwise have an effect on using the Service or the Security Servers.

13.2 Rights and obligations of the Customer Organisation and the Intermediary

The Customer Organisation and Intermediary shall accept the information security requirements set by the Service Producer and undertake to comply with them by accepting the Terms and Conditions of Use. The Customer Organisation and Intermediary shall accept the Service implementation as offered and assess its suitability in terms of any requirements applicable to its own activities.

The Customer Organisation and Intermediary are required to comply with good information security practices. The Customer Organisation and Intermediary are responsible for the information security of their Security Servers or security server solutions as well as their E-services and Information Systems.

The Customer Organisation and Intermediary using the Service are required to:

- ensure that their Information Systems have an appropriate standard of information security, monitor, and carry out information security updates
- report information security incidents as required by the Service Producer, and
- ensure the secure maintenance of the Security Server and the associated systems in terms of access rights, user IDs, backup copies and fault situation management. These are described in more detail on the Service Management website or equivalent.

With regard to Security Servers, the Customer Organisation and Intermediary shall ensure that:

- installations and configurations are completed according to the instructions issued by the Service Producer
- updates are appropriately installed on the Customer Organisation’s or Intermediary’s Security Server, and updates are made on a regular basis
- adequate arrangements are made for backup and recovery
- logs generated in the Customer Organisation systems and on the Security Server are appropriately filed and archived for the period specified in legislation or other requirements.

The Customer Organisation entitles the Service Producer to target scans on the public interfaces of the E-service of the Customer Organisation in order to detect any vulnerabilities in data protection or information security. The Customer Organisation undertakes to eliminate any significant vulnerabilities detected by a deadline set by the Service Producer. If the Customer Organisation does not rectify the detected vulnerabilities by the set deadline, the Service Producer shall be entitled to prevent use of the Service as stated in section *12 Service Producer's right to prevent Service use*. If the Customer Organisation makes use of the Service through the Intermediary, the Intermediary shall fulfil similar obligations on behalf of its own Customer Organisation, depending on what has been agreed between the Customer Organisation and the Intermediary.

If an Information System of the Service Producer used to provide the Service or an Information System of the Customer Organisation connected to the Service disrupts the functioning or information security of the Information System used to provide the Service or that is connected to the Service, the party responsible for the Information System causing the disruption shall immediately rectify the situation. If necessary, the Service Producer or the Customer Organisation may disconnect their Information System from a system maintained by the other party. If the Customer Organisation makes use of the Service through an Intermediary, the Intermediary shall fulfil similar obligations on behalf of the Customer Organisation.

Service Providers may require that the Customer Organisations meet information security requirements set by them in their agreements, data access authorisations or equivalent. These parties may set specific information security requirements applicable to the users of their services. The information security requirements applicable to Service Providers are determined on the basis of the information security requirements applicable to the service/system to be connected to the Service.

The Customer Organisation shall immediately notify the Service Producer or the Data Exchange Layer Operator authorised by the Service Producer if the Customer Organisation’s Information System connected to the Service, including the Security Server, is subjected to or threatened by a major security breach or other event that may jeopardise the information security or functioning of the Service or significantly disrupt it. The notification shall describe the content of the disruption or the threat, its estimated duration and, where possible, any protection measures. The Customer Organisation shall also notify the Service Producer when the disruption or threat is over. Additionally, the Customer Organisation shall notify the Service Producer of any vulnerabilities detected, any corrective measures to be taken and information security updates associated with Security Server installation packages. If the Customer Organisation makes use of the Service through the Intermediary, the Intermediary will take care of similar obligations on behalf of its own Customer Organisation, depending on what has been agreed between the Customer Organisation and the Intermediary.

14 Data processing and protection of privacy

14.1 Processing of personal and other data and protection of privacy

The Service Producer, Customer Organisation and Intermediary shall each provide for and ensure that personal and other data is processed appropriately, and that personal data is processed without putting information security or protection of privacy at risk. The Service Producer, Customer Organisation and Intermediary shall assume all the responsibilities of data controller in accordance with the General Data Protection Regulation (2016/679), and each of them must produce and publish the necessary notifications and bulletins related to their own processing of personal data.

