DRAFT 15
December 2025

Government Proposal to Parliament for an Act Amending the Act on Central Government's Joint e-Service Support Services

MAIN CONTENT OF THE PROPOSAL

The proposal suggests amending the Act on Central Government's Joint e-Service Support Services.

The objective of the proposal is to enable electronic notifications sent by authorities to the messaging service produced by the Digital and Population Data Services Agency to be displayed to users of the messaging service not only through the service's own user interface (the Suomi.fi Messages service), but also through a digital service provided by a private operator. According to the proposal, the Act on Central Government's Joint e-Service Support Services would in the future define a viewer, meaning a digital service that functions as a user interface for the messaging service. The Act would be supplemented with a clarifying provision on the duty of the service provider, namely the Digital and Population Data Services Agency, to provide a viewer, as well as a provision on assigning this auxiliary public administration task to a private operator by contract. The Digital and Population Data Services Agency would be required to provide a viewer even if a private operator were to provide a viewer application on the basis of a contract. In addition, the Act would lay down general requirements applicable to private operators providing a viewer application, the minimum content of the contract, obligations of cooperation, arrangements for disruption situations, and supervision.

In accordance with the Government Programme of Prime Minister Petteri Orpo's Government, the proposal promotes Finland's gradual transition towards digital services as the primary channel for dealings with public authorities. Furthermore, the proposal would enable the display of official notifications from authorities in private digital mail services in a cost-effective manner.

The proposed Act is due to enter into force on 1 July 2026.

———

CONTENTS

MAIN CONTENT OF THE PROPOSAL....1
1 BACKGROUND AND PREPARATORY WORK....4
1.1 BACKGROUND....4
1.2 PREPARATORY WORK....6
2 CURRENT SITUATION AND ASSESSMENT....7
2.1 GENERAL REGULATION CONCERNING NOTIFICATION AND NOTIFICATION PROCEDURES....7
2.1.1 EXISTING REGULATORY FRAMEWORK....7
2.1.2 PENDING AMENDMENTS....8
2.1.3 OTHER ELECTRONIC MESSAGES SENT BY AUTHORITIES AND RELATED REGULATION....9
2.2 ACT ON CENTRAL GOVERNMENT'S JOINT E-SERVICE SUPPORT SERVICES AND SUOMI.FI MESSAGES....10
2.2.1 GENERAL....10
2.2.1.1 PURPOSE OF THE SUPPORT SERVICES ACT....10
2.2.1.2 SUOMI.FI MESSAGES IN GENERAL....10
2.2.2 THE DIGITAL AND POPULATION DATA SERVICES AGENCY AS SERVICE PROVIDER OF SUOMI.FI MESSAGES....11
2.2.3 AUTHORITIES AS USERS OF SUOMI.FI MESSAGES....13
2.2.3.1 OBLIGATION TO USE SUPPORT SERVICES....13
2.2.3.2 EXEMPTION FROM THE OBLIGATION TO USE SUPPORT SERVICES…13
2.2.3.3 ENTITIES ENTITLED TO USE SUPPORT SERVICES....14
2.2.3.4 USE OF THE MESSAGING SERVICE....15
2.2.4 PUBLIC ADMINISTRATION CLIENTS OF SUOMI.FI MESSAGES....16
2.2.4.1 IMPLEMENTATION OF SUOMI.FI MESSAGES....16
2.2.4.2 USE OF SUOMI.FI MESSAGES....17
2.2.4.3 ENDING THE USE OF SUOMI.FI MESSAGES....18
2.3 OTHER REGULATIONS CONCERNING SUOMI.FI MESSAGES....18
2.3.1 ACT ON THE PROVISION OF DIGITAL SERVICES....18
2.3.1.1 GENERAL....18
2.3.1.2 ACCESSIBILITY....20
2.3.2 PROCESSING OF PERSONAL AND OTHER DATA IN SUOMI.FI MESSAGES....21
2.3.3 ACT ON INFORMATION MANAGEMENT IN PUBLIC ADMINISTRATION24
2.3.4 OTHER GENERAL ADMINISTRATIVE LAWS AND THE NON-DISCRIMINATION ACT....25
2.3.5 ACT ON ELECTRONIC COMMUNICATIONS SERVICES....25
2.3.6 EIDAS REGULATION....26
2.3.7 CYBERSECURITY REGULATION AND SUPERVISION....27
2.4 SUOMI.FI MESSAGES AS A PUBLIC ADMINISTRATION TASK....28
2.5 PRIVATE DIGITAL MAIL SERVICES....30
2.5.1 THE MARKET FOR PRIVATE DIGITAL MAIL SERVICES IN FINLAND....30
2.5.2 REGULATION OF PRIVATE DIGITAL MAIL SERVICES....32
2.5.2.1 ACT ON ELECTRONIC COMMUNICATIONS SERVICES....32
2.5.2.2 REGULATION AND SUPERVISION OF PERSONAL DATA PROCESSING....32
2.5.2.3 EIDAS REGULATION....33
2.5.2.4 CYBERSECURITY REGULATION AND SUPERVISION....34

2.5.2.5 REQUIREMENTS UNDER CHAPTER 4 OF THE INFORMATION MANAGEMENT ACT....34
2.5.2.6 ACT ON INFORMATION SECURITY INSPECTION BODIES....34
2.6 ASSESSMENT OF THE CURRENT SITUATION....35
2.6.1 UTILISATION OF SUOMI.FI MESSAGES....35
2.6.2 USE OF PRIVATE DIGITAL MAIL SERVICES....36
2.6.3 CARRYING OUT THE TASK INCLUDED IN THE MESSAGING SERVICE (PROVIDING A VIEWER APPLICATION) AS A PUBLIC ADMINISTRATION TASK....38
3 OBJECTIVES....39
4 PROPOSALS AND THEIR IMPACTS....41
4.1 MAIN PROPOSALS....41
4.2 PRINCIPAL IMPACTS....42
4.2.1 IMPACT ON PUBLIC FINANCES....42
4.2.2 BASIC AND HUMAN RIGHTS IMPACTS....43
4.2.2.1 EQUALITY....43
4.2.2.2 LEGAL PROTECTION....44
4.2.2.3 PROTECTION OF PRIVATE LIFE....46
4.2.3 SOCIAL EFFECTS....49
4.2.3.1 IMPACT ON PUBLIC AUTHORITIES....49
4.2.3.2 INFORMATION SOCIETY AND DATA PROTECTION....50
4.2.3.3 IMPACT ON AUTHORITIES' INFORMATION MANAGEMENT....54
4.2.3.4 IMPACT ON COMPANIES....56
4.2.3.5 IMPACTS ON THE INTERNAL MARKET....59
5 OTHER OPTIONS FOR IMPLEMENTATION....63
5.1 ALTERNATIVES AND THEIR IMPACTS....63
5.2 LEGISLATION AND OTHER MEANS IN PLACE IN OTHER COUNTRIES....64
5.2.1 SWEDEN....64
5.2.2 DENMARK....67
5.2.3 NORWAY....69
5.2.4 NETHERLANDS....71
5.2.5 BELGIUM....72
5.2.6 ESTONIA....74
6 FEEDBACK....75
7 PROVISION-SPECIFIC RATIONALE....75
8 ENTRY INTO FORCE....81
9 IMPLEMENTATION AND MONITORING....81
10 RELATIONSHIP TO THE CONSTITUTION AND THE LEGISLATIVE PROCEDURE....82
10.1 PROTECTION OF PRIVATE LIFE....82
10.2 LEGAL PROTECTION AND GOOD GOVERNANCE....83
10.3 DELEGATION OF PUBLIC ADMINISTRATION TASKS TO PARTIES OTHER THAN THE AUTHORITIES....84
THE DRAFT ACT....89
Amendment to the Act on Central Government's Joint e-Service Support Services....89

EXPLANATORY NOTE

1 Background and preparatory work

1.1 Background

The Government Programme of Prime Minister Petteri Orpo's Government states that Finland will gradually transition to digital services as the primary channel for accessing the services of public authorities. Legislation will be amended to make digital communications the primary channel for communications by public authorities. In addition, the Government Programme states that the Government will explore a cost-effective way to send mail from public authorities to private digital mail services.

On 27 March 2024, the Ministry of Finance launched the Digital First programme (VM006:00/2024) and established its steering group. Furthermore, on 13 May 2024, the Ministry of Finance appointed a legislative working group (VM085:00/2024), which prepared a Government Proposal to Parliament on legislation concerning the primacy of electronic communication in public administration (HE 124/2025 vp). In addition to the legislative amendments enabling primacy, an implementation and legislative project will be carried out during the government term, under which private digital mail services will be introduced alongside the public administration's common messaging service. Through these services, users may choose to receive, in addition to other electronic communications, electronic notifications sent by public authorities.

At its meeting on 30 January 2025, the Ministerial Committee on Economic Policy supported the expansion of implementation measures in line with the Government Programme and the central government productivity programme, with the aim of primarily delivering official communications digitally by enabling the delivery of notifications sent by public authorities also to private digital mail services. In addition, the Ministerial Committee decided to initiate work to create well-functioning markets for private digital mail services. Through an inclusive process, the characteristics of a functioning digital mail services market will be defined, including technical and other requirements, pricing or financing models, and measures to ensure the emergence of well-functioning markets, taking into account information security, security of supply, and cost-effectiveness.

At its meeting on 7 October 2025, the Ministerial Working Group on Reforming Society decided on the fundamental implementation principles for enabling the delivery of electronic notifications from public authorities also to private digital mail services:

1. The service produced and maintained by the Digital and Population Data Services Agency will continue to operate as the centralised backend service for official communications, to which authorities will continue to submit notifications and other official messages. However, the obligation of use laid down in section 5 of the Support Services Act would apply only to authorities' notifications. The development of the service will build on the existing Suomi.fi Messages service and its technical interfaces. In addition, the Digital and Population Data Services Agency will continue to provide the Suomi.fi Messages service as a unified user interface for electronic official communications.

2. The storage of official messages outside the backend service will be avoided. Private digital mail services will act as providers of a viewing connection for the display of messages from public authorities. The user may, if they so choose, save a message to a location of their preference.

3. The user has the right and the opportunity to choose from which approved digital mail service they read electronic messages sent by public authorities to the backend service and, where necessary, respond to them. The user may, at their discretion, smoothly switch the service they use or discontinue the service altogether. The user must separately authorise the digital mail service they use in a service managed by the Digital and Population Data Services Agency, which provides the user with a centralised view of the service or services through which their official messages can be accessed.

4. Users who have not opted out of digital official communications will always have access to the Suomi.fi Messages service. This solution ensures continuity of service in situations where a private digital mail service ceases operations or otherwise temporarily becomes unavailable.

5. If the user chooses to make use of an approved private digital mail service, the user is not obliged to monitor the underlying Suomi.fi Messages service, as monitoring another approved digital mail service is sufficient.

6. Private digital mail services may provide a viewing connection to authorities' notifications once they have met the prescribed criteria and obligations and have received a positive decision authorising them to operate as providers of a viewing connection.

7. The development-related costs for authorities sending messages will be minimised.

8. In the legislative drafting process, an assessment will be made of the extent to which a private digital mail service operator performs a public administration task when providing a viewing connection to a notification sent by an authority. On the basis of this assessment, the regulatory need under section 124 of the Finnish Constitution concerning the assignment of a public administration task to an entity other than a public authority will be further specified. Based on the same assessment, the minimum criteria required of a private digital mail service operator to act as a provider of a viewing connection to an authority's notification will also be refined. In addition, the adequacy of supervisory duties already prescribed by law for authorities, or any potential need to establish supervisory arrangements, will be evaluated.

9. Due to scheduling and resource constraints, the use of Suomi.fi Authorisations and other features and functionalities related to special needs in private digital mail services will be excluded from the scope of implementation. Acting on behalf of another party by means of Suomi.fi Authorisations will continue to be possible in Suomi.fi Messages.

10. Approved private digital mail service operators and other actors involved in the ecosystem will be required to engage in mutual cooperation in order to ensure information exchange and interoperability.

11. In the preparatory work, compensation to be paid to private digital mail service operators will be assessed in light of public finance flexibility and competition law impacts. Alternatives for the payment model include, on the one hand, making the operation free of charge from the perspective of public finances and, on the other hand, an annual fixed budget to be distributed among participating operators based on the service through which the user first opens each message from a public authority.

12. The technical implementation of the backend service is intended to be brought into production as quickly as possible. The schedule is affected by the simultaneously implemented project to establish the primacy of electronic communication from public authorities, development work on Suomi.fi Messages arising from other ongoing Government Programme projects, and the ongoing modernisation and development of the Suomi.fi Messages interfaces, on which the use of the backend service is planned to be based. The production deployment schedule will be clarified in the implementation project of the Digital and Population Data Services Agency. The schedule will also be influenced by the timelines of the sending organisations and the digital mail service operators for any potential changes. If necessary, the information system changes required to establish the primacy of electronic communications from public authorities will be prioritised.

In connection with the aforementioned point 11, on 11 November 2025, the Ministry of Finance informed the Ministerial Working Group on Reforming Society of the policy that no state funding will be provided for displaying authorities' notifications in private digital mail services.

1.2 Preparatory work

The draft Government Proposal has been prepared as official work at the Ministry of Finance. In accordance with the guidelines of the Ministerial Committee on Economic Policy, the more detailed technical and functional objectives, requirements, and features for implementation were specified in a series of workshops held in April–May 2025, which involved the project's key stakeholders. The workshops were organised by the Digital and Population Data Services Agency. In addition, in autumn 2025, the Digital and Population Data Services Agency held planning meetings with stakeholders, in which, among other matters, proposed legislative amendments were discussed.

The draft Government Proposal was prepared and sent for a consultation round at the same time that the Government Proposal to Parliament on legislation concerning the primacy of electronic communication in public administration (HE 124/2025 vp) was under consideration in Parliament. For this reason, the draft submitted for consultation describes the legal situation that was in force during the preparation process and separately refers to the changes proposed in the Government Proposal being considered by Parliament, to the extent that these changes are intended to modify the legal situation or otherwise affect provisions relevant to this proposal. Since the Government Proposal under consideration in Parliament proposes amendments to a law that is central to this proposal, the Act on Central Government's Joint e-Service Support Services, the sections proposed in the draft have been numbered on the assumption that the Government Proposal being considered in Parliament has been approved and that the proposed provisions are in force as presented. Substantively, the changes proposed in the draft are not dependent on the approval of the Government Proposal currently under consideration in Parliament.

The draft Government proposal was circulated for comment on [dates]. The consultation period was approximately seven weeks. However, it fell during the general holiday season, which meant that the consultation period was one week shorter than the standard. The shorter consultation period was due to the Government's objective to submit the Government's proposal to Parliament during the spring session of 2026 and the EU notification procedure in the field of technical regulations described below.

The preparatory documents for the Government Proposal are available in the public service at https://vm.fi/hankkeet under the identifier VM062:00/2025.

