Terms of use of Suomi.fi e-Identification

Terms of use for the Client Organisation

01 April 2026

Contents

Terms of use of Suomi.fi e-Identification

Terms of use for the Client Organisation

1 General

These Terms of Use shall apply to e-Service support Services, i.e. the Suomi.fi e-Identification, provided by the Digital and Population Data Services Agency. Suomi.fi e-Identification provides E-Services with an identification service that allows End Users to use services electronically.

The general terms of use also apply to the use of the content and material available through the Service unless specifically otherwise stated or agreed.

The Client Organisation utilising the Service shall accept these Terms of Use as binding upon itself before it can access the Service. The Terms of Use shall be accepted on behalf of the Client Organisation by a person who has the right to sign for the organisation in legal transactions.

In addition to accepting these terms of use, the Client Organisation may need to apply for a separate access licence or similar from the Data Producer. In addition to accepting these terms of use, the Client Organisation may be required to accept other special terms of the Data Producer. These special terms of use may be connected to e.g. compliance with information security requirements. The service utilises data retrieved from the population information system and data from the producers of Identification Tokens. Identification data may also be retrieved from other registers.

2 Definitions

E-service refers to the Client Organisation’s electronic service that is linked to the Service.

Access licence refers to an administrative decision by the Digital and Population Data Services Agency on the Client Organisation’s permission to use the Service.

Client organisation refers to the organisation that uses and utilises the Service. Legislation sets restrictions to the extent to which organisations can use and utilise the Service.

User refers to a person representing the Client Organisation who, on behalf of the Client Organisation, uses the Service or its part, such as the management interface, and whose assigned role corresponds to a user role specified in the Service. The User may also be a person who represents the Client Organisation’s provider or another person appointed by the Client Organisation.

End User refers to the end customer using the Service, such as a citizen. The End User may also be an EU citizen.

Service refers to Suomi.fi e-Identification, which is a service supporting the use of electronic services and is produced and maintained by the Digital and Population Data Services Agency.

Service Management website refers to the service utilised in the management and activation of the Service that enables self-service for the Client Organisation. The management of service settings is implemented as part of the features of the Service Management website.

Service Provider refers to the Digital and Population Data Services Agency, which is the party responsible for producing the service.

Suomi.fi e-Identification enables End Users to electronically identify themselves when using online services and allows single sign-on between E-services.

Suomi.fi for Service Developers website is the website maintained by the Finnish Digital Agency that provides the guidelines, solutions, and good practices for the use of the Finnish Digital Agency's electronic services for Suomi.fi's Client Organisations.

Data Producer refers to the register authorities or other parties that disclose data to the Service for use or processing, or for further disclosure to the E-service. The provisions of special and general legislation that are applied to the activities of each registration authority or other party shall be applied in regard to data disclosure. Data may be disclosed by different means and for different purposes in compliance with the conditions and requirements set by each Data Producer. A specific data permit or equivalent may be required to disclose data.

Data permit refers to the administrative decision made by an official in the Population Information System regarding the disclosure of data from the population information system. This administrative decision is called a data permit and it is made on the basis of a data disclosure application, i.e. the initiation of a case.

Identification data refers to the data that the E-service receives from the Service when a user signs on. Identification data may be retrieved from the information systems of both the identification token provider and the Data Producer.

Identification token refers to a list, device, software, or procedure that enables the End User to use Suomi.fi e-identification.

Producer of an Identification token refers to the organisation that provides the Identification token, such as a bank, mobile operator, or the Finnish Digital Agency.

Intermediary refers to the technical operator which is the primary contact to the Digital and Population Data Services Agency in regard to adding permit holders to data permits. The intermediary may be an operator in the public or private sector which, however, is not granted an access licence to the Service.

3 Service description

Suomi.fi e-identification is an identification service that uses strong identification to identify natural persons when they use electronic public administration services together with a service by such an identification service provider as referred to in the Act on Strong Electronic Identification and Electronic Trust Services (617/2009), and that manages the identification process as well as discloses the specified identifying data on the person from the registers of Data Producers to the Client Organisation. The service also provides other identification services and compilation and administration services related to identification which may use identification methods other than strong electronic identification as referred to in the Act on Strong Electronic Identification and Electronic Trust Services.

Suomi.fi e-Identification allows users to securely identify themselves in E-services through various identification tokens.

4 Changes to the service and its terms of use

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

The Service Provider is entitled to modify these Terms of Use, any terms and conditions drawn up for Service Users, and any other special terms of the Service after announcing such changes on the Service Management site or an equivalent platform. In addition, the Client Organisation’s contact persons shall be informed of the changes by e-mail.