The Service Producer processes personal data concerning the Service's customer data in the manner explained in greater detail in the Service privacy statement. Data on the Customer Organisations, Intermediaries and Users is saved in the registers of the Service in the manner explained in greater detail in the Service privacy statement. In addition, personal data is processed by the Customer Organisations and/or Intermediaries on their Security Servers and systems connected to them if personal data is processed through the Service. The Customer Organisation and/or Intermediary may also process personal data in the E-services.

The Service Producer processes personal data in its Service, in its customer and user register, and in its other registers, as explained in greater detail in the Service privacy statement. Data on the Customer Organisations, Intermediaries and Users is saved in the registers of the Service, as explained in greater detail in the Service privacy statement. The Service Producer does not process the personal data transferred through the Security Servers.

The Service Producer has the right to process and disclose personal data in compliance with the current regulations of the Data Protection Act and other legislation as well as in the manner explained in greater detail in the Service privacy statement. After termination of a customer relationship or Service provision, the data will be kept on file for the time period required to meet statutory obligations.

The Customer Organisation and Intermediary shall appropriately file and archive the event and log data generated in their systems and servers for the period stipulated in legislation or other requirements.

14.2 Cookies

Cookies are used in the Service for both persons identified on the Service Management website and those logged in to the API Catalogue. The processing of data is described in more detail in the privacy statement.

15 Customer Organisation’s hardware, software and connections

The Customer Organisation shall be responsible for procuring the hardware, software and network connections required to use the Service, ensuring their function, maintaining them, and the costs incurred for them. The Customer Organisation shall also be responsible for ensuring that the hardware, software and connections do not interfere or otherwise disrupt the Service or other users.

16 Service Producer’s liability and limitation of liability

The Service Producer's liability is exclusively limited to the Service and the integrity and correctness of the data processed and offered in the Service to the extent that it is processed in the Service or disclosed through the Service, and to the extent that the Service Producer is liable for the systems and servers used to process data or to disclose it. The limitation of liability does not apply to situations where losses are incurred as a result of the Service Producer’s intentional act or gross negligence.

The Service Producer’s liability is limited to the functioning of the installation component offered for Security Servers and the functioning and maintenance of the Service’s Central Server. The Service Producer shall be responsible for the data needed to provide the Service on the Central Server. This includes, for example, the data required to route data communications between Security Servers specified by Customer Organisations and/or Intermediaries, such as the location of the Security Server.

The Service Producer is liable for the quality and cost-effectiveness of the Service and for ensuring that the Service is generally suitable for its purpose, performs well, and is reliable and as user-friendly and accessible as possible.

The Service Producer is responsible for the accuracy of the combined data required to provide the Service as well as for the information security of the data processed in the Service to the extent that the data processing is under Service Producer’s liability.

The Service Producer shall ensure that the Service provided by it is designed, built and maintained so that:

- the Service provided offers a good standard of technical quality and information security
- it is tolerant to normal and anticipated external disruptions and information security threats
- its performance, usability, quality and reliability are monitored
- any significant information security violations and threats targeted at it as well as any faults and disruptions that significantly undermine its functionality can be detected and corrected, and

- the modifications made in it do not cause unreasonable disruptions to the Customer Organisation’s E-service that utilises the Service or to other tasks performed using the Service.

The Service Producer shall not be liable to the Customer Organisation, Intermediary or a third party for:

- any errors made by Service Providers or other third parties
- the applicability and suitability of the Service for any special needs of the Customer Organisation, Intermediary or the E-service
- errors or losses caused by the use of the Service in the E-service or the use, interpretation or abuse of the data contained in the Service in the E-service, or the corruption or losses of data in the E-service
- any action that violates the Terms and Conditions of Use or the legislation related to the E-service, and the damages incurred
- temporary malfunctions that prevent use of the Service, outages due to service or installation work of the Service for which advance notification has been given, or outages due to installations or repairs that are critical to the functionality and information security of the Service, or
- technical faults beyond the Service Producer's control or any outages of the telecommunications network or the Internet.

The Security Server of the Customer Organisation or Intermediary and the management and information security of the Information Systems connected to it are the responsibility of the Customer Organisation or Intermediary, as described in section *13 Information security and related requirements*. The Service Producer shall not be liable for any information security incidents, data leaks or operational disruptions resulting from the maintenance or use of the Service's Security Servers by the Customer Organisation or Intermediary.