The draft law concerning private digital mail services must be notified to the European Commission in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council, which lays down a procedure for the provision of information in the field of technical regulations and rules on information society services. The Commission and the other Member States have the opportunity to submit comments on the content of the draft within three months of the notification being submitted. During this period, the proposal may not be adopted. If the Commission or another Member State submits, within the prescribed time limit, a detailed opinion stating that the planned measure may result in obstacles to the free movement of services within the internal market, the adoption of the proposal must be postponed by an additional month. More detailed information on Directive (EU) 2015/1535 and the related notification procedure is provided below in section 4.2.3.5. The draft law was notified to the Commission on [date] ([link to the notification]). [to be supplemented later with the outcome of the procedure]

Certain aspects of the draft law concerning private digital mail services are also notified to the European Commission on the basis of Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (the Services Directive). The Commission shall bring the submitted provisions to the attention of the other Member States. The submission of the provisions does not prevent Member States from adopting those provisions. With regard to certain notified provisions, the Commission shall, within three months of the notification, examine whether the provisions are compatible with EU law and, where appropriate, adopt a decision requesting the Member State concerned to refrain from adopting them or to repeal them. More detailed information on the Services Directive and the related notification procedure is provided below in section 4.2.3.5. The draft law was notified to the Commission on [date] ([link to the notification]). [to be supplemented later with the outcome of the procedure]

2 Current situation and assessment

2.1 General regulation concerning notification and notification procedures

2.1.1 Existing regulatory framework

Administrative procedure is governed, as a general act, by the Administrative Procedure Act (434/2003). Chapter 9 of the Administrative Procedure Act contains the general provisions on the service of documents, and Chapter 10 lays down the procedure to be followed in service of documents. Pursuant to section 54 of the Administrative Procedure Act, an authority has an obligation to serve the decision it has issued as well as any other document that affects the handling of the matter. Regular and verifiable service of documents are regulated in sections 59 and 60 of the Administrative Procedure Act. Under section 5(2) of the Administrative Procedure Act, regular and verifiable electronic service of decisions is governed by the Act on

Electronic Services and Communication in the Public Sector (13/2003; hereinafter the Act on Electronic Services).

Sections 18 and 19 of the Act on Electronic Services regulate verifiable and regular electronic service of documents, which may generally be used for the service of the same types of documents as those served by regular and verifiable service under sections 59 and 60 of the Administrative Procedure Act. According to sections 18 and 19 of the Act on Electronic Services, both verifiable electronic service and regular electronic service require the consent of the party concerned.

The regulation laid down in the Act on Electronic Services is technology-neutral in that it allows the use of various electronic methods for the service of documents. Accordingly, as a starting point, an authority may use any electronic method it considers appropriate, provided that the method complies with the requirements of the law. Electronic service of documents may therefore be carried out, for example, by email, via a messaging service (the Suomi.fi Messages service), through a public authority's digital service, or through another service that meets the statutory requirements (which may, as such, also be a private digital mail service, if the person has indicated it as their contact detail and the authority has an interface with that service). However, requirements related, inter alia, to information security and confidentiality may impose restrictions on the method of service.

The provisions of the Act on Electronic Services concerning the service of documents constitute a general regulatory framework that enables the use of electronic methods of service for those authorities and other actors falling within the scope of application of the Act. It is therefore not necessary to regulate electronic service of documents or its use separately, as the electronic service of an authority's document is possible directly under general legislation, unless other legislation, international agreements, or, for example, EU law explicitly prohibit it. In some cases, the circumstances of service may make electronic service of the document impossible, for instance, if the service is carried out in a situation where the person does not have access to an electronic device.

2.1.2 Pending amendments

In the Government Proposal currently before Parliament on establishing the primacy of electronic communication in public administration (HE 124/2025 vp), it is proposed to amend the provisions on service of documents in the Act on Electronic Services. A key change is that sections 18 and 19 of the Act on Electronic Services would no longer require the consent of the party concerned for electronic service of documents. In practice, this change would also mean that the register maintained under section 11 of the Act on Central Government's Joint e-Service Support Services (571/2016; hereinafter the Support Services Act) would no longer store, for each user, information on their general consent to electronic service under the Act on Electronic Services. Instead, the register would record whether the person has an active messaging service account.

According to section 18(1) of the Act on Electronic Services as proposed in this Government Proposal, an authority may serve a document, which under the law would otherwise be delivered by mail against acknowledgement of receipt or by other formal service, electronically via a message. According to proposed section 18(2), an authority may send a document: 1) to a messaging service; 2) to a transaction service; or 3) to an electronic address other than those referred to in points 1 or 2, which the recipient of the service has provided as

a contact detail. The detailed reasoning for the proposed subsection emphasises the role of the messaging service as a channel for sending electronic notifications.

Under the Act on Electronic Services, it is therefore proposed that authorities, as a starting point, deliver electronic notifications to the messaging service maintained by the Digital and Population Data Services Agency under the Support Services Act (the Suomi.fi Messages service). However, authorities would have discretion in choosing the method of electronic service. In addition to the messaging service, authorities could also send notifications to a transaction service under their responsibility or to another electronic address provided by the recipient as a contact detail. Sending a notification to the messaging service would require that the service is activated for the recipient. Sending a notification to a transaction service under the authority's responsibility would also require that the recipient has the messaging service activated to receive the notification or has provided another electronic address for receiving the notification. Sending a notification to another electronic address would require that the recipient has provided that electronic address as a contact detail to the authority. On this basis, the Act on Electronic Services would more clearly direct authorities to send notifications to a service maintained by a public authority (either the messaging service maintained by the Digital and Population Data Services Agency, Suomi.fi Messages, or a transaction service under the authority's responsibility).

2.1.3 Other electronic messages sent by authorities and related regulation

Not all communication from a public authority to a client of the administration involves documents subject to the service obligation under section 54 of the Administrative Procedure Act. An authority's communication with a client may, for example, consist of advice under section 8 of the Administrative Procedure Act. According to this section, the authority must, within the limits of its powers, provide clients with advice related to the handling of an administrative matter as needed, and respond to questions and inquiries concerning transactions. In addition, under the service principle of section 7 of the Administrative Procedure Act, an authority may communicate to clients of the administration other information deemed necessary. Section 20 of the Act on the Openness of Government Activities (621/1999; hereinafter the Openness Act) regulates an authority's obligation to provide information. According to this section, an authority must inform the public about its activities and services, as well as the rights and obligations of individuals and organisations in matters within its field of competence. In addition to these messages, documents that fall outside the service obligation may include, for example, various communications related to actual administrative activities—such as social services, education, or healthcare—that are not connected to the handling of an administrative matter, reminder messages, and automated notifications concerning, for instance, information security or document receipt.

There is no general legislation governing how other authority communications should be delivered to clients of the administration. The choice of delivery method is, however, guided by any applicable legislation concerning the matter being communicated, as well as requirements related to information security and confidentiality. For example, section 5(1) of the Act on the Provision of Digital Services (306/2019) obliges authorities to provide everyone with a messaging service or another sufficiently secure electronic transmission method for receiving authority communications, even if the authority is not required to use Suomi.fi Messages.

2.2 Act on Central Government's Joint e-Service Support Services and Suomi.fi messages

2.2.1 General

2.2.1.1 Purpose of the Support Services Act

The Support Services Act regulates common support services for digital services in public administration. According to section 2(1) of the Act, a support service means a common e-service support service used by a user organisation, such as an authority, to support its service, other tasks assigned to it, or the services it provides. The Act lays down provisions on the different support services and the requirements applicable to them, the tasks related to their provision, and the processing of personal and other data in connection with their provision. In addition, the Act regulates the right and obligation to use support services and the conditions for their use. The Digital and Population Data Services Agency provides support services, with only a few exceptions.

The purpose of the Support Services Act is to improve the accessibility, quality, information security, interoperability, and governance of public services, as well as to promote the efficiency and productivity of public administration. In particular, the Act aims to ensure that support services help achieve greater cost-effectiveness in service provision and to guarantee the quality and interoperability of services by regulating the uniform production and use of support services.

Section 3 of the Support Services Act lists the common support services for digital services. There are nine support services in total, all of which are part of the Suomi.fi services. For the purposes of this proposal, the relevant support service is the messaging service referred to in section 3(1)(7) of the Support Services Act, provided and maintained by the Digital and Population Data Services Agency as Suomi.fi Messages.

2.2.1.2 Suomi.fi Messages in general

The messaging service under the Support Services Act, i.e., Suomi.fi Messages, allows a user organisation, such as an authority, and a user, i.e., a client of the administration, to send electronic messages to each other. Authorities can also serve documents to clients electronically or by mail through this service. Suomi.fi Messages thus functions as a digital mail service for administrative messages for clients of the administration, citizens and businesses, allowing them to receive messages from various authorities and other public administration actors. Through the service, clients of the administration can also send messages to a user organisation, initiate a matter with an authority, or provide additional information related to a matter, if the Suomi.fi Messages user organisation, such as an authority, has enabled this functionality.

Authorities can serve decisions electronically to clients of the administration via Suomi.fi Messages. A decision or document can also be served electronically in a formal manner through the Suomi.fi Messages service. Electronic service of documents may be used, for example, in administrative and court matters, as provided in the Act on Electronic Services or other applicable legislation. The Suomi.fi Messages service is not intended for inter-authority communication or for businesses to communicate with their customers outside of official duties.

Clients of the administration can access their Suomi.fi Messages digital mail service via the Suomi.fi web service and mobile application. Users of Suomi.fi Messages receive a notification of a new message at their registered email address, and in the case of the mobile application, via a push notification. Use of the Suomi.fi Messages service is free of charge for both users and user organisations. However, the user organisation is responsible for costs arising from any modifications that may be required in its own systems to implement the use of Suomi.fi Messages, as well as for postage costs for messages delivered by paper mail.

In addition to enabling electronic communication with clients of the administration, Suomi.fi Messages allows user organisations, if they wish, to send their paper letters to clients centrally using the printing, enveloping, and distribution service (TKJ service). By using the TKJ service, user organisations can send messages to clients in a single operation, regardless of whether the recipient uses Suomi.fi Messages or receives paper mail. The TKJ service operates such that the Digital and Population Data Services Agency has procured a service provider for this purpose, and user organisations of the messaging service may, if they wish, use the procured service or handle the mailing of their paper letters through their own contractual partners. However, a user organisation must use Suomi.fi Messages itself in order to take advantage of the TKJ service, and it may send via the TKJ service only those messages that it has sent through Suomi.fi Messages.

Use of Suomi.fi Messages requires the client of the administration to use strong electronic identification with the Suomi.fi e-Identification service. The granting of access rights to Suomi.fi Messages is managed via the Suomi.fi e-Authorisations. Both of the above-mentioned services are support services as referred to in the Support Services Act. In addition, information on the death of a user of Suomi.fi Messages is retrieved from the Population Information System for the Suomi.fi Messages service.

2.2.2 The Digital and Population Data Services Agency as service provider of Suomi.fi Messages

Pursuant to section 4(1) of the Support Services Act, the Digital and Population Data Services Agency produces and develops the messaging service, i.e., Suomi.fi Messages. Chapter 4 of the Support Services Act (sections 16–21) sets out requirements regarding support services and their use, which primarily apply to the service provider, but also, for example, to user organisations. In the case of the messaging service, the requirements for the service provider therefore apply to the Digital and Population Data Services Agency.

Under section 16 of the Support Services Act, the service provider is responsible for the quality and information security requirements set out in that section. According to subsection 1 of that section, the service provider is responsible for the quality and cost-effectiveness of the support service it produces, as well as for ensuring that the service is generally suitable for its intended purpose, performs reliably, is operationally robust, and is as user-friendly and accessible as possible. The service provider must, in implementing a support service, comply with the enterprise architecture and interoperability specifications of public administration. According to subsection 2, the service provider is responsible for the accuracy of the data integration required to produce the support service, as well as for the information security of the data processed in the support services, in addition to what is stipulated in the EU General Data Protection Regulation and the Finnish Data Protection Act (1050/2018). Subsection 3 sets out more detailed requirements regarding the quality, functionality, and information security of the support service. The purpose of these provisions is to ensure that the service provider properly manages the technical implementation of the support service, both when

designing, building, and maintaining the service. Under subsection 4, the service provider must prepare a service description for the service it provides, which it must maintain and which must show, with sufficient detail, the specific requirements set out in that provision.

Section 17 of the Support Services Act contains special provisions regarding the information security of the information systems used in service production. Subsection 1 stipulates that the service provider is responsible for ensuring the information security of the information systems used to produce the support service. Under subsection 2, a support service must be produced and developed in such a way that, if necessary, it is possible to establish processing environments that meet either basic or elevated information security requirements. In addition, the need for and implementation of information security requirements must be assessed using risk management methods. Subsection 3 sets out the information security requirements for the integration of user organisations' information systems. According to the legislative history of the Support Services Act, this subsection was specifically intended to emphasise the requirements for information systems and the conditions for their integration, since these services involve the processing of data of public administration clients, some of which may be sensitive personal data. It was also considered necessary to regulate the integration of user organisations' information systems separately, to ensure that such integration does not compromise the information security of the systems themselves or of the data processed within them. (HE 59/2016 vp, p. 58)

Section 18 of the Support Services Act sets out the procedural requirements necessary for the production of support services, as well as for the provision of services of public administration and the use of other support services, including notification obligations in the event of faults or disruptions. The section imposes obligations on both the service provider and the user organisation. Subsection 1 provides that the party responsible for an information system causing harm has an obligation to take action if a system used to produce a support service, or a system connected to a user organisation's support service, causes harm to the operation or information security of the support service or any system connected to it. Under subsection 2, the service provider is obligated to notify the user organisations that use its support services, as well as the users of those services, of any significant information security breach affecting or threatening the support service, or of any other event that prevents or substantially disrupts the service or compromises information security. The service provider must provide information on the estimated duration of the disruption or threat, any available protective measures, and the conclusion of the disruption or threat.

As in subsection 2 above, Section 18(3) of the Support Services Act establishes a notification obligation for the user organisation toward the service provider. Subsection 4 imposes a duty on the service provider to report regularly on the functionality and information security of its support services and to immediately notify the Ministry of Finance, or an authority designated by it, of any significant deviations relating to these services.

Section 19(1) obliges service providers to ensure, through contingency plans, preparatory measures for operations during disruptions under normal conditions or in exceptional circumstances, and other necessary actions, that operations and service production continue as smoothly as possible during both disruptions under normal conditions and in exceptional circumstances. Subsection 2 provides that, in normal conditions and during related disruptions, the prioritisation and urgency of production and use of services referred to in the Support Services Act, as well as other determinations of importance, must follow principles pre-defined by the Ministry of Finance, unless otherwise provided by law. The Government decides on principles of broad and socially significant importance. Subsection 3 refers to the

Emergency Powers Act (1552/2011) regarding the service provider's preparedness obligations, the guidance of central government information management, and the organisation of electronic services during exceptional circumstances.

Sections 20 and 21 of the Support Services Act regulate the log registry maintained by the Digital and Population Data Services Agency, which records information on the use of support services and the processing of data stored therein, as well as the use and disclosure of information from the log registry. The content of these sections is described in more detail in Chapter 2.3.2 in connection with the processing of personal and other data in Suomi.fi Messages.

In the report of the Administrative Committee on the draft Support Services Act, it is noted that the service provider for support services is an authority, whose task as a service provider is to produce support services under official responsibility, in compliance with general legislation governing public administration and the requirements for service production set out in the proposed Act (HaVM 13/2016 vp, p. 8). In the case of the messaging service, this obligation rests with the Digital and Population Data Services Agency.