The Client Organisation accepts the new Terms of Use by continuing to use the Service, unless the Service Provider requires separate approval of the changes in a manner determined by the Service Provider. In case that the Client Organisation does not accept the changed Terms of Use, it shall notify the Service Provider of this as well as the date on which the E-service shall terminate the use of the Service. In this case, the Service use must be terminated no later than on the date when the changes to the Terms of Use enter into force.

5 Service activation

5.1 Registration and approval in the Service

Using the service requires that the Client Organisation and its e-services register for the service, provide the data required by the Service Provider, and accept the Terms of Use of the Service. Moreover, using the strong electronic identification service requires an access licence issued by the Finnish Digital Agency or being added to an equivalent licence.

Organisations with a Finnish business ID or those registered in the EU/EEA may register for the service. Legislation imposes limitations to the access of organisations to

the service. The Act on Common Administrative e-Service Support Services (571/2016) contains provisions on organisations that may use the Service.

In case of changes to the Terms of Use, registration, Service activation and submitting Client Organisation details shall be performed through the Service Management website or in another manner as required by the Service Provider.

The Service Provider requires the Client Organisation to provide specific information, descriptions, and/or accounts on the e-service, organisation or contact persons that the Client Organisation has requested to be linked to the Service when applying for an access licence. The information, descriptions and/or accounts shall be transmitted to the Data Producers of the Service or the operators responsible for the technical aspects of Service provision.

The Service Provider will assess whether the organisation meets the requirements for registration. If the organisation is approved as a Client Organisation in the Service, the Client Organisation may join the Suomi.fi e-identification service.

In addition, the use of the Service requires that the Data Producer (here Finnish Digital Agency) approves the Client Organisation as a client for the access licence it has granted. The access licence is related to the disclosure of the population information system data used in the Service to the E-service as part of the Service. Client Organisations may be added to an access licence through placing an access licence order to the Data Producer.

If an access licence application or similar is submitted to the Service Provider by an Intermediary, the access licence to the Service is granted to the Client Organisation. The Intermediary acts as a technical and/or administrative contact organisation on behalf of the Client Organisation, but it is not in a contractual relationship with the Service Provider.

5.2 Joining and testing the Service

Before employing the Service in its actual production environment, the Client Organisation shall test the connection of its E-service and the Service functionalities in the Service Provider’s test environment.

After appropriate testing, the Client Organisation may start using the Service in the production environment.

5.3 Activation of the Service

The Client Organisation may activate the Service once the Service Provider has approved the Client Organisation, granted its approval for the use of the Service, and all measures required for using the Service, such as connections, have been appropriately taken.

The service description shall be available to the End User when using the service. The End User may use the service when they have access to the Identification Tokens required to use the Service.

6 Parties to the Service and their responsibilities

6.1 Parties to the Service

The Service management organisation is formed by the Ministry of Finance and the Finnish Digital Agency. The Finnish Digital Agency produces the Service and has contracted production services related to the identification function of the Service from third parties. The Finnish Digital Agency is responsible for the continuity of the service and for managing disruptions.

Client Organisations utilise the identification service by connecting their E-services to the Service.

End Users utilise the Service to identify themselves in the E-services.

6.2 Rights and obligations of the Service Provider

The Service Provider is responsible for providing the Service and developing it. The Service Provider shall ensure that the Service meets legislative requirements. The Service Provider 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.

The Service Provider is responsible for providing the Client Organisation with the necessary materials and instructions for connecting to the service and for providing service support during the production phase and after development measures. The instructions are available on the Suomi.fi for Service Developers website. The Service Provider is responsible for maintaining the test and production environment and other support services as well as for receiving and processing fault reports.

The Service Provider is responsible for concluding agreements or similar with the Producers of identification tokens to provide the Identification tokens used in the Service. The Service Provider decides, with consideration to statutory requirements, which Identification tokens are offered in the Service. The Service Provider shall notify in advance of any changes to the Identification tokens used in the Service, if advance notice is possible.

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

The Service Provider 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 Provider considers justified. For example, the Service Provider has the right to modify the functionalities or interfaces of the Service.

The Service Provider is entitled to issue orders requiring the Client Organisation to install updates to its E-services that the Service Provider considers necessary, such

as information security or version updates. The Service Provider shall also set a deadline for installing such updates.

The Service Provider is entitled to collect data on the E-services connected to the Service and their use for statistical purposes as well as to publish statistics.