An essential part of the Service is the use of connections to the Security Servers of third parties, including Security Servers provided by the Intermediary and the E-services provided by a third party. The Terms and Conditions of Use and other terms of the third party in question shall apply to such third-party servers and services. The Service Producer shall in no part be liable for losses incurred for such third-party servers or services, their functionality or use, or otherwise. The Service Producer shall also not be liable for the information security, data protection or contents of such third-party servers or services.

17 Non-disclosure and confidentiality

The Service Producer applies the provisions of the Act on the Openness of Government Activities (621/1999) in its activities. According to the Act on the Openness of Government Activities, official documents shall be in the public domain, unless otherwise provided.

All material concerning the business or technical solutions of the Service Producer, Customer Organisation, or any subcontractors they use that is disclosed in connection with the Service shall be deemed secret and may not be disclosed to third parties unless otherwise agreed or required. When providing information on the Service, the Service Producer and the Customer Organisation shall mark any

documents or sections therein that are secret, also in the material of any subcontractors used.

Any documents and other material handed over in connection with Service provision and information related to them that has been marked as secret or which otherwise, based on the context, may be deemed secret, are covered by the stipulations on business secrets and shall be kept confidential and secret. This also applies to information obtained/received by the Service Producer, Customer Organisation or Intermediary that they knew to be secret or should have known was secret, or information that the other party has indicated as being secret.

The Service Producer and the Customer Organisation shall explain to their personnel and any subcontractors as to which data material generated in the course of the cooperation between the Service Producer and Customer Organisation and/or Intermediary or otherwise processed in connection with the Service, is confidential. The Service Producer and Customer Organisation shall also explain how the secrecy and confidentiality of said data material should be secured and arranged in practice.

The non-disclosure obligation shall also remain valid after Service provision or utilisation has ended.

The non-disclosure obligation referred to in this section does not apply to material and data that are required to be published as part of the Service or its use.

The Service Producer, Customer Organisation and Intermediary have the right to publish information on their activities in an ordinary and general way without violating the non-disclosure conditions defined in this chapter.

The duty of non-disclosure shall not apply to information that is publicly available or that has become known to a party legally through a third party without a non-disclosure obligation being applied.

18 Liability for damages

The Service Producer shall not be liable to pay compensation for any indirect damages incurred by a Customer Organisation, User or End User in the course of using the Service. The Service Producer shall be liable for any direct damages incurred by a Customer Organisation, Intermediary, User or End User, if such damages were caused by the wilful conduct or gross negligence of the Service Producer.

If the Service Producer is obliged to pay compensation to a third party as a result of the activities of an E-service, Customer Organisation or Intermediary, the Customer Organisation or Intermediary shall compensate the Service Producer in full for any compensation paid by the Service Producer to a third party.

19 Force majeure

Cases of force majeure shall release the Service Producer from any obligations related to the Service if it prevents any performance related to the Service or makes it

unreasonably difficult. For example, a force majeure event may be a war, insurgency, civil unrest, compulsory acquisition or confiscation by an authority for a public need or another order, a strike or a work stoppage, a natural disaster including an earthquake or a flood, interruption in public traffic or energy supply, a disruption in energy supply, shortage of raw materials or accessories, a cable fault or other data communication outage caused by or within the control of a third party, or other reason that was not known in advance and that could not reasonably have been anticipated.

Where possible, the Service Producer shall issue a notification of a force majeure event on its website, the Service Management website as well as to Customer Organisation and/or Intermediary contact persons by email immediately upon observing such an event.

20 Monitoring and control

The Service Producer shall monitor and control Service use as well as the implementation of information security and data protection and the legality of data processing in the utilisation of the Service.

For its part, the Customer Organisation and Intermediary shall control the implementation of information security and data protection and the legality of data processing. The Customer Organisation and Intermediary shall appoint a person responsible for information security and data protection if so required by the Service Producer, and ensure that personnel using the Service receive adequate information security training.

In order to enable ex post control, event and log data on disclosures and other processing of data shall be kept. The Service Producer shall maintain specifically defined event and log data on the Service. The storage of log data is described in greater detail in the privacy statement, which can be viewed on the Service Management website or equivalent.

The Customer Organisation and/or Intermediary shall keep a record of any event and log data that are required by the Service or a third party. The event and log data are based on identified Customer Organisations and Users as well as other information on data processing. If there is cause to suspect abuses, the event and log data make it possible to investigate which party has processed the data. The Service Producer has the right to obtain any information on Service use it requires from a Customer Organisation, Intermediary or a User by the deadline it sets.