2.2.3 Authorities as users of Suomi.fi Messages

2.2.3.1 Obligation to use support services

Pursuant to section 5 of the Support Services Act, state administrative authorities, agencies, institutions and state enterprises, well-being services counties and authorities of well-being service federations, municipal authorities, as well as courts and other judicial bodies are obliged to use the messaging service and other specific support services separately defined in the Act.

State administrative authorities are state bodies appointed to perform administrative tasks. These include central government authorities, i.e., the Government and ministries, as well as other administrative authorities under the Government whose territorial jurisdiction is general. State bodies under central government authorities include, for example, the Centres for Economic Development, Transport and the Environment. Examples of state agencies and institutions include state research institutes and centres, as well as specialist agencies, such as the Finnish Meteorological Institute and, among other agencies, the Finnish Competition and Consumer Authority. (HE 59/2016 vp, p. 41)

Municipal authorities are obliged to use support services when performing the tasks assigned to them by law. Municipal authorities also have the right to use support services in the performance of other tasks. Municipal authorities are most often multi-member municipal bodies, such as the council and municipal government, as well as committees, boards, and working groups. Authorities and bodies of joint municipal authorities and other inter-municipal cooperation organs are also considered municipal authorities and bodies. The definition of a municipal authority is ultimately derived from whether the body has legally mandated tasks and powers based on a legal norm. (HE 59/2016 vp, p. 41)

2.2.3.2 Exemption from the obligation to use support services

The authorities required to use support services, such as the messaging service, have been described above. According to section 7 of the Support Services Act, an entity required to use support services must apply for an exemption from the obligation to use the service from the

service provider producing the relevant support service. An exemption may be granted if it is necessary for the entity required to use the support service to use another service in its operations or part thereof for technical, operational, cost-efficiency, or information security reasons. The Ministry of Finance may, on its own initiative or at the request of the service provider, take the matter for decision if it concerns an issue of significance for the general guidance referred to in this Act or for the general guidance of information management in public administration. If the legislative proposals in the Government Proposal to Parliament on establishing the primacy of electronic communication in public administration (HE 124/2025 vp) enter into force as proposed, the rules on exemptions from the obligation to use support services would be clarified further in section 7 of the Support Services Act. To date, very few applications for exemptions from the obligation to use have been submitted.

The preparatory works of the Support Services Act state that, in light of the purpose of the Act, the grounds for exemption from the obligation to use support services should be interpreted narrowly. An exemption must be objectively necessary for the reasons referred to in the provision. Technical and operational reasons may include, for example, situations where a support service does not meet essential requirements relating to service quality or other functionality that the user organisation needs in order to perform its duties. Naturally, an operational reason for not using a support service may also be that the organisation has no need for the particular support service in its activities. Reasons related to information security include, for example, the special need to protect sensitive personal data or to meet the requirements for handling security-classified information, as well as the assessment of whether such data can be processed in support services and under what possible special arrangements. (HE 59/2016 vp, p. 41)

Cost-efficiency, together with functional considerations, may also constitute a ground for exemption from the obligation to use support services, for example, when assessing the obligation in relation to the utilisation of national and regional investments that have already been made. Cost-efficiency and functional considerations may support the integration of systems rather than the replacement of existing solutions. The assessment must be carried out taking into account, on the one hand, the characteristics of the public administration service and, on the other hand, the specific features of each common digital public administration service. For example, the cost savings resulting from the adoption of the natural person identification service are so significant for user organisations that the costs incurred by its implementation cannot reasonably constitute an obstacle to its adoption. (HE 59/2016 vp, p. 42) The obligation to use support services can therefore be regarded as strict in nature, and any deviation from it should be carefully assessed by authorities.

2.2.3.3 Entities entitled to use support services

In addition to the entities obliged to use support services, such as the messaging service, the Support Services Act also regulates actors that are entitled to use support services. Under section 5(2) of the Act, public authorities, independent public institutions, Parliament and its offices, funds outside the Government budget, as well as entities assigned to independently perform a public administration task by an Act, by a decree issued under an Act, or by a decision of a state administrative authority issued under an Act, may use all support services for the performance of the public administration task provided for by law. Municipal authorities may use all support services also in the performance of their other tasks.

In addition, under section 5(3) of the Support Services Act, entities that perform a public task on the basis of a contract founded on an Act, or on grounds other than those referred to in

subsection 2, may use other support services in the performance of that task, with the exception of identification services, the aggregation and management service for online payments, and the messaging service. The decision to provide these support services to such organisations is made by the service provider producing the relevant support service, which, where necessary, also determines whether the user organisation falls within the category of organisations referred to in the subsection in question or in subsection 2.

According to the provision-specific explanatory memorandum to section 5(3) of the Support Services Act, the intention has been to define, more loosely than in subsections 1 and 2, the right of actors connected to public administration to generally use support services in the performance of a public task. However, with regard to certain support services, it has been considered necessary to restrict the right of use, for example for reasons related to the cost-effective use of support service resources, equal treatment, and competition considerations. Actors referred to in this subsection include, for example, so-called outsourced services enabled by law and voucher-based services, in which the performance of a public task is carried out by a private entity on the basis of a contract concluded with a public authority. (HE 59/2016 vp, pp. 42–43)

2.2.3.4 Use of the messaging service

The use of the messaging service is regulated in section 3(1)(7) of the Support Services Act. According to the provision in question, the messaging service enables a user organisation and a user to send electronic messages to each other, and by using it, a document may be served either electronically or by mail. If the legislative proposals set out in the Government proposal to Parliament on legislation concerning the primacy of electronic communication in public administration (HE 124/2025 vp) enter into force as proposed, a new section 8a would be added to the Support Services Act, under which the messaging service would be used in the user organisation's electronic communication procedure. Under that section, the messaging service could also be used for sending and receiving other electronic messages between the user organisation and the user, as well as for service of documents carried out by post and for sending other letters. The section would specify the purposes for which the messaging service is used, thereby also clarifying the content of the obligation to use the service.

If the legislative proposals concerning the primacy of electronic communication in public administration referred to above enter into force as proposed, new sections 8b and 8c would be added to the Act on Common Support Services, in addition to the new section 8a. Pursuant to the new section 8b of the Support Service Act, the Digital and Population Data Services Agency, acting as the service provider, would be responsible for sending to the user the notification provided for in the new section 19a proposed to be added to the Act on Electronic Services in the same legislative proposal, the so-called alert message, when a user organisation sends a service of documents or another message to the user via the messaging service. Thanks to the alert message, it would be easier for the user to monitor messages addressed to them that have arrived in the messaging service. In addition, pursuant to the new section 8c of the Support Service Act, user organisations would be able to arrange the delivery of their letter mail by means of the so-called printing, enveloping and distribution service of the messaging service. Section 8c would aim to clarify the procedure to be followed when making use of the centralised letter mail functionality (the TKJ service) associated with the messaging service.

In order to adopt the use of Suomi.fi Messages, an organisation that is obliged or entitled to use the messaging service must apply for a right of use from the Digital and Population Data

Services Agency. Organisations subject to the obligation to use the service must apply for at least one right of use with a broad scope of use. If an organisation expands the use of the service beyond a previously granted limited right of use, it must, if necessary, apply for a new right of use. An organisation entitled to use the messaging service, on the other hand, must apply for a new right of use for each new adoption of Suomi.fi Messages.

2.2.4 Public administration clients of Suomi.fi Messages

2.2.4.1 Implementation of Suomi.fi Messages

Public administration clients of Suomi.fi Messages, i.e., natural persons, companies, and other entities, may adopt the service. For a natural person to adopt Suomi.fi Messages, they must have a personal identity code registered in the Finnish Population Information System. For companies and other entities, use of the service requires a business ID. For a company, Suomi.fi Messages may be adopted by a person who is a registered signatory of the company in the Trade Register and authorised to represent the company alone, or a person authorised by them for this purpose via Suomi.fi Authorisations. Suomi.fi Messages may also be adopted on behalf of another person, provided that the right to act on behalf of that person is recorded in the Suomi.fi Authorisations service.

Adoption and use of Suomi.fi Messages require strong electronic identification via Suomi.fi authentication. Therefore, the user must have a means of strong electronic identification that can be transmitted through Suomi.fi e-Identification and that enables them to authenticate to the service. A person acting on behalf of another must have their own means of strong electronic identification. Currently, the adoption and use of Suomi.fi Messages also require that, during authentication, information about the person’s Finnish personal identity code registered in the Population Information System is transmitted.

The adoption of Suomi.fi Messages currently requires the person’s general consent to electronic communications at the time of adoption. In addition, the person must add a valid email address to the service as the primary email address for the Suomi.fi Messages account. To activate Suomi.fi Messages, the person must enter in the Suomi.fi Messages user interface a verification code that has been sent to the email address provided at the time of adoption.

If the legislative amendments proposed in the Government proposal on the primacy of electronic communication in public administration (HE 124/2025 vp) enter into force as proposed, Suomi.fi Messages would henceforth be adopted by opening a messaging service account, which could be opened in one of two ways: either on the initiative of the authority or at the request of the user.

In the first procedure, i.e., the authority-initiated procedure, Suomi.fi Messages would be adopted for a natural person on the initiative of the authority, such that a messaging service account would be opened for the natural person by the authority without the person’s request when they authenticate to a service via Suomi.fi e-Identification. During the authentication event, the person would be informed about Suomi.fi Messages and the effects of adopting the service. In addition, the person would be asked to provide an email address for receiving notifications or to confirm that they do not wish to provide an email address. If the person provides an email address, they would need to verify it using a verification code sent to that email address. Suomi.fi Messages would become available to the person after they have confirmed the email address provided in the user interface or have confirmed that they do not wish to provide an email address. Thus, Suomi.fi Messages would be made available to the

person even if they do not provide an email address for notifications. However, in such a case, the person would be clearly informed at the time of adoption that they must monitor the messages arriving in the Suomi.fi Messages service using a browser or mobile application. Suomi.fi Messages would not become available to the person if the authentication event is interrupted before a choice regarding providing an email address is made, for example.

The authority-initiated adoption would apply only to the natural person themselves authenticating via Suomi.fi e-Identification. Suomi.fi Messages would therefore not be adopted in the above-described authority-initiated manner, for example, for a dependant, principal, grantor, or a legal entity on whose behalf a natural person is acting in the service portal in which Suomi.fi Messages would be adopted during authentication.

Adoption of Suomi.fi Messages in the first-mentioned procedure would require that the person is an adult natural person with a Finnish personal identity code registered in the population information system, and possesses a strong electronic identification method compatible with Suomi.fi e-Identification, through which the person's Finnish personal identity code is conveyed during authentication. It would also be a requirement that the person has not been assigned a guardian or confirmed a power of attorney for guardianship based on information recorded in the guardianship register referred to in the Guardianship Service Act (442/1999). Additionally, it would be required that the person uses Suomi.fi e-Identification after 12 January 2026, and that Suomi.fi Messages are not already in use for them at that time.

Once Suomi.fi Messages have been adopted through the authority-initiated procedure, the person would, during the same authentication event, receive information on how they can terminate the use of Suomi.fi Messages. If the person decides to terminate the use of Suomi.fi Messages, the service would be reactivated for them via the authority-initiated procedure six months after the termination, provided that the procedure can still be applied to the person.

In the second procedure, Suomi.fi Messages would be adopted at the request of a natural person, company, or legal entity. A natural person could adopt Suomi.fi Messages at their request, provided that the authority-initiated procedure described above does not apply to them. Adoption of Suomi.fi Messages for a natural person in this procedure would require that the person has a Finnish personal identity code registered in the population information system and possesses a strong electronic identification method compatible with Suomi.fi e-Identification, through which the person's Finnish personal identity code is communicated during authentication and with which they can authenticate to the service. The person must also give general consent for electronic communication at the time of adoption.

2.2.4.2 Use of Suomi.fi Messages

A natural person who uses Suomi.fi Messages can receive verifiable electronic service of documents, regular electronic notifications, and other electronic messages from authorities and organisations that use Suomi.fi Messages as part of their operations. The messages that arrive in the person's Suomi.fi Messages account are those that the authority has addressed to the person's personal identity code when sending the message. If the user organisation has allowed it, the person can reply to the message sent by the user organisation or start an entirely new conversation with the organisation through Suomi.fi Messages.

A person using the Suomi.fi Messages service receives a notification for each message arriving in the service in the email address registered to their Suomi.fi Messages account. A person who has the Suomi.fi mobile app and has allowed push notifications will receive, in

addition to or instead of email notifications, a push notification for each new message arriving in their Suomi.fi Messages account.

If the proposed changes to the legislation on the primacy of electronic communication in public administration (HE 124/2025 vp) come into force as proposed, natural persons, companies, and organisations who adopted the Suomi.fi Messages service before 12 January 2026 would continue to automatically receive notifications of incoming messages at the email address provided during adoption. However, those natural persons, companies, and organisations who adopt Suomi.fi Messages after 12 January 2026 will receive email notifications of incoming messages only if they provide an email address for notifications during the adoption process. If, during adoption, they confirm that they do not wish to provide an email address for notifications, they will not receive email notifications of new incoming messages. In such a case, notifications can still be enabled later, because the company, organisation, natural person, or their authorised representative may add an email address to the Suomi.fi Messages account afterwards. After that, the Digital and Population Data Services Agency would begin sending notifications to that email address. Even if a person does not provide an email address, they could still receive push notifications about new messages in Suomi.fi Messages via the Suomi.fi mobile app, provided they have the app installed and push notifications enabled. All users of the service could receive notifications in Suomi.fi Messages about messages sent to various authorities' or other organisations' service portals in accordance with the new section 19b of the Act on Electronic Services, proposed in the same proposal.

2.2.4.3 Ending the use of Suomi.fi Messages

Currently, all parties with full rights to a natural person's Suomi.fi Messages account can terminate the use of the account electronically in service settings. In that case, the person will no longer receive electronic messages in Suomi.fi Messages and will instead start receiving paper mail. The person, their legal representative, or authorised proxy may also request that the Digital and Population Data Services Agency terminate the use of Suomi.fi Messages by phone or in-person service. Digital and Population Data Services Agency has established a separate process for ending Suomi.fi Messages in situations where it is not possible to do so electronically via Suomi.fi Messages.

If the proposed changes to the legislation on the primacy of electronic communication in public administration (HE 124/2025 vp) come into force as proposed, the use of Suomi.fi Messages could be ended by closing the messaging service account. The messaging service account would be closed at the request of the person or their authorised proxy via the Suomi.fi mobile app or web service, or, if necessary, through the Digital and Population Data Services Agency customer service. Ending the use, i.e., closing the messaging service account, would mean that the person would no longer receive service of documents or other official messages electronically via Suomi.fi Messages, but would instead receive official mail in paper form. If the request to end use comes from a natural person to whom the authority-initiated procedure for Suomi.fi Messages adoption applies, a six-month period would begin, after which it would again be possible to activate Suomi.fi Messages for that person through the authority-initiated procedure. The authority-initiated procedure would not apply to other persons after the six-month period.

2.3 Other regulations concerning Suomi.fi Messages

2.3.1 Act on the Provision of Digital Services

2.3.1.1 General

The Act on the Provision of Digital Services (306/2019, hereinafter “Digital Services Act”) contains provisions on the provision of digital services by authorities. The Act applies to state authorities, state enterprises, municipal authorities, parliamentary offices, the Office of the President of the Republic of Finland, independent public institutions, the Finnish Independence Fund, the Orthodox Church and its congregations, universities and universities of applied sciences, as well as entities performing public administration duties, unless otherwise provided elsewhere in the law.