The Service Provider shall investigate any faults and suspected misuse for their part and, if necessary, in cooperation with the Client Organisation or other parties. The Service Provider is responsible for the Service systems, applications and interfaces as well as for investigating and coordinating related to fault situations.

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

6.3 Rights and obligations of the Client Organisation

The Client Organisation shall ensure that the E-services meet the legislative requirements. The Client Organisation shall meet any obligations that it is responsible for fulfilling. The Client Organisation shall comply with these Terms of Use. The Client Organisation is responsible for the actions of its Users.

The Client Organisation is entitled to receive from the Service Provider adequate information required to connect to the Service and continue Service use after any changes.

The Client Organisation is entitled to adjust the settings and other options related to the utilisation and use of the Service on the Service Management website or similar for each E-service. The Data Producer or Producer of an identification token may have set restrictions on the available settings. The Client Organisation does not have the right to use the data transmitted in the identification process for purposes other than using the E-service.

Before joining the Service, the Client Organisation must provide the Service Provider with the required details on the organisation and its appointed contact persons and implement the technical requirements necessary for joining the Service, which are described on the Suomi.fi for Service Developers website.

The Client Organisation is responsible for ensuring that the Service Provider is provided with the personal details and other information on its contact persons and Users required for using the Service. The Client Organisation is obligated to provide information on their E-Service and its operating principles. The Client Organisation is responsible for providing the Service Provider with descriptions of the E-service if the Service Provider so requires.

The Client Organisation shall keep the data submitted to the Service Provider up to date and without delay provide any data that has changed through the Service Management website or by other means required by the Service Provider. The Client Organisation is responsible for ensuring, on its own initiative, that any incorrect, incomplete, or outdated data it is providing is rectified.

The Client Organisation shall ensure that it has been granted an access licence or equivalent or that is has otherwise been approved to use the Service. The Client Organisation shall evaluate and ensure that the conditions and requirements of the third party are met. The Client Organisation shall comply with the conditions and requirements of any access permits or equivalent set by third parties.

The Client Organisation shall join the test environment provided by the Service Provider and thereafter the production environment after the Service Provider has granted approval for this. The Client Organisation shall ensure that it tests the Service and the E-service to be connected before importing the E-service into the production environment of the Service and ensure sufficient testing in case of any changes.

The Client Organisation is responsible for its E-service connected to the Service and the related activities. The Client Organisation shall implement any modifications required in the E-Service in case of any changes made to the Service.

The Client Organisation is responsible for ensuring that the functionalities determined by the Service interface specifications have been implemented in the E-service. In particular, the E-service must support the single sign-out session of the Service and the related single sign-out functions.

The Client Organisation shall investigate any faults and suspected misuse for their part and, if necessary, in cooperation with the Service Provider or other parties. The Client Organisation is responsible for investigating and coordinating any fault situations in the E-service and related systems.

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

7 Data processing and protection of privacy

7.1 Processing of personal and other data and protection of privacy

The Service Provider processes personal data in the Service. In addition, the Client Organisations process personal data in their E-services and connected systems.

The Service Provider and Client Organisation 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 Provider and Client Organisation shall assume all the responsibilities of data controller in accordance with the General Data Protection Regulation (679/2016), and each of them must produce and publish the necessary notifications and bulletins related to their own processing of personal data.

The Service Provider processes personal data in its Service, customer and user register, and its other registers, as explained in greater detail in the Service privacy statements.

The data shall be stored for the time period necessary to fulfil the statutory obligations after the end of the customer relationship or Service production.

The Client Organisation shall file and archive the event and log data generated in its systems and servers appropriately and for the time period stipulated in legislation or other requirements.

7.2 Cookies

The Service uses cookies for the End Users and persons identified through the management interface of the Service Management website. The cookies used in the Service are described in more detail for End Users on the Suomi.fi website.

8 The Client Organisation's right to use the Service and the material contained within

The Client Organisation is granted the right to use the Service in compliance with these Terms of Use and any other special conditions, including requirements set by third parties, in their own internal use, and to offer or utilise the Service when providing its services to End Users.

The Client Organisation is not entitled to disclose material received through the Service to third parties if the material is not public, nor is it entitled 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 Provider or other rightsholders.

9 Service fees and allocation of costs

The Service is free of charge for organisations in the public administration and the companies they own. Further provisions on service fees are laid down in the Act on Common Support Services for Electronic Administrative Transactions (571/2016) and the Decree of the Ministry of Finance issued under the Act on Criteria for Charges Payable to the State (150/1992). The Service shall be priced according to the valid price list.