21 Reporting

The Service Producer shall monitor quality deviations, outages and fault situations as well as information security and data protection incidents in the Service and the implementation of repairs associated with them, and report on them to different parties. The Service Producer shall report the aforementioned issues and Service development to the Customer Organisations and Intermediaries on the Service Management website or otherwise. In addition, the Service Producer or NIIS may

collect operational data on, for example, the energy consumption of Security Servers, and utilise this data in developing the Service.

22 Auditing of the Service

The service may be audited by the Ministry of Finance, the Finnish Transport and Communications Agency Traficom, another party that audits the Service Producer's activities, or a party that the Service Producer has contracted to conduct an audit. Customer Organisations or Intermediaries shall not be entitled to audit the Service or inspect it.

The Service is based originally on the Estonian X-Road product whose source code has been audited by the Finnish Communications Regulatory Authority. NIIS is nowadays responsible for the development of X-Road technology, a core component used by the Service. Efforts to develop the Service further will be audited in connection with application development and before they are introduced in productive use.

23 Transfer of rights and obligations

A Customer Organisation or Intermediary shall not be entitled to transfer the right to use the Service, or the rights and obligations associated with it to a third party without first notifying and gaining the express consent of the Service Producer. If an organisation wishes to transfer its obligation to use the Service, it shall be done in accordance with the Service Producer's instructions, which are described on the Service Management website or equivalent.

A Customer Organisation that is part of the central government shall, however, be entitled to transfer the right to use the Service and the associated rights and obligations, fully or in part, to another central government unit, to which some of the Customer Organisation’s tasks are to be transferred. Written notification of this transfer shall be given to the Service Producer in advance.

The Service Producer shall be entitled to transfer the right to provide the Service and the associated rights and obligations fully or in part to another central government unit to which some of the Service Producer’s tasks may be transferred.

24 Termination of the Service

When making a decision on termination of the Service, statutory obligations shall be taken into consideration.

A Customer Organisation has the right to terminate use of the Service at any time without giving a reason. The Customer Organisation may deactivate or terminate use of the Service as required by the Service Producer. For more details on terminating use of the Service, visit the Service Management website or equivalent.

The Intermediary has the right to terminate use of the Service at any time without giving a reason. However, termination shall be done in accordance with the agreements concluded with its own Customer Organisations. An Intermediary may

deactivate or terminate use of the Service as required by the Service Producer, in accordance with agreements concluded with its own Customer Organisations. For more details on terminating use of the Service, visit the Service Management website or equivalent.

The Service Producer has the right to terminate Service provision fully or in part for a particularly weighty reason. The Service Producer may close down or suspend the Service if there is reason to suspect that the information security of the Service is under threat or that the functionality of the Service does not comply with the requirements.

The Service Producer also has the right to terminate Service provision to a certain Customer Organisation or Intermediary or to withdraw the user rights of a certain User on grounds set out in the section *12 Service Producer's right to prevent Service use*, or if there is justified reason to suspect other misuse. Service provision may be terminated, or a user right withdrawn with immediate effect. If the Service Producer finds that immediate termination is not necessary, it will give written advance notification of the termination and its grounds.

The Service Producer shall not be liable for any loss of income or other damages incurred by termination of Service use or provision to Customer Organisations, Intermediaries or other parties.

25 Applicable law and resolution of disputes

Finnish law shall be applied to the Service, excluding provisions on the conflict of laws.

The Service Producer’s decisions related to registration, approval of Service use and preventing Service use are administrative decisions, and any disputes associated with these shall be resolved in an appeal procedure. Claims for a revised decision concerning decisions made by the Service Producer may be addressed to the Service Producer. Claims for a revised decision must be made by means of a written claim for a revised decision. A decision issued on a claim for a revised decision may be appealed against. This may be done by lodging a written appeal with the Helsinki Administrative Court.

Instructions for claiming a revised decision and appeal instructions

Every effort shall in the first instance be made to resolve any other disputes by negotiations between the parties.

Legislation or terms and conditions shall be applied to the contractual relationships and Terms and Conditions of Use between a Customer Organisation or Intermediary and another authority, Service Provider or third party according to what has been specifically provided or agreed in each case.

Disputes between a Customer Organisation or Intermediary and another authority, Service Provider or third party shall be resolved according to what has been specifically provided or agreed in each case.