The purpose of the Digital Services Act is to promote equality in society, particularly by increasing the possibility of persons with disabilities or functional limitations to independently manage various societal functions.

Chapter 2 of the Digital Services Act regulates the provision of digital services by authorities to the public. According to section 5, subsection 1, an authority must provide everyone with the opportunity to submit electronic messages and documents related to their matters using digital services or other electronic communication methods. The purpose of this provision is to clarify the authority’s obligation to provide public administration clients with the possibility to handle their matters and other communication addressed to authorities electronically using electronic communication methods. Chapter 2 of the Digital Services Act does not apply to police investigations or pre-trial investigations. In Government proposal HE 124/2025, it is proposed that police investigations and pre-trial investigations be added to the scope of the law.

In practice, the regulation in the Digital Services Act means that an authority has an obligation to organise its service operations so that electronic transactions with the authority are possible in all services falling within the authority’s field of responsibility and competence. Because the authority is obliged to provide public administration clients with the possibility of sending electronic messages to the authority, the possibility of electronic transactions is not limited solely to the institution of proceedings. Using digital services and other electronic communication methods, it must be possible for public administration clients to interact with the authority for any reason related to their need to obtain information about the authority’s operations, the use of its services, the requirements for instituting proceedings, or other interactions.

According to section 5(1) of the Digital Services Act, the authority must also provide everyone with the opportunity to use the messaging service referred to in the Support Services Act or another sufficiently secure electronic communication method to receive electronic messages and documents from authorities in their matter if the authority is able to deliver the message or document electronically. According to the Government proposal for the Digital Services Act, the purpose of this provision is to emphasise that the authority should also actively offer public administration clients the possibility of receiving messages and documents related to their matters electronically whenever the authority is able to send the message or document electronically (HE 60/2018, p. 68). The methods and formats for delivering documents can also be regulated differently elsewhere in legislation.

The legislative history also refers to a sufficiently secure electronic transmission method, where the authority has discretion regarding which method of electronic communication is used by both the sending authority and the receiving administrative client. If the client's message has been sent to the authority via ordinary email or a form in a digital service, responding to the message may not necessarily be possible using the same transmission method, especially if the message contains confidential information. In such cases, the authority should respond either in a general manner without including confidential content or, if possible, by other means such as by phone, secure email, Suomi.fi Messages, or by letter.

2.3.1.2 Accessibility

The European Parliament and Council Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies (hereinafter the Accessibility Directive) has been implemented through the Act on Digital Services. In addition, the European Parliament and Council Directive (EU) 2019/882 on the accessibility requirements for products and services (hereinafter the Accessibility Requirements Directive) complements, in part, the accessibility requirements for digital services provided to consumers, as regulated in Chapter 3a of the Act on Digital Services. The Accessibility Directive's requirements have been applied since 2019, whereas the Accessibility Requirements Directive's requirements have been applied as of 28 June 2025.

In the Accessibility Directive, accessibility refers to the principles and techniques that must be followed in the design, development, maintenance, and updating of websites, mobile applications, and the content presented therein, so that they are more accessible to users, particularly persons with disabilities (Recital 2). In practice, the directive defines website accessibility as ensuring that content is designed so that all user groups can access the site either without assistive devices or with assistive technologies.

Accessibility, according to the Accessibility Requirements Directive, is to be achieved systematically by removing barriers and preventing their creation, preferably following universal or inclusive design approaches, thereby ensuring that persons with disabilities have an equal opportunity, on par with others, to access services and products. The directive refers to the United Nations Convention on the Rights of Persons with Disabilities (Treaty Series Nos. 26 and 27/2016). According to this Convention, this design approach "means the design of products, environments, programmes, and services to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design". Similarly, universal design in line with the Convention on the Rights of Persons with Disabilities "shall not exclude assistive devices for particular groups of persons with disabilities where this is needed". Accessibility should also not exclude the implementation of reasonable accommodations if such are required under EU law or national law. According to the Accessibility Requirements Directive, accessibility and universal design should be interpreted in accordance with General Comment No. 2 (2014) on Article 9 (Accessibility) issued by the Committee on the Rights of Persons with Disabilities (Recital 50).

Under section 7 of the Digital Services Act, a service provider must ensure that the content of its digital services is perceivable and understandable, and that the user interfaces and navigation are controllable and functionally reliable in accordance with accessibility requirements. The informational content of digital services must meet accessibility requirements when the content is made available to service users. Accessibility requirements are common standards, compliance with which ensures that the service provider meets the accessibility obligations. According to section 8(1) of the Act, a service provider may deviate

from accessibility requirements only if a prior accessibility assessment demonstrates that implementing the requirements would impose a disproportionate burden on its operations.

Accessibility and availability are part of implementing equality. Meeting accessibility requirements is essential when a public authority provides digital services. It is important that every person, regardless of disability or other functional limitation, can use a public authority's digital services on an equal basis.

2.3.2 Processing of personal and other data in Suomi.fi Messages

Under section 1(3) of the Support Services Act, the processing of personal and other data required for providing support services is subject to Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), the Personal Data Act, and the Act on the Openness of Government Activities, unless otherwise provided in the Support Services Act or other legislation.

The processing of personal data is primarily governed by the EU General Data Protection Regulation (GDPR). The regulation and its national implementation are further specified and complemented in the Personal Data Act.

The processing of personal data in Suomi.fi Messages is based on the statutory obligation of the Digital and Population Data Services Agency in accordance with Article 6(1)(c) of the General Data Protection Regulation. The Digital and Population Data Services Agency processes personal data to ensure messages reach the correct recipient, to notify users of received and unread messages, to implement official notifications and allow users to choose the delivery method, and to store event and log data to verify the accuracy of processing and investigate any errors. Processing personal data for statistical purposes or to determine the usage and costs of Suomi.fi Messages is based on performing a task carried out in the public interest, as referred to in Article 6(1)(e) of the General Data Protection Regulation. When used for statistical purposes, the data is collected and published so that no individual natural person or company can be identified.

User organisations of Suomi.fi Messages act as data controllers under the GDPR for the content of the messages they send. The Digital and Population Data Services Agency acts as a data processor on their behalf. Messages transmitted through Suomi.fi Messages in the records of user organisations may include sensitive personal data or information concerning criminal convictions or offenses. As the service provider, the Digital and Population Data Services Agency is not a party to the electronic communications and, in principle, does not have the right to read messages received by or sent from the service by natural persons or companies. Suomi.fi Messages functions solely as a messaging platform for messages sent by customer organisations. The Digital and Population Data Services Agency does not collect or process data belonging to special categories of personal data, nor information concerning criminal convictions or offenses.

Information transmitted via Suomi.fi Messages is always encrypted and travels through a secure channel, but the customer organisation, as the data controller of the message content, must always assess the service's security and data protection risks in relation to its intended use.

The Digital and Population Data Services Agency acts as the data controller for personal data related to Suomi.fi Messages when processing data associated with the administrative, operational, and technical production of the service, as well as for the content of messages it sends. According to section 11(1) of the Support Services Act, the provider of the messaging service must maintain a register of general consents provided by users for the purpose of carrying out electronic notifications related to official activities.

The Support Services Act also contains detailed provisions on the processing of personal and other data in the production of support services. Section 12(1) of the Act grants the Digital and Population Data Services Agency the right to process the personal and other data referred to in section 9 for the purpose of producing and developing the support services for which it is responsible. According to section 12(2) of the Act, the Digital and Population Data Services Agency, acting as the service provider, has the right as a data controller to process data recorded from the use of the support service under its responsibility in order to demonstrate the correctness of data processing in the support service, or otherwise for the production and development of the support service under its responsibility, as well as to ensure its functionality and information security. The data must be deleted from the register immediately after the processing is no longer justified for the purposes referred to in this subsection. The justification for processing and the necessity of such processing must be assessed at least every five years, unless otherwise provided by law. According to subsection 5 of the same section, when providing the messaging service, the service provider has the right to disclose to the user organisation the information from the register referred to in section 11(1) that is necessary for carrying out notifications and for verifying notifications performed using the messaging service.

Under section 13(3) of the Support Services Act, the service provider must retain the information in the register referred to in section 11(1), as well as any information necessary to verify the processing of the register and the notifications, unless the user organisation has other legal obligations regarding retention. The service provider must retain messages transmitted via the messaging service for two years, unless the user deletes them earlier. If the proposed changes to the legislation on the primacy of electronic communication in public administration (HE 124/2025) come into effect as proposed, this retention period would be five years, unless the user deletes the messages earlier. According to subsection 4 of the same section, the information referred to in subsection 3 must be deleted from the register immediately after there is no longer a legal basis for its processing. The data controller must assess the need to retain such information at least every five years, unless otherwise provided by law.

Currently, the register for Suomi.fi Messages stores personal data of natural persons using the service, such as personal identity codes, email addresses, or unique login codes for mobile application users. In addition, the register stores data regarding, among other things, the user’s consent to electronic delivery or its withdrawal, the user’s language preference, unique identifiers of received and sent messages, and related metadata. If the proposed changes to the legislation on the primacy of electronic communication in public administration (HE 124/2025 vp) come into effect as proposed, instead of storing consent information, the register would store information on whether the user’s messaging service account is active or closed. For a person acting on behalf of another in Suomi.fi Messages, the email address of the person acting on behalf of someone else is also stored.

In addition to these data, event and log information is recorded. Log information includes details of processing actions performed by the Digital and Population Data Services Agency

and by user organisations, as well as actions affecting the register. Event data record the user's actions while using Suomi.fi Messages.

Under section 20(1) of the Support Services Act, the Digital and Population Data Services Agency is obliged to maintain a log register of the handling of data collected from the use of its support services to ensure that the processing is lawful. The log register contains information about the data processor, the timing of the processing, and the system data or categories of data that were processed. It also records the party to whom the data have been disclosed under section 14 of the Support Services Act. According to section 20(2) of the Support Services Act, the Digital and Population Data Services Agency must retain the data in the log register for at least two years, starting from the beginning of the calendar year following their recording.

Section 21 of the Support Services Act regulates how the Digital and Population Data Services Agency may use the information stored in the log register and specifies to whom and for what purposes the data may be disclosed. According to subsection 1 of the provision, the Digital and Population Data Services Agency may use the information stored in the log register regarding the use of support services to monitor and supervise the processing of recorded data and to maintain information security. Under subsection 2, the Digital and Population Data Services Agency may disclose data from the log register to police and pre-trial investigation authorities for the purpose of investigating crimes related to the unlawful processing of data recorded from the use of support services, unless separate legislation provides otherwise regarding the disclosure of individual data to the police. Subsection 3 allows the Digital and Population Data Services Agency to disclose information from the log register concerning the use of the service to the person whose data have been processed, subject to the restrictions set out in sections 11 and 12 of the Act on the Openness of Government Activities. In addition, such information may be disclosed for another specified purpose with the explicit consent of the person concerned and the data processor identified in the log register.

The processing of personal data is supervised by the Data Protection Officer as the national supervisory authority in accordance with section 8 of the Data Protection Act. The Data Protection Act also sets out provisions on legal remedies in personal data processing and potential sanctions.

The Act on the Openness of Government Activities applies, as described above, to the confidentiality and disclosure of personal and other data required for the provision of support services, unless otherwise provided in the Support Services Act or other legislation. The Act on the Openness of Government Activities establishes the right to access information contained in public documents held by authorities, as well as the confidentiality obligations of personnel working for an authority, the secrecy of documents, and other necessary restrictions to protect public and private interests. It also sets out the duties of authorities to implement the purposes of the Act. According to section 4, the Act on the Openness of Government Activities applies to authorities, but subsection 2 clarifies that provisions concerning authorities also apply to organisations, institutions, foundations, and private individuals performing public duties when exercising public authority under a law, regulation, or other legal provision.

Section 1 of the Act on the Openness of Government Activities sets out the principle of publicity, according to which documents held by authorities are public unless otherwise provided in this or other legislation. Chapter 3 of the Act on the Openness of Government

Activities regulates the right to access information contained in a document, while Chapter 4 governs the provision of such information. Chapter 6 of the Act addresses confidentiality obligations and the types of documents that must be kept secret. Section 24 of the chapter in question specifies the most common grounds for confidentiality. In turn, Chapter 7 of the Act contains provisions on exceptions to confidentiality and the cessation of secrecy. Section 26 of the Chapter in question defines the general grounds for disclosing information that would otherwise be confidential.

The activities of authorities sending Suomi.fi messages as well as the operations of the Digital and Population Data Services Agency are subject to the Act on the Openness of Government Activities. Documents sent to public administration clients through the Suomi.fi Messages service by user organisations may constitute official documents of the authority and are therefore governed by the provisions of the Act on the Openness of Government Activities. In addition, messages sent via the Suomi.fi Messages service may contain information that must be kept confidential under the Act, in which case the confidentiality provisions of the Act on the Openness of Government Activities must be observed.

2.3.3 Act on Information Management in Public Administration

According to section 1(3) of the Support Services Act, the management of information and the use of information systems related to the provision of support services are governed by the Act on Information Management in Public Administration (906/2019, hereinafter Information Management Act), unless otherwise provided by the Support Services Act or other legislation.

The Information Management Act sets out the general obligations of public authorities regarding information management and the use of information systems. It ensures that authorities manage their data consistently and with high quality, and that the processing of information is secure and in line with the principle of openness. The purpose of the Act is also to enable the safe and efficient use of authorities' data resources and to promote interoperability between information systems and data repositories. The Information Management Act applies to the management of information and the use of information systems when public authorities process information resources, unless otherwise provided in law. The Act also applies in certain respects to private individuals and organisations, as well as to public-law entities that do not act as authorities, insofar as they perform public administration tasks. In addition, the Act applies in certain respects when these entities exercise public authority as referred to in section 4(2) of the Act on the Openness of Government Activities, or when that Act has been specifically made applicable to their activities.

Chapter 2 of the Information Management Act contains provisions on the planning and description of information management. It is the responsibility of information management entities, such as state agencies, to ensure that information management is organised appropriately in accordance with section 4(2) of the Act. Under section 5 of the Act, an information management entity must also maintain an information management model that defines and describes information management in its operating environment as well as assess changes and impacts related to significant administrative reforms and the deployment of information systems that affect the planned content of the information management model.

Chapter 4 of the Act contains provisions on information security, including obligations regarding the security of information resources and information systems, as well as the communication and preparedness measures related to disruptions. For example, section 14 of

the Information Management Act requires that a public authority implement data transfers over public networks using encrypted or otherwise secured transmission methods when the information being transferred is confidential. In addition, the data transfer must be arranged so that the recipient is verified or identified in a sufficiently secure manner before gaining access to the confidential information being transferred.

Chapter 4a of the Information Management Act contains provisions on cybersecurity obligations in the public administration sector, implementing the NIS2 Directive (EU) 2022/2555, including the duties related to cybersecurity and the monitoring of compliance. Certain authorities and specific activities of authorities are excluded from the scope of Chapter 4a, as listed in section 3(3) of the Act. The Digital and Population Data Services Agency is not excluded from the scope of Chapter 4a and is therefore required to comply with the cybersecurity obligations set out in Chapter 4a of the Information Management Act.