The Service Provider shall be responsible for the costs incurred from Service activation instructions and support as well as the costs incurred from any of its other obligations.

The Client Organisation shall be responsible for setting up the required and appropriate connections; making any modifications required in its own systems; any other costs that may be incurred for connecting to the Service; and any other costs that may be incurred for obligations it may have.

10 Service availability

While the Service Provider does not guarantee that the Service will be available continuously, every effort will be made to ensure its uninterrupted availability.

For the sake of clarity, it is stated here that the Service Provider shall at all times have the right to interrupt Service provision because of a modification, an update 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 interruptions and fault situations in Service provision

Any interruptions and fault situations in the Service shall be notified in the Service and the Service Management website or similar, to the Client Organisation's contact persons and Users per e-mail, and to the advisory service on Suomi.fi services as soon as possible after detecting the fault, if possible.

Advance notification of interruptions is provided if possible.

12 Service Provider's right to prevent Service use

The Service Provider shall reserve the right to refuse approval of a Client Organisation or a User as a user of the Service with just cause.

By its decision, the Service Provider 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.

In addition, the Service Provider has the right to prevent a Client Organisation or User from using the Service:

- if the Client Organisation or a User of the Client Organisation violates these Terms of Use, conditions related to using the Service set by other parties, or is in violation of good practice or the law, or if there is just cause to suspect this;
- if the Client Organisation does not submit the required information or reports;
- if the Client Organisation fails to comply with other legislation in its activities; or
- if the Client Organisation 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.
- if the Client Organisation neglects the payment of the Service fees despite being liable to pay.

Additionally, if the Client Organisation fails to make the changes required due to modifications made to the Service, the Service Provider has the right to prevent the Client Organisation from using the Service until these changes have been appropriately completed. Other consequences of failing to complete the required modifications by the set deadline may include the technical inability of the Client Organisation to use the Service.

The Service Provider 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.

13 Data security and related requirements

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

The Client Organisation shall accept the data security requirements set by the Service Provider and undertake to comply with them by accepting the Terms of Use. The Client Organisation shall accept the Service implementation as offered, and assess its suitability in terms of any requirements applicable to its own activities.

Data Producers may require that the Client Organisation meet data security requirements set by them in their data permits or equivalent.

The management and data security of the E-service and the information systems connected to it are the responsibility of the Client Organisation.

The Client Organisation using the Service is required to:

- ensure data security in their information systems appropriately;
- monitor the publication of any security updates and implement them;
- report information security incidents as required by the Service Provider; and
- ensure the secure maintenance of the E-service and the associated systems in terms of access rights, user IDs, backup copies, and fault situation management.

The Client Organisation is required to comply with good information security practices.

Managing and ensuring information security is an essential part of the Service. If the Service Provider decides to implement vulnerability scans, the Client Organisation grants the Service Provider the permission to target scans on the public interfaces of the E-service of the Client Organisation in order to detect any vulnerabilities in data protection or information security. The schedule of the vulnerability scans shall be agreed upon jointly so that they can be implemented without causing disruptions in the use of the E-service. The Client Organisation undertakes to eliminate any significant vulnerabilities detected by a deadline set by the Service Provider.

The Service Provider may make Service use conditional on fulfilment of specific information security requirements applicable to the Client Organisation and the E-service. The Service Provider may impose stricter requirements than those listed above.

More stringent forms of the aforementioned requirements also may have been imposed in data permits or equivalent between a third party and the Client Organisation.

If an information system of the Service Provider used to provide the Service or an information system of the Client 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 Provider or the Client Organisation may disconnect their information system from a system maintained by the other party.

The Service Provider shall immediately notify the Client Organisation and End 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. This notification shall indicate the estimated duration of the disruption or threat and, where possible, any protective measures that can be taken by the Client Organisation and End User. In addition, the Service Provider shall notify the Client Organisations and End Users when the disruption or threat is over.

The Client Organisation shall notify the Service Provider without delay if its information system connected to the Service is subjected to or threatened by a major security breach or other event that may jeopardise the data security or functioning of the Service or significantly disrupt it. The notification shall include the content of the incident or threat, its estimated duration and, where possible, any protective measures. The Client Organisation shall also notify the Service Provider when the disruption or threat is over.

If the Service Provider finds this possible and necessary in individual cases, the Service Provider or its supplier shall notify the Client Organisations of any observed vulnerabilities, potential corrective measures, and information security updates which are associated with the Service, or which otherwise have an impact on using the Service.

The Client Organisations and Users shall be notified of any information security incidents and threats observed as stated in section Notification of interruptions and fault situations in Service provision.