Chapter 5 of the Information Management Act regulates the creation of information resources and the methods of electronic data transfer. Under section 24 of the Information Management Act, a public authority may transfer data via technical interfaces to entities other than another public authority, provided that the receiving entity has a legally established right to access and process those data. A technical interface may be opened once the conditions set out in section 22 are met, in accordance with the provisions of that section. The public authority providing the data must, when necessary, ensure that the receiving entity complies with the obligations on data processing established in the Information Management Act.

2.3.4 Other general administrative laws and the Non-Discrimination Act

The Digital and Population Data Services Agency, as the service provider of the messaging service, has the task of providing support services under official duty while complying with the general laws governing public authority activities. In addition to the laws described in section 2.3 of this chapter, the general administrative laws include, for example, the Act on Electronic Services, discussed in section 2.1.1 above, as well as the Administrative Procedure Act, the Language Act (423/2003), and the Sámi Language Act (1086/2003).

The Administrative Procedure Act regulates, among other things, the equal treatment of individuals dealing with public authorities, the principles of service, the duty to provide guidance, the processing and initiation of administrative matters, as well as the notification of administrative decisions and other documents. For example, the principle of service laid down in section 7 of the Administrative Procedure Act obliges authorities to organise proceedings and case handling in a manner that ensures the person dealing with the administration receives proper services and that the authority can carry out its tasks effectively.

The Language Act guarantees every person the right to use their own language, either Finnish or Swedish, in courts and other public authorities. The Language Act provides, among other things, the right to use Finnish and Swedish when dealing with public authorities and safeguards linguistic rights. The Sámi Language Act, in turn, safeguards, among other things, the right of the Sámi people to use their own language in courts and when dealing with public authorities.

In addition to general administrative laws, when producing the Suomi.fi Messages messaging service, the service provider, i.e., the Digital and Population Data Services Agency, must comply with the general administrative law principles set out in section 6 of the Administrative Procedure Act. These principles include, for example, the general requirement

to treat individuals using the services of the administration equally. Closely linked to this is the Non-Discrimination Act (1325/2014), whose purpose is, among other things, to promote equality and prevent discrimination. This act applies to both public and private activities. Section 5 of the Non-Discrimination Act establishes the obligation of a public authority to promote equality in its operations. Under this section, the authority must assess how its activities affect different population groups, evaluate how equality is otherwise realised in its operations, and take necessary measures to promote the realisation of equality. The Act also lays down, among other things, the prohibitions of discrimination and countermeasures and the grounds for justifying different treatment.

2.3.5 Act on Electronic Communications Services

The purpose of the Act on Electronic Communications Services (917/2014) is, according to section 1 to ensure the confidentiality of electronic communications and the protection of privacy, among other things. According to the definitions in section 3 of the Act, a communications provider means a telecommunications operator, corporate subscriber, or any other entity that transmits electronic communications other than for personal or comparable customary private purposes. Further, according to section 3(37) of the Act, a communications service refers to a service that consists wholly or mainly of the conveyance of communications in a communications network, a transmission and broadcasting service in a mass communications network, and an interpersonal communications service.

The Communications Authority (currently the Finnish Transport and Communications Agency, Traficom) issued an opinion on 28 April 2016 (document number 1260/04/2016) to the Transport and Communications Committee on the Government Proposal to Parliament for Acts on Central Government's Joint e-Service Support Services and amendments to the Act on the Arrangement of State's Common ICT Services (HE 59/2016 vp). According to the Communications Authority’s assessment at the time, the messaging service proposed in the proposal would, by default, be provided in the role of a communications provider as defined in section 3(36) of the Information Society Code (currently the Act on Electronic Communications Services). According to the provision in question, a communications provider means a telecommunications operator, a corporate subscriber, or any other party that conveys electronic communications for other than personal or comparable private purposes. In offering a messaging service, the Communications Authority stated that, in principle, the obligations in Chapter 17 of the Act on Electronic Communications Services must be observed, concerning the processing of electronic messages and transmission data, as well as the general obligation in section 247 of the Act to ensure information security. This interpretation aligns with the Communications Authority’s case law, where, for example, Posti (the Finnish postal service) has been considered a communications provider when providing its Netposti service.

Chapter 33 of the Act on Electronic Communications Services regulates information security, incident management, and notification of incidents. However, the Act on Electronic Communications Services does not apply to trust services referred to in Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation), i.e., the provision of trust services under the eIDAS Regulation. The eIDAS Regulation, as well as cybersecurity-related regulation and supervision, are explained in more detail in Chapters 2.3.6 and 2.3.7 of this proposal.

2.3.6 eIDAS Regulation

The eIDAS Regulation established an interoperability framework for electronic identification with the aim of enabling electronic identification means issued in one Member State to be used for authentication to public electronic services in another Member State. Additionally, the regulation aims to harmonise the rules on trust services across the EU. On 11 April 2024, the European Parliament and the Council adopted Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (hereinafter the "eIDAS amending regulation"). The eIDAS Regulation itself is a directly applicable legislation in the Member States. However, in certain matters, the regulation leaves national discretion to the Member States.

According to Article 2(1) of the eIDAS Regulation, the regulation applies to electronic identification schemes notified by a Member State and to trust service providers established in the Union. According to Article 3(19), a trust service provider is defined as a natural or legal person who provides one or more trust services, either as a qualified or non-qualified trust service provider. A qualified trust service provider, according to Article 3(20) of the eIDAS Regulation, is a trust service provider who provides one or more qualified trust services and has been granted approved status by the supervisory body.

A trust service, according to Article 3(16) of eIDAS, is an electronic service normally provided for remuneration. In addition, for a service to qualify as a trust service, it must consist of one of the tasks listed in the article. According to subparagraph (k), one such task is the provision of electronic registered delivery services. An electronic registered delivery service, according to Article 3(36), means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

Under Article 3(17) of eIDAS, a qualified trust service is a trust service that meets the applicable requirements set out in the eIDAS Regulation. Obtaining qualified trust service status is at the discretion of the service provider, as stated in Article 21. However, the regulation of non-qualified trust services under eIDAS is not optional. The eIDAS rules apply automatically if the definitions of a trust service and a trust service provider are fulfilled.

The security and notification requirements applicable to trust service providers are regulated by the NIS2 Directive and, at the national level, by the Cybersecurity Act (124/2025). These security requirements apply to both qualified and non-qualified trust service providers. In addition, non-qualified trust service providers are subject to Article 19a of the eIDAS amending Regulation, which sets requirements for risk management and incident reporting. Pursuant to Article 19a(2), the Commission adopted Implementing Regulation (EU) 2025/2160 on 27 October 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards, specifications and procedures for the management of risks to the provision of non-qualified trust services. According to Article 19a(2), compliance with these standards, technical specifications, and procedures is deemed to satisfy the requirements set out in the article.

During the preparation of the proposal, it was assessed that the Suomi.fi Messages messaging service would be considered a non-qualified trust service under the eIDAS Regulation. As such, it must meet the general security, risk management, and incident reporting requirements

set out in the above regulations. The Digital and Population Data Services Agency has not, to date, applied for qualified trust service status for the Suomi.fi Messages service.

The Cybersecurity Centre of the Finnish Transport and Communications Agency (Traficom) supervises compliance with the eIDAS Regulation. Digital and Population Data Services Agency also acts as an appeals authority in matters concerning the operation of trust services. For non-qualified trust service providers, Digital and Population Data Services Agency supervises them only on the basis of incident reports submitted by the providers or complaints filed about the services.

2.3.7 Cybersecurity regulation and supervision

The requirements and supervision of cybersecurity under the NIS2 Directive are implemented nationally through the Cybersecurity Act and, for the public administration sector, through the Information Management Act. As noted in section 2.3.3, the Digital and Population Data Services Agency is obligated to comply with the cybersecurity obligations under Chapter 4a of the Information Management Act. According to section 18(h) of the Information Management Act, the Transport and Communications Agency supervises compliance with the obligations set out in Chapter 4a and under the NIS2 Directive in the public administration sector.

Given that the Suomi.fi Messages service is considered a non-qualified trust service provider under the eIDAS Regulation, the Cybersecurity Act also applies to it. In section 2 of the Cybersecurity Act, the definitions refer to the concepts of a qualified trust service provider (point 6) and a trust service provider (point 9) mentioned in section 2.3.6, following the definitions in the eIDAS Regulation. According to section 3(2)(2) of the Act, it also applies to any entity that is, in any case, a trust service provider.

Section 26 of the Cybersecurity Act regulates the authorities responsible for supervising compliance with the Act, the regulations issued under it, and the provisions adopted under the NIS2 Directive. Under section 26(1)(1), the Transport and Communications Agency supervises the entities listed in Annex I, points 1–7, and Annex II, points 1–5, to the extent applicable.

2.4 Suomi.fi Messages as a public administration task

According to section 124 of the Constitution, a public administration task may be delegated to a party other than a public authority only by or under an Act if this is necessary for the appropriate performance of the task and if basic rights and liberties, legal remedies and other requirements of good governance are not endangered. However, a task involving significant exercise of public powers can only be delegated to public authorities. This proposal introduces regulation that would make it possible to delegate a task assisting a public administration function to an entity other than a public authority.

According to section 21 of the Postal Act (415/2011), a universal service provider must ensure the availability and proper implementation of the mail-based notification procedure provided for in the Act throughout the country. Under Subsection 2, a public authority may also agree with a postal company other than the universal service provider on the implementation of the mail-based notification procedure set out in the Act. The authority may enter into such an agreement only with a postal company that is capable of properly carrying out the task.

In the Government proposal amending the Postal Act, the relationship of the provisions on collection and delivery under section 21 to section 124 of the Constitution was assessed comprehensively. It was noted that these provisions are particularly relevant to public administration because, in a significant portion of administrative matters, initiating a case, sending requests for information and responses, and notifying decisions all take place by post. (HE 52/2022 vp, p. 117)

According to the reasoning in the cited proposal, authorities do not automatically use the universal service provided by Posti Oy, but instead negotiate postal services separately with Posti Oy. Not all authorities necessarily use the letter services provided by Posti Oy, as they may also enter into commercial agreements with other postal companies for letter services. The universal service can generally be considered a basic infrastructure service as defined in legislation, rather than a public administration task under section 124 of the Constitution. Liability provisions related to official duties apply, by their nature, to Posti Oy only when it performs a public administration task as a universal service provider. The advice of receipt procedure has been regarded as an important form of administrative procedure, which is why the universal service provider is considered, in this respect, to be carrying out a public administration task as referred to in section 124 of the Constitution. Carrying out a public administration task also entails liability under the Criminal Code (39/1889). When the universal service provider, under an agreement with a public authority, ensures the statutory notification procedure, this activity can be regarded as performing a public administration task under section 124 of the Constitution. Furthermore, the reasoning notes that an ordinary notification is currently the most common form of notification, and the liability provision in section 21 of the Postal Act has been drafted to apply generally to tasks related to the notification procedure. The current provision does not limit its application only to the advice of receipt procedure, for example. However, in the reasoning, the legal situation at the time was considered unclear, which is why the provision has been clarified, particularly regarding the allocation of official liability. (HE 52/2022 vp. pp. 29–30)

According to the reasoning for section 21(2) of the Postal Act, the subsection would be amended so that a public authority could agree to have the notification procedure carried out by a postal company other than the universal service provider. Carrying out the notification procedure would mean distributing and delivering notifications to recipients. The public authority could enter into such an agreement only with a postal company that has the capacity to properly perform the task. In addition to the universal service provider, many other postal companies also distribute official letters and ordinary notifications delivered by post. The amendment would clarify the legal situation and grant, besides the universal service provider, other postal companies a statutory right to carry out the postal notification procedure considered a public administration task under the law. The amendment would not transfer the performance of the notification procedure away from the universal service provider; it would merely establish the legal basis for the fact that notifications may be distributed not only by the universal service provider but also by other postal companies distributing official letters. (HE 52/2022 vp, p. 81)

Section 2b(1)(3) of the Act on the Finnish Tax Administration (503/2010) provides for the delegation of electronic notification and the management of related consents to a private entity. According to the reasoning in the Government Proposal, with regard to electronic notifications, a private entity would manage the consent given by the customer for electronic notifications and would also forward the documents to an electronic notification service used by the customer. Substantively, the customer would provide consent to the Tax Administration, even if the technical maintenance is carried out by a private party. The

documents would be delivered to a secure electronic notification service whose security has been approved by the Tax Administration. Such notification services could include, for example, the citizen's service account or NetPosti. In its opinion PeVL 30/2012 vp, the Constitutional Law Committee concluded that transferring the technical tasks mentioned in the provision is appropriate, and that the regulation otherwise meets the Committee's established requirements for transferring such tasks. (HE 76/2012 vp, p. 57)

Both postal and electronic notification procedures concern the same statutory procedure, which is considered an essential part of administrative proceedings. Notification by the authority, as provided in the Administrative Procedure Act, is part of handling an administrative matter and a prerequisite for exercising the right of appeal (HE 72/2002 vp, p. 116). The purpose of both postal and electronic notifications is to ensure that the statutory obligation to notify by the authority is fulfilled.

Section 5 of the Support Services Act provides a statutory obligation for authorities to use a messaging service, which can be used in the user organisation's electronic notification procedure in accordance with section 3(1)(7) of the same Act. If the proposed changes in the Government Proposal on prioritising electronic notification in public administration (HE 124/2025 vp) come into force as proposed, the purpose of using the messaging service would be further clarified by explicitly regulating it in the proposed section 8a of the Support Services Act.

In addition to authorities being obliged under the Support Services Act to use the messaging service, the provision of the service is a statutory task assigned to the Digital and Population Data Services Agency. Thus, this is a service explicitly established by law, for which the Act sets out specific requirements regarding its implementation and operation. Furthermore, the messaging service is regulated under the Digital Services Act, whose section 5 obliges authorities to provide everyone with the possibility to use a messaging service or another sufficiently secure electronic communication method for receiving messages. The messaging service ensures that authorities can deliver notifications and messages in a legally compliant, sufficiently secure, and reliable manner.

Both verifiable and regular electronic notifications can be sent via the messaging service, and the service allows the handling of confidential documents. The messaging service thus differs from the other electronic communications referred to in section 18(2)(3) of the Government proposal to Parliament for legislation on the primacy of electronic communication in official matters (HE 124/2025 vp), in that its use is explicitly mandated for authorities and it, in principle, enables the service of notifications for documents of all content types. If the proposed changes in the Government Proposal (HE 124/2025 vp) come into force as proposed, the messaging service would differ from other notification channels referred to in the Act on Electronic Services in that a notification could be delivered to the messaging service account of a person using the service without their consent, which would emphasise the service's significance in electronic notification procedures.

As noted above, the task of delivering notifications is, by its nature, an integral part of administrative procedures. Furthermore, when assessing the relationship of this task to section 124 of the Constitution, an analogy can be drawn from the evaluation made in the preparatory work for the Postal Act regarding the nature of the notification procedure. Based on the above, it can be concluded that the messaging service plays a central role in authorities' electronic notification procedures. Taken together, these factors support the view that providing the messaging service should be considered a public administration task. This conclusion is also

in line with the view presented in the response given to the Administrative Committee during the parliamentary consideration of the Government Proposal that led to the enactment of the Support Services Act (HE 59/2016 vp, HaV, 2 June 2016).