14 The liability and limitation of liability of the Service Provider

The Service Provider 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 Provider is responsible for the accuracy of the combined data required for the provision of the Service and for the security of the data processed in the Service.

The Service Provider shall ensure that the Service it provides is designed, built and maintained so that:

- the produced Service is secure and of good quality in terms of its technical aspects;
- it can withstand normal, expected external interference and security threats;
- its performance, usability, quality, and reliability are monitored;
- significant data breaches and threats affecting it as well as faults and disruptions that significantly interfere with its operation can be detected; and
- the modifications made in it do not cause unreasonable disruptions to the Client Organisation's E-Service that utilises the Service or to other tasks performed using the Service.

The Service Provider shall not be liable to the Client Organisation or a third party for:

- possible errors by Data Producers, Providers of identification tokens, or data sources;
- the termination of the provision of a specific Identification token;
- the applicability and suitability of the Service for any special needs of 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 of Use, Access licence or similar of the E-Service or the legislation, 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 Provider’s control or any outages of the telecommunications network or the Internet.

The use of the Service is intrinsically linked to the utilisation of data and services provided by third parties (Data Producer and Provider of Identification tokens). The Terms of Use and other terms of the third party in question shall apply to such third-party data and services. The Service Provider shall in no part be liable for losses incurred for such third-party data, servers or services, their functionality or use, or otherwise. The Service Provider shall also not be liable for the information security, data protection or contents of such third-party servers or Services.

The Service Provider'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 Provider 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 Provider's intentional act or gross negligence.

15 Liability for damages

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

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

In other cases, the Tort Liability Act applies to compensation for damages.

16 Force majeure

Cases of force majeure shall release the Service Provider 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.

The Service Provider shall notify on a force majeure incident immediately after its appearance on its website, Service Management website, or similar, if possible.

17 Monitoring and supervision

The Service Provider 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 Client Organisation shall control the implementation of information security and data protection and the legality of data processing. The Client Organisation shall appoint a person responsible for information security and data protection if so required by the Service Provider and ensure that personnel using the Service receive adequate information security training.

In order to enable ex post control, event and log data on data disclosures and other processing of data shall be kept. The Service Provider shall maintain specifically defined event and log data on the Service. The Client Organisation shall maintain any

event and log data required by the Service. The event and log data is based on identified Client Organisations and Users as well as other information on the End User and the processing of data. If there is reason to suspect misuse, the event and log data enable investigating which party has processed the data and on what grounds. The Service Provider has the right to obtain any information on Service use it requires from a Client Organisation or a User by the deadline it sets.

18 Service audit

Efforts to develop the Service further will be audited in connection with application development and before they are introduced in productive use.

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

19 Transfer of rights and obligations

The Client Organisation is not entitled to transfer the right to use the Service or the related rights and obligations to a third party without prior notification to the Service Provider and the Service Provider’s approval, as legislation sets restrictions to the extent to which organisations can use and utilise the Service.

A Client 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 Client Organisation's tasks are to be transferred. Written notification of this transfer shall be given to the Service Provider in advance.

The Service Provider 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 Provider’s tasks may be transferred.

20 Termination of the service

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

A Client Organisation has the right to terminate use of the Service at any time without giving a reason. The Client Organisation may deactivate or terminate the use of the Service by notifying of this on the Service Management website or in another manner required by the Service Provider. The User may notify of terminating the use of the Service on the Service Management website or in another manner required by the Service Provider.

The Service Provider has the right to terminate Service provision fully or in part for a particularly weighty reason. The Service Provider may close 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 Provider also has the right to terminate Service provision to a specific Client Organisation or to withdraw a specific User's access rights on grounds set out in section Service Provider's right to prevent Service use, or if there is justified reason to suspect other misuse. The provision or use of the Service may be terminated with immediate effect. If the Service Provider finds that immediate termination is not necessary, it will give written advance notification of the termination and its grounds.

The Service Provider shall not be liable for any loss of income or other damages incurred by the discontinuation of Service use or provision to Client Organisations or other parties.

21 Applicable law and resolution of disputes

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

The Service Provider'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 Provider (Finnish Digital Agency) may be addressed to the Service Provider. Provisions on submitting a claim for a revised decision are laid down in the Administrative Procedure Act (434/2003).

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

Legislation or terms and conditions shall be applied to the contractual relationships and Terms of Use between a Client Organisation and a Data Producer or another authority according to what has been specifically provided or agreed in each case.

Disputes between a Client Organisation and a Data Producer or another authority shall be resolved according to what has been specifically provided or agreed in each case.