2.5 Private digital mail services

2.5.1 The market for private digital mail services in Finland

Private digital mail services refer to commercial services where, at their simplest, the service user has access to an electronic mailbox for the centralised receipt of messages sent by various organisations and operators. The services may also include other functionalities, such as the ability to archive incoming documents and messages. In general, the purpose of private digital mail services is often to serve as more than just a digital mailbox, but rather as a comprehensive service that brings together the everyday administrative tasks of citizens and businesses. This is not, for example, an email service based solely on receiving and sending messages among an unlimited group of people.

Since 2001, Posti Group Corporation (hereinafter Posti) has been offering an electronic mailbox service called NetPosti, which Finnish citizens can use to receive electronic messages from companies, organisations, and public authorities. NetPosti was renamed OmaPosti in 2019, and Posti continues to offer this service. Currently, OmaPosti is a digital mailbox service that allows users to receive electronic letters from companies, organisations and, authorities, as well as track and manage their parcel deliveries. The user can also pay invoices directly via OmaPosti and archive electronic letters and invoices. The service can be used via a web browser or the OmaPosti mobile app, and users receive notifications of new mail arriving in the service via email or the mobile app.

Currently, in addition to Posti, Kivra Oy (hereinafter Kivra) also provides private digital mail services to consumers and businesses in Finland. Kivra is a company originally founded in Sweden in 2011 and established in Finland in 2018. It has been offering its digital mail service in Finland since early 2020. Kivra's Kivra digital mailbox service allows users to receive electronic mail from various verified companies, organisations, and authorities, pay bills, archive documents as well as receive payslips and admission tickets. The user may also authorise another person to read messages received by the service. Kivra can be used with a web browser or the Kivra mobile app, and users receive notifications of new messages via email or the mobile app.

Kivra and OmaPosti are free of charge for users who receive digital mail through these services. Companies and organisations that send messages via digital mail services pay digital mailbox operators for the delivery of messages. For example, companies and organisations pay a ‘digital stamp fee’ for the use of the Kivra service for the submission of documents. The fact that the largest possible user base promotes the digital mail operator's business opportunities among businesses, organisations, and public authorities has an impact on the free provision of services.

In general, the digital mail market is characterised by what is known as the network effect, which means that the benefit a user derives from a service depends on the extent to which others use the same service. In the digital mail market, this means that the more organisations send messages to a particular digital mail service, the more the digital mail service benefits and attracts users. The effect also works in reverse, in that the fewer users a particular digital mail service has, the less incentive organisations have to send messages to that digital mail

service. This may lead to market concentration and, as the industry stabilises, it may become challenging for new players to enter the market.

At present, no other private operators offer similar digital mailbox services on the Finnish market or the possibility to receive, for example, electronic messages from public authorities in a centralised manner. However, based on a report on private digital mail services commissioned to support the legislative process, there may be interest in the banking sector in forwarding digital official mail. Interest could also be found in the telecommunications operator sector, whose services use strong authentication and functionalities comparable to digital mail. However, operators in these sectors do not currently offer solutions for transmitting official communications.

Through the Kivra and OmaPosti services, users can receive electronic messages not only from private operators but also from public authorities. The organisations that send messages through the services currently include public authorities and public administration actors, such as wellbeing services counties and agencies. Public administration actors who send electronic messages via private digital mail services agree on the delivery of messages with private digital mail services separately.

Legislation does not actually prevent authorities or other public actors from using private digital mail services to communicate with their customers, even if the authorities are subject to the obligation to use Suomi.fi messages in accordance with the Support Services Act. As a general rule, authorities should apply for an exceptional permit under section 5 of the Support Services Act (or section 7 if the proposed changes in the Government Proposal on the primacy of electronic communication in public administration (HE 124/2025 vp) come into force as proposed) if they do not use the messaging service in accordance with the statutory obligation to use it. The chosen method of communication, such as using private digital mail services, must nevertheless meet the legal requirements, for example, regarding information security. For instance, the Act on Electronic Services, which regulates the delivery of authorities' notifications, is technology-neutral, meaning that an authority may deliver documents electronically in a manner it considers appropriate. However, the chosen method of delivery must comply with the requirements of the Act on Electronic Services. For example, in the case of verifiable electronic notifications, section 18(3) of the Act on Electronic Services requires that the recipient of the notification be identified using secure and verifiable technology. Requirements relating to information security and confidentiality may also impose limitations on the method of notification.

For documents other than notifications, the legislation governing the matter being communicated guides not only the security and confidentiality requirements but also the manner in which an authority may deliver messages electronically. Section 5(1) of the Digital Services Act also guides authorities in selecting the method for delivering messages. According to this provision, an authority must provide everyone with the opportunity to use a messaging service as referred to in the Support Services Act, or another sufficiently secure electronic transmission method, for receiving the authority's electronic messages and documents regarding their matter, if the authority is able to deliver the message or document in electronic form. This obligation applies to the authority regardless of whether it is required to use the Suomi.fi Messages service.

2.5.2 Regulation of private digital mail services

2.5.2.1 Act on Electronic Communications Services

As described in section 2.3.5, during the enactment of the Support Services Act, the Finnish Communications Regulatory Authority (now the Finnish Transport and Communications Agency, Traficom) issued a statement noting that a messaging service would be provided in the role of a communication intermediary in accordance with the Act on Electronic Communications Services. In its statement, the Authority notes that this interpretation would correspond to the Authority's case law, in which entities such as Posti has been considered a communications provider when providing its Netposti service. Based on this policy regarding the Netposti service (now OmaPosti), other private digital mail services, alongside Suomi.fi Messages, are also considered to fall within the scope of the Act on Electronic Communications Services.

As noted in section 2.3.5, however, the Act on Electronic Communications Services does not apply to private digital mail services with regard to security, incident management, and incident notification, because the Act does not apply in cases where a trust service provider under the eIDAS Regulation is concerned. The eIDAS Regulation, as well as cybersecurity-related rules and supervision, are described in more detail with respect to private digital mail services in sections 2.5.2.3 and 2.5.2.4 of this proposal.

2.5.2.2 Regulation and supervision of personal data processing

Private digital mail operators are required to comply with the applicable personal data processing legislation, primarily the EU General Data Protection Regulation (GDPR), when processing personal data in connection with the digital mail services they provide. Private digital mail operators apply the rules on personal data processing independently, meaning that they determine, for example, the legal bases for processing, purposes of use, and other details of personal data processing in relation to the services they offer on their own authority.

Chapter VI of the GDPR provides for independent supervisory authorities tasked with monitoring compliance with data protection rules. In Finland, the Data Protection Ombudsman acts as the supervisory authority in accordance with section 8 of the Data Protection Act. According to section 9 of the Act, the Data Protection Ombudsman has an office that includes at least two deputy ombudsmen and a necessary number of rapporteurs and other staff familiar with the Ombudsman's area of responsibility. The duties and powers of the Data Protection Ombudsman are set out in Article 55–59 of the GDPR. The supervisory role of the Data Protection Ombudsman is based in particular on Article 57(1)(a) of the GDPR, which requires each supervisory authority to monitor and enforce the application of the regulation within its territory. Section 14 of the Data Protection Act further provides that the Data Protection Ombudsman has other duties and powers as laid down in this Act or other laws. In addition, the Data Protection Ombudsman supervises compliance with the Act on the Processing of Personal Data in Criminal Matters and in connection with Maintaining National Security (1054/2018) under the provisions of its Chapter 8. Data protection regulation and its general supervision cover extensively the processing of personal data under the Support Services Act. Supervision of data protection also applies to the processing of personal data in private digital mail operations.

According to section 303(1) of the Act on Electronic Communications Services, the task of the Finnish Transport and Communications Agency (Traficom) is to supervise compliance

with this Act and the provisions and decisions issued under it, unless otherwise provided in this Act. Traffic and communication metadata may include personal data, such as IP addresses or email addresses, and Traficom is responsible for supervising the processing of such personal data in accordance with the Act on Electronic Communications Services.

2.5.2.3 eIDAS Regulation

As noted above, the eIDAS Regulation sets out rules for qualified and non-qualified trust service providers, which are subject to the security and notification requirements established by the NIS2 Directive and, consequently, in national cybersecurity law. Non-qualified trust service providers are also subject to Article 19a of the eIDAS amending regulation, which sets requirements for risk management and incident reporting.

Referring to the point about messaging services in section 2.3.6, this proposal assumes that private digital mail services would be considered trust services under the eIDAS Regulation, and therefore must comply with the general security, risk management, and incident reporting requirements laid out in the aforementioned regulations. This is based on the fact that private digital mail services are generally publicly available and offered for a fee. They also meet the definition of an electronic registered delivery service. Private digital mail service providers have not yet applied for approved trust service status for their services. As such, they would be considered non-qualified trust service providers.

Under the eIDAS Regulation, private digital mail operators, as trust service providers, would also be required to comply with accessibility requirements for trust services under Article 15 of the eIDAS Regulation. According to this article, trust services must be made available in a clear and understandable language, in accordance with the United Nations Convention on the Rights of Persons with Disabilities and the Accessibility Directive. In addition, under Article 13(1) of the eIDAS Regulation, trust service providers are responsible to a natural or legal person for damage caused intentionally or negligently that results from the failure to comply with the obligations set out in this Regulation. According to the Article, any natural or legal person who has suffered material or non-material damage because the trust service provider has violated the Regulation has the right to seek compensation in accordance with Union law and national legislation. For a non-qualified trust service provider, the burden of proof regarding intent or negligence lies with the natural or legal person seeking compensation for the aforementioned damage.

Since private digital mail services would be non-qualified trust service providers, the Cybersecurity Centre of the Finnish Transport and Communications Agency, which supervises compliance with the eIDAS Regulation, monitors them only on the basis of incident notifications made by service providers or complaints made about the services. Digital and Population Data Services Agency also acts as an appeal authority in matters concerning the operation of trust services.

2.5.2.4 Cybersecurity regulation and supervision

The cybersecurity requirements laid down in Chapter 4a of the Information Management Act do not apply, according to section 3 of the Information Management Act, to a private operator performing a public administration task. Thus, as referred to in the Information Management Act, the public administration sector's cybersecurity requirements and their supervision do not apply to private operators performing a public administration task. However, private digital mail services are subject to the Cybersecurity Act in situations where the private operator is

considered to be engaging in an activity referred to in Annex I of the Cybersecurity Act. For private digital mail services, the activity referred to in the Annex could correspond to point 6: digital infrastructure. For example, according to subpoint g of point 6, trust service providers engaged in an activity covered by the Annex, which, as noted in section 2.5.2.3, would include private digital mail services, are subject to these provisions.

In section 2 of the Cybersecurity Act, the definitions refer to the concepts of a qualified trust service provider (point 6) and a trust service provider (point 9) mentioned in section 2.3.6 and 2.5.2.3, following the definitions in the eIDAS Regulation. According to section 3(2)(2) of the Act, it also applies to any entity that is, in any case, a trust service provider. The requirements of the Cybersecurity Act therefore apply to those private digital mail services that are trust service providers as referred to in the eIDAS Regulation. As noted in section 2.3.7, compliance with the Cybersecurity Act, its regulations, and the provisions issued under the NIS2 Directive is supervised for such operators by the Finnish Transport and Communications Agency Traficom.

2.5.2.5 Requirements under Chapter 4 of the Information Management Act

Chapter 4 of the Information Management Act regulates requirements for information security. The provisions of the chapter also obligate private operators when they perform public administration tasks. Private digital mail service providers have not yet performed public administration tasks, so the information security requirements of Chapter 4 of the Information Management Act have not applied to them. No separate supervisory authority has been established for Chapter 4 of the Information Management Act.

2.5.2.6 Act on Information Security Inspection Bodies

The Act on Information Security Inspection Bodies (1405/2011) regulates, according to Section 1, a procedure through which companies can reliably demonstrate to third parties that a certain level of information security has been implemented in their operations. According to the explanatory memorandum for the section (HE 45/2011 vp), inspection bodies and the reliability of their operations are important for companies as they develop information security within their organisations. Through inspection bodies, companies can also consistently prepare for situations in which their level of information security is an absolute requirement for success in procurement competitions, such as in international and national procurements or collaborative projects in the defence and security sectors.

Section 9 of the Act provides more detailed regulations on the tasks of an inspection body when performing an information security inspection task. According to section 10 of the Act, multiple different criteria or guidelines can be used as bases for information security inspections, depending on the selection of the inspected target.

2.6 Assessment of the current situation

2.6.1 Utilisation of Suomi.fi Messages

The number of citizens who have adopted Suomi.fi messages has increased over the years by approximately 15,000 users per month, i.e., about 180,000 users per year, under the current situation in which the adoption of Suomi.fi messages requires the consent of the public administration client. Authorities have attempted to increase the number of users through communication measures, but despite these measures, Suomi.fi Messages have been used only

to a limited extent and remain poorly known. On 12 May 2025, the Digital and Population Data Services Agency, as part of a programme primarily aimed at promoting digital government communication, encouraged individuals who did not yet have Suomi.fi Messages in use to start using the Messages service together with Suomi.fi e-Identification. As a result, the number of Suomi.fi Messages users had increased by approximately 700,000 new users by mid-November 2025. In total, there were about 2.4 million users at that time. The largest increase in users occurred during the first weeks after the launch of the encouragement campaign. If the proposed changes to the legislation the primacy of electronic communication in public administration (HE 124/2025 vp) come into force as proposed, the number of Suomi.fi message users could increase from the current level to possibly 4.4 million.

Authorities have not fully complied with the obligation to use Suomi.fi messages as referred to in section 5 of the Support Services Act. According to the 2022 audit report of the National Audit Office of Finland (VTV), the use of the service in public administration has so far been limited, and the service utilisation rate is significantly lower than that of corresponding services in other Nordic countries (VTV audit reports 10/2022). The limited use of the service has partly been due to the fact that citizens and businesses had not previously adopted Suomi.fi messages comprehensively, and the number of end users of the service has therefore been limited. Public administration has also perceived integration into the service as difficult and expensive, and it has not always been seen as worthwhile due to the low number of users. Also, for example, the absence of some technical functionality, parallel communication methods, and preconceived notions about the service have restricted the adoption of the service across different authorities.

Suomi.fi Messages have been used only to a limited extent in the municipal sector, for example. According to the municipal digital survey (2024) conducted by the Association of Finnish Local and Regional Authorities, only a few municipalities have adopted Suomi.fi Messages comprehensively in the services of different functions and sectors. In wellbeing services counties, Suomi.fi Messages have been used even more limitedly than in the municipal sector, even though the wellbeing services counties are also legally obliged to use the messaging service, i.e., Suomi.fi Messages. In the current situation, a quarter of wellbeing services counties have not adopted Suomi.fi Messages at all. Half of the wellbeing services counties that have adopted the service send only a few hundred Suomi.fi messages annually, meaning that the service is in use in a very limited part of the regions' operations.

Authorities and public administration organisations, however, have increasingly adopted the Suomi.fi messages service. According to the list of organisations and services using Suomi.fi Messages maintained by the Digital and Population Data Services Agency, approximately 390 authorities and public administration entities use Suomi.fi Messages to send messages to their clients so far. The number of authorities using Suomi.fi Messages is expected to increase in the near future if the changes proposed in the Government proposal on the primacy of electronic communication in public administration, which among other things, clarify the content of the obligation to use support services, enter into force as proposed (HE 124/2025 vp). During 2025, the adoption of Suomi.fi Messages has progressed especially in wellbeing services counties and at the Social Insurance Institution of Finland (Kela), which started using Suomi.fi Messages in June 2025. By November 2025, it had already sent over 2.2 million Suomi.fi Messages.

The increased use of Suomi.fi Messages by both government customers and khas led to a rise in the number of Suomi.fi Messages sent during 2025, thereby enabling savings in public administration even before the priority of electronic notification procedures comes into force.

During 2025 (situation as of 20 November 2025), a total of 23 million Suomi.fi messages have been delivered. The number has increased by approximately 50% compared to the 2024 reference period. Among the most significant authorities sending Suomi.fi Messages, the number of Suomi.fi messages delivered by the Tax Administration increased by 62% during the reference period, by the Transport and Communications Agency (Traficom) by 43%, by the Police by 72%, and by employment services (municipalities from the beginning of 2025) by 88%.

Despite the obligation to use Suomi.fi Messages under the Support Services Act, authorities may also use other electronic channels to deliver messages and notifications. For example, authorities may have their own electronic service platforms, to which authorities' messages and documents are delivered. As previously noted, some authorities also use private digital mail services to deliver electronic messages and notifications to administration clients. However, it is unclear to what extent authorities subject to the usage obligation have assessed the use of other communication services in relation to the necessity requirement for deviating from the usage obligation, since no applications for deviation from the usage obligation have so far been submitted regarding Suomi.fi Messages.

In the current situation, authorities' practices regarding the delivery methods of messages and notifications therefore vary, and not all official correspondence is delivered centrally through the Suomi.fi Messages service. Administration clients may thus receive authorities' messages and notifications through multiple channels, which complicates the management of electronic mail received from authorities.

The user interface of Suomi.fi Messages has been assessed as inadequate relative to the needs of business users and business messages. For example, the service does not allow restricting service by subject on behalf of and within the company, or, for instance, in a situation where the company uses an accounting firm. The signatory or authorised representative currently gains access to process all messages sent to or from the company, which has been perceived as problematic. Suomi.fi Messages are currently assessed to primarily serve sole proprietors or small businesses, where the authorised signatory handles all administrative interactions of the company with authorities. The challenges concerning legal persons in the Suomi.fi Messages user interface currently still require significant development work, which is why the regulation under the Support Services Act cannot yet be examined for legal persons within the scope of this project.

2.6.2 Use of private digital mail services

The offering and use of private digital mail services have become more widespread in Finland in recent years. Currently, there are two private operators providing digital mail services on the Finnish market. The market has so far included Posti, which has offered an electronic mail service for a longer time, and Kivra, which entered the Finnish market a few years ago.

Several Finns have adopted either one or possibly both of these private digital mail services. For example, according to Posti, its OmaPosti service had 2.9 million users in April 2025, and according to Kivra, its service is used by over 6.5 million people in Finland and Sweden. According to a survey commissioned by the Digital and Population Data Services Agency in early autumn 2025, about 52% of approximately one thousand Finnish respondents aged 18–99 reported using the OmaPosti digital mail as their digital mail service, and 10% reported using Kivra's digital mail service.

Authorities and public administration bodies have also adopted private digital mail services to deliver official messages to public administration clients. According to a survey conducted in autumn 2025 by the Digital and Population Data Services Agency on the use of digital mail services by public administration organisations, of the 208 organisations that responded, 14% used OmaPosti and 12% used Kivra to send official messages to individual clients, such as decisions, invoices, invitations, notifications, and other communications. The survey indicated that private digital mail services are used to some extent in wellbeing services counties, while their use in municipalities and at the government level is less frequent. According to a study commissioned to support legislative preparation on private digital mail services, one reason for using private digital mail services in municipalities and wellbeing services counties has been that integration into the services via the operators has been relatively easy.

Currently, authorities that send electronic messages and notifications via private digital mail services have made separate agreements regarding the transmission of messages with the private digital mail operators. Due to the network effects characteristic of the digital mail market, potential new operators might find it difficult in the current model—which is based solely on separate agreements between sending authorities and digital mail operators—to get authorities to use their digital mail service, for example, as senders of notifications, if the operator does not currently have a sufficient number of end users. It is likewise more difficult to attract end users to the service if the organisations sending messages and notifications through the service do not include organisations that are relevant to the end user.

However, not all authorities use private digital mail operators for the transmission of electronic messages, and some authorities may use the service of only one private digital mail operator to transmit their messages. As noted above, authorities may use, in addition to private digital mail services, other communication channels to transmit their messages, which has led to the dispersal of official mail across different delivery channels. Consequently, citizens and businesses must follow and use multiple services in order to receive electronic mail from public actors. Currently, citizens and businesses also do not have the possibility to receive electronic mail from public and private actors centrally in a single digital mailbox. This complicates the management of incoming digital mail and smooth services processes, and imposes an administrative burden on citizens and businesses, which may also reduce the incentives to adopt new digital communication channels.

Authorities can be expected to send messages and notifications increasingly via the Suomi.fi Messages service if the proposed legislative changes concerning the primacy of electronic communication come into force as presented (HE 124/2025 vp). Authorities falling under the Suomi.fi Messages usage obligation could, however, still send electronic mail to private digital mail services even after the entry into force of the above-mentioned legislative changes, taking into account the obligations under the Support Services Act. Not all authorities, for example, will necessarily use Suomi.fi Messages for all subject areas if they apply for a justified exception from using Suomi.fi Messages. Thus, official messages and notifications may still be dispersed across different digital mailboxes. In addition, messages from private operators and possibly also some messages from public actors not subject to the usage obligation would still be read separately, for example, from private digital mail services.

Receiving official messages in a single, centralised digital mailbox has received support from citizens. Of the respondents in a survey conducted in early autumn 2025 on behalf of the Digital and Population Data Services Agency, 83% would prefer a single digital mailbox for messages sent by authorities rather than using multiple digital mailboxes in parallel. On the other hand, slightly more than half of the respondents, 54%, would like official messages to be

separate from other digital mail, whereas 46% of respondents would like all messages, both from authorities and private operators, to appear in the same digital mailbox. Almost half of the respondents supported a single centralised digital mailbox in any case, so a single digital mailbox for all messages can be seen as a solution supported by citizens.

According to the survey, citizens value the ability to choose the digital mailbox service themselves and to decide in which digital mailboxes official messages are displayed. If a citizen were to adopt a new private digital mailbox, 54% of respondents would want to give permission themselves for official messages to appear in the new private digital mailbox. Among the respondents, 35% would instead want official messages to appear automatically in the new private digital mailbox. Furthermore, 58% of respondents considered it important to be able to choose into which digital mailbox messages sent by authorities are delivered. Of the respondents, 25% were neutral on the matter.

Based on the study on private digital mail services conducted to support legislative preparation, it is also considered desirable among state authorities that messages from the private and public sector be combined into a single channel and that users have the option to choose which digital mailbox they use from among multiple digital mail services. According to the study, it is also considered desirable in the municipal and well-being services sector to have a single communication channel for clients and for users to have the ability to choose from which channel they receive notifications and messages.

Private digital mail services have the potential to offer public administration clients a better user experience for receiving and managing digital mail from authorities than Suomi.fi Messages, since private digital mailbox services may enable functionalities that are not necessarily included in the Suomi.fi Messages service. Private digital mailbox services could also be better suited to meet the needs of companies operating as public administration clients and other legal persons for managing digital official mail than the Suomi.fi Messages service. In addition, through value-added services provided to sender organisations by private digital mailbox services, authorities could enable functionalities that facilitate the management of digital official mail for public administration clients, such as paying invoices sent by authorities directly through the private digital mail service. However, implementing value-added services may require the development of a backend service managed by the service provider.

2.6.3 Carrying out the task included in the messaging service (providing a viewer application) as a public administration task

The starting point of the Government proposal on the primacy of electronic communication in public administration (HE 124/2025 vp) is that the messaging service, i.e., Suomi.fi Messages, would continue to serve as a kind of electronic counterpart to a physical mailbox from the perspective of correspondence from public administration in which authorities would primarily send electronic notifications. Under the changes proposed in the said Government proposal, electronic communication via Suomi.fi Messages would no longer require the explicit consent of the recipient, and the authority could send an electronically served document or a notification concerning the electronic service of documents to Suomi.fi Messages if the recipient uses Suomi.fi Messages. In contrast, electronic service to another electronic address or in a service not linked to Suomi.fi Messages would require that the authority has been provided with an electronic contact address to which the electronic service or, in the case of a service, a notification concerning the electronic service of documents is

sent. As considered above in Chapter 2.4, the provision of the messaging service must be regarded as a public administration task.

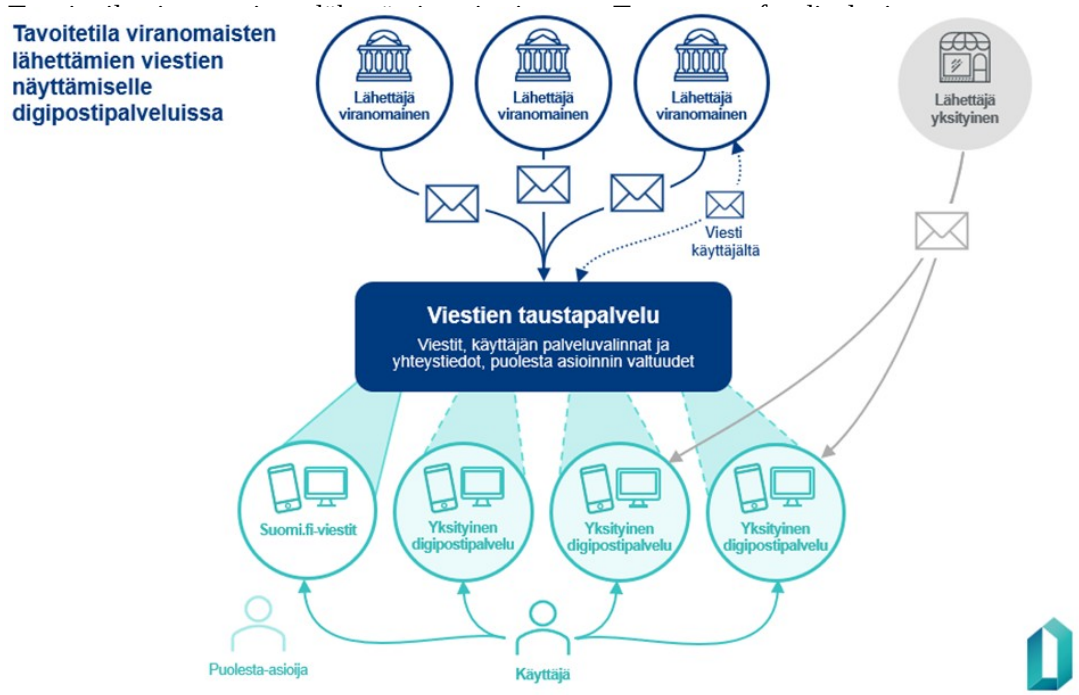
The purpose of this Government proposal is to allow a person or entity using a private digital mail service to read the notifications from that service, even if the actual service of documents is stored in the messaging service maintained by the Digital and Population Data Services Agency as a so-called backend service. On this basis, private operators would be granted the right to provide a viewer application linked to the backend service. For the sake of clarity, the Support Services Act would also assign a similar task to the Digital and Population Data Services Agency, even though it already provides a viewer application as a messaging service provider. As noted above, technical-administrative processing and preparatory tasks that are appropriately linked to the exercise of administrative decision-making power, and which have an assisting or complementary character in relation to the exercise of public authority, also fall under the concept of a public administration task. When the messaging service and the electronic service of documents it is intended for are considered as a whole, displaying the notification to the recipient must be regarded as an essential part of the implementation of the service of documents. For this reason, displaying an electronic communication sent by the authority and stored in the messaging service account using a viewer application is such an assisting task closely linked to a public administration task that it must be considered part of the public administration task. For this reason, the solution and the conditions under which a private service provider may be allowed to provide a viewer application enabling a view into the messaging service must be regulated by law.

In the current situation, there is no legal provision, in the manner required by Section 124 of the Constitution, regarding entrusting the assisting task of carrying out the service of documents to private digital mail operators. This may partly explain why authorities have not made significant use of private digital mail services in their service of documents. Some electronic service of documents, however, has been delivered with the help of private digital mail operators without actual legislative support in accordance with section 124 of the Constitution. In such cases, private digital mail services are not obliged to comply with the general administrative laws in this regard, and persons processing the service of documents in private digital mail services do not operate under official liability, even if a provision on compliance with general administrative laws may be included in the contract with the private service provider. In order for private digital mail operators to participate in carrying out the public administration task of delivering service of documents in accordance with Section 124 of the Constitution, and thus display the authorities' service of documents via their viewer applications, the matter must be regulated by law.

3 Objectives

The objective of the proposal is to enable the display of authorities' service of documents, which are stored in the messaging service maintained by the Digital and Population Data Services Agency, also in the user interfaces of private digital mail services, in addition to the user interfaces provided by the common Suomi.fi Messages service produced by Digital and Population Data Services Agency. By making broader use of private digital mail services in the delivery of authorities' electronic service of documents, the aim is to support a high-quality service experience for citizens and the possibility to choose the service they use for receiving service of documents, as well as to create conditions for new digital business models, the strengthening of a digital growth environment, and innovations. The objective is also that electronic mail sent by both authorities and private senders could, if desired, generally be received in a single service.

Fig. 1. Target state of the proposal



Proposals and their impacts

4.1 Main proposals

The proposal suggests amending the Act on Central Government's Joint e-Service Support Services so that displaying electronic notifications stored in the Suomi.fi Messages service of authorities via a viewer application could be assigned to a private operator on a contractual basis. Public administration clients would thus be able to read authorities' notifications, in addition to the interface of the Suomi.fi Messages service administered by the Digital and Population Data Services Agency, also via the interfaces of private digital mail services with an agreement. This would be possible in such a way that private digital mail services would display, in the viewers they provide, authorities' notifications stored centrally in the messaging service functioning as a backend service of the Digital and Population Data Services Agency.

The Support Services Act is proposed to be amended by adding a new Chapter 2 b on service provider's viewers. The Support Services Act would define a viewer application as a digital service functioning as the interface of the messaging service under the Support Services Act. With the inclusion of new actors, the law would clarify the role of the Digital and Population Data Services Agency in providing a viewer application for the messaging service, even if it also assigns the task of providing the viewer application to private operators. This would ensure that public administration clients could always use the interface of the Suomi.fi Messages service to read and receive notifications.

The new Chapter 2 b would regulate the transfer of the task of displaying authorities' electronic notifications to another service provider on the basis of an agreement and the conditions for doing so. Other service providers would perform an assistive task to a public administration function when they display authorities' electronic notifications, stored in the messaging service account, via a viewer application. At the same time, the law would regulate criminal liability related to the performance of a public administration function and make reference to liability for damages. Thus, the law would stipulate the assignment of the said task, which assists in a public administration function, to a private operator in the manner required by Section 124 of the Constitution.

In practice, the display of notifications is proposed to be arranged such that the Digital and Population Data Services Agency, acting as the service producer, and the service provider enter into an agreement under which the service provider links its viewer application to the backend service of the Suomi.fi Messages service via an interface. The recipient of the notifications could choose from the connected providers the digital mail services in which they want to receive authorities' notifications. Thus, it would be possible for the recipient to receive and read authorities' notifications in the viewers of those private digital mail services with an agreement and which the Suomi.fi Messages service user register recognises as chosen by the recipient.

In the proposed new Chapter 2 b of the Support Services Act, provisions would be made regarding the requirements imposed on service providers, with whom the service producer could enter into an agreement for the performance of the task assisting in a public administration function related to the display of notifications. The contract would enable the display of notifications through viewers for all service providers that meet the statutory requirements. In order for an agreement to be concluded, service providers would be required to be reliable and authorised to conduct business in Finland, and they would need to have the technical, financial, professional, and operational capabilities and personnel necessary to perform the task, as separately specified. Furthermore, the chapter would provide for the minimum content of the agreement between the service producer and the service provider participating in the display of notifications. The requirements imposed on service providers and the minimum content of the contract would ensure the proper performance of the service provider's duties.

The new Chapter 2 b would also regulate cooperation between the service producer and service providers, as well as the disconnection of the service in case of a disruption. The service provider and the service producer would have a duty to cooperate to ensure the security, interoperability, and proper functioning of the messaging service. The aim is to ensure that authorities' electronic notifications are delivered smoothly and securely to the correct recipients. Provisions would also allow the service producer and the service providers to disconnect their information systems, services, or viewer applications from a system maintained by another party if the messaging service, the system used for its production, or a viewer application linked to the messaging service causes harm to the operation or security of the messaging service or the linked viewer application.

The proposed Chapter 2 b of the Support Services Act would also provide for the authority and right of the service producer, the Digital and Population Data Services Agency, to supervise the operations of service providers. The provisions concerning supervision are intended to ensure that service providers comply with the obligations and requirements arising from the provision of the viewer application and that such compliance can also be monitored.

4.2 Principal impacts

4.2.1 Impact on public finances

The legislative proposal would have direct financial impacts, particularly on the Digital and Population Data Services Agency. The economic effects of the proposal would affect both the development and maintenance costs of the technical implementation as well as administrative costs at Digital and Population Data Services Agency. The development and maintenance costs would include, for example, expenses related to product management and development of the technical implementation of the viewer application and its associated backend service. Regarding product management, this ensures the maintenance of the viewer application, including preparation for and response to potential disruption situations. Financial impacts would also arise from the regular auditing of the viewer application, which ensures the quality and reliability of the service. In terms of product development, financial effects would result from the continued development of the viewer application in areas requiring further development. Further development needs for the viewer application and the backend service arise from customer and authority feedback, changes in legislation and regulations, and development needs identified within the ecosystem. Additionally, technological advancements would generate new development targets, creating opportunities to improve the service's quality, efficiency, and effectiveness.

In addition to the costs related to the technical implementation and its development, financial impacts for the Digital and Population Data Services Agency would arise from coordinating, managing, and supervising the network of private operators, providing the necessary legal support, and performing customer service and advisory tasks toward both the organisations sending messages and the end users.

According to the Digital and Population Data Services Agency's assessment, the need for customer service, guidance, and digital support would likely increase somewhat in the initial phase, particularly if, as proposed, customers were able to receive official notifications through private digital mail services. Guiding users through a more complex service involving multiple actors would increase the duration of customer service and digital support encounters, even though the customer support for private digital mail services would be provided by the private operators themselves. Delivering official notifications also through private digital mail services would likely increase the demand for incident handling and require the Digital and Population Data Services Agency to provide situational guidance to users toward the customer service of digital mail operators. The change would also require more extensive guidance materials than before and potential modifications to customer service systems.

The management of the cooperation network established with private digital mail operators—including, for example, ensuring the operators' compliance and security, as well as other necessary coordination, communication, and collaboration—would constitute a new set of responsibilities for the Digital and Population Data Services Agency and would generate additional costs.

For the Digital and Population Data Services Agency, the economic impacts would arise both from personnel costs and purchased service costs. During the development phase, the estimated cost of the development project is a total of EUR 8.5 million for the years 2025–2027. In accordance with the guidelines of the Finnish Ministerial Finance Committee, the Digital and Population Data Services Agency has been allocated EUR 1.6 million for

purchased services and personnel costs arising from implementation in 2025, funded from the 2024 budget item 28.70.01 Guidance and Development of Public Administration ICT, as well as a further EUR 6.9 million in the third supplementary budget for 2025 under budget item 28.30.03 Operating Expenses of the Digital and Population Data Services Agency.

In addition to development costs, the Digital and Population Data Services Agency estimates that the legislative proposal would result in an ongoing annual cost of approximately EUR 2.15 million from 2028 onwards. Furthermore, the legislative proposal may also have indirect financial effects on the future development of the Suomi.fi Messages service, since technical development must take into account a more complex overall system due to the backend service opened to private digital mail operators in connection with the viewer application.

The proposal is not expected to generate immediate financial benefits for public finances. The savings targets concerning the primacy of electronic service of documents set under the Central Government Productivity Programme are expected to be achieved through the Government proposal on the primacy of electronic communication in public administration (HE 124/2025 vp). However, the present proposal improves the operational opportunities of commercial digital mail operators as part of the authorities' electronic service of documents, which is expected to support the business prospects of digital mail services as well as their broader utilisation and usage in society. The widespread use of digital mail services creates conditions for cost-effective electronic communication both in public administration and in the private sector.

4.2.2 Basic and human rights impacts

4.2.2.1 Equality

The proposal would increase recipients' freedom of choice regarding the receipt of electronic notifications and other messages sent by authorities. In the future, public administration client could choose whether to receive electronic official messages via the Suomi.fi Messages user interface or through one or more private service providers. In some cases, services provided by private providers may be easier to use or offer functionalities that are not implemented in the Suomi.fi Messages interface. In addition, private service providers' platforms can also receive messages sent by private-sector actors, allowing users to receive both official and private messages in a single service as a general rule.

The broader possibility of using private service providers to receive official messages could improve the equal access to official communications for certain individuals in vulnerable situations. For example, a person may be accustomed to using a private provider's service but may encounter difficulties using the Suomi.fi Messages interface. The ability to use a familiar service can promote such a person's equal opportunity to receive official notifications electronically.

Authorities deliver electronic notifications to the messaging service in accordance with the usage obligation set out in the Support Services Act, from which they could also be read through private service providers' platforms. As with Suomi.fi Messages, using private digital mail services requires a device suitable for reading the messages, an internet connection, and a tool for strong electronic identification. A person's choice of service would therefore not affect from which authorities they can receive electronic notifications, nor what devices or other prerequisites they need to receive such notifications.

The proposal would have no immediate impact on people who currently receive official notifications and other messages by paper mail. Such individuals could continue to receive paper notifications from authorities if they wish. However, the ability to choose a service could increase the number of people who switch from receiving paper notifications to electronic notifications. For these individuals, the proposal is expected to have positive equality impacts. Electronic delivery of official notifications can be more reliable and faster than paper mail, as well as independent of the recipient's location. Due to the freedom of choice in the service, the number of people switching from paper mail to electronic notifications is expected to remain small.

Potential equality risks of the proposal are mainly linked to people's varying abilities to use digital services. Future innovations in private digital mail services could enable new functionalities for receiving and responding to official notifications, which could further improve user experience. In some cases, this may widen differences in individuals' ability to receive official notifications, depending on whether they interact with authorities electronically or via paper. This particularly affects people with very limited or no digital skills, who are thus excluded from using electronic services. Authorities must still ensure that everyone has the opportunity to receive their notifications through non-digital means. Therefore, the ability for individuals who use electronic services to choose which service they receive electronic notifications through is not expected to have significant effects on equality between people.

4.2.2.2 Legal protection

The legislative proposal would increase people's opportunities to decide how they receive official documents that concern their rights and obligations. Under the proposal, individuals would be able to access authorities' electronic notifications not only through the authorities' own online services and the Suomi.fi Messages service, but also via services provided by other service providers that have agreements with the service operator. The proposal may therefore have an impact on the implementation of the authorities' obligation to deliver notifications under Section 54 of the Administrative Procedure Act. The notification obligation is part of the right to legal protection and good administration protected in Section 21 of the Constitution. An effective method of delivery also promotes the service principle set out in Section 7 of the Administrative Procedure Act, according to which a person interacting with the administration should receive appropriate administrative services. The effects of the proposal on legal protection and good administration relate to the efficiency of official notifications, i.e., how quickly, reliably, and accessibly a person receives information about an electronic notification addressed to them in the digital mail service they have chosen.

Allowing public administration clients to choose the service for receiving official notifications is expected to have minor positive effects in terms of strengthening legal protection and improving good administration for those who primarily use, for example, a private service provider's digital mail service. In the future, these individuals would be able to receive official notifications and other electronic messages in the service they are accustomed to using. Private service providers may also offer functionalities that are not available in Suomi.fi Messages. This can make it easier for a person to respond to a notification or message received from an authority. However, such individuals often already have good digital skills, and they would also be able to use Suomi.fi Messages. Therefore, the above-mentioned improvements in user experience are relatively minor from the perspective of legal protection.

The option to choose a viewer may also entail risks concerning legal protection. A person should understand that choosing a viewer application and having this recorded in the service provider’s user registry means that they will need to monitor the chosen service to receive electronic notifications and other messages from authorities in the future. In administrative practice, the ordinary electronic notification method, which relies on the presumption of receipt, is generally used. Authorities therefore often do not need to ensure that a person has actually received the document. If a person does not understand the effects of their choice of viewer application, negative legal protection consequences may follow.

With the proposed amendments, it will be possible, in addition to Suomi.fi Messages, to deliver documents through other service providers both as verifiable electronic notifications under Section 18 of the Act on Electronic Services and as regular electronic notifications under Section 19. It can be assessed that, in practice, the legal protection effects of the proposal would be more significant in cases using regular electronic notifications than in those using verifiable notifications. In the case of verifiable notifications, the authority must ensure that the recipient has actually received the document. The authority must also ensure actual receipt if the notification is delivered electronically through another service provider that has an agreement with the service operator. The individual should, for example, be able to confirm receipt of the document through a separate confirmation function in the service provider’s service. Information about this confirmation must be transmitted via the messaging service to the authority that sent the notification. If the authority does not receive confirmation that a verifiable notification has been delivered, it must attempt delivery by other means, such as via a advice of delivery letter. In the case of verifiable notifications, a person's legal protection would not be compromised even if they did not understand how to monitor the viewer application they have chosen.

A regular electronic notification, on the other hand, is subject to a presumption of receipt, which means that the authority does not need to verify separately that the person has actually received the document. According to Section 19 of the Act on Electronic Services, a recipient of a regular electronic notification is considered to have received the document on the third day after the message was sent, unless evidence to the contrary is provided. The calculation of this period begins the moment the authority sends the notification to the messaging service, where it can be read using the viewer application. In the case of regular electronic service, it is the responsibility of the person themselves to monitor the notifications received on the service chosen by the person. If a person does not understand that they must monitor the viewer application they have selected, they may, in practice, fail to notice even those notifications from authorities that would require them to take action.

Central to the prevention of any legal security risks is public information on the changes resulting from the proposed act and personal information in connection with a choice of the viewer application to be used. As a service provider, the Digital and Population Data Services Agency is responsible for ensuring that the impact of choosing another viewer application is communicated in the Suomi.fi Messages in a sufficiently clear and understandable manner. The Digital and Population Data Services Agency and service providers participating in the electronic notification procedure could also use communication and service design to ensure that individuals do not choose to use a viewer application service that they do not actually use. From the point of view of legal security risks, it is also important that the selection of a viewer application other than Suomi.fi Messages requires active action by the person and is based on their own voluntary selection. Monitoring the arrival of new notifications would also be facilitated by the nudge notification proposed in the Government proposal HE 124/2025 vp, which would be sent automatically to the email address provided by the person or, in the

future, possibly also to another electronic address specified by the person, whenever a notification arrives at the messaging service operating as a backend service. A person would have the opportunity to provide an electronic address for nudge notifications either immediately upon opening a messaging service account or at a later stage if they so wish. The nudge notification could include information about which service the person has chosen to use for reading messages.

Technical incidents in the messaging service or connected viewers that have a negative impact on the implementation of notifications may also pose risks to the implementation of legal protection. Such legal risks are sought to be mitigated by the provisions in the proposal concerning cooperation between service producers and service providers and responding to disruptions.

4.2.2.3 Protection of private life

The proposal would enable private digital mail operators to participate in the authorities' electronic notification procedure in such a way that notifications and related messages could be read in private digital mail services using viewers. Private digital mail service providers would thus, in this respect, process documents and messages sent by authorities to public administration clients in connection with service of documents, as well as the personal data of the public administration clients contained therein. The proposal may therefore affect the protection of personal data, which is partly included in the protection of private life guaranteed in Section 10(1) of the Constitution, as well as the protection of the confidentiality of communications, which is provided for in section 10(2) of the Constitution in connection with the protection of private life. The effects of the proposal on the protection of personal data relate to the realisation of the data subject’s data protection rights and to the secure and lawful processing of personal data. With regard to the protection of the confidentiality of communications, the effects of the proposal relate to the risk of third parties gaining access to confidential messages received by public administration clients from authorities.

The amendments proposed in the proposal are assessed as having minor effects facilitating the exercise of data protection rights. As a result of the proposal, service of documents by authorities would by default be sent more often to a messaging service and, through it, made available in private digital mail services via an interface, instead of documents being sent directly to private digital mail services. Consequently, an increasing number of documents and messages related to service of documents sent by authorities would be stored centrally in the messaging service managed by the Digital and Population Data Services Agency. Centralising the storage of personal data in a single service is assessed as facilitating the exercise of the data protection rights of public administration clients as data subjects, for example, when a data subject exercises the right of access to their personal data or the right to restrict the processing of their personal data. However, the impact is assessed to be minor, as private digital mail services are not known to have been used to any significant extent in service-of-documents procedures.

On the other hand, the proposed amendment could temporarily cause uncertainty among data subjects as to through which channel they may exercise their data protection rights with regard to the content of documents and messages sent via Suomi.fi Messages, since, as a result of the changes in the proposal, the roles in the processing of personal data related to service of documents sent via Suomi.fi Messages would be divided among several different actors. Any potential ambiguities in the exercise of data subjects’ data protection rights can, however, be avoided through clear, transparent, and timely information jointly provided by the controllers

and processors within the Suomi.fi Messages service as a whole. Accordingly, in practice, data subjects' opportunities to exercise their data protection rights would not be weakened in this respect.

The personal data processed in Suomi.fi Messages mainly concern public administration clients, and some of the personal data may be sensitive or special categories of personal data or confidential information. As a result of the proposed amendment, an increasing number of documents served by authorities and the related messages would be processed in private digital mail services via an interface through a viewer application. Consequently, an increasing amount of the above-mentioned personal data would be processed by multiple actors in several processing environments. As a result, the potential attack surface of the Suomi.fi Messages service as a whole would expand both technically and organisationally, as new interfaces may contain vulnerabilities and personal data would be processed by, and potentially be accessible to, a broader range of parties. This increases the risk of personal data breaches and unnecessarily broad access to personal data and unauthorised access to confidential messages, among other things.

However, it should be noted that a public administration client would be able to decide for themselves which digital mail service provider with an agreement with a service provider would process the messages included in service of documents delivered via Suomi.fi Messages and the personal data contained therein, as the public administration client could choose whether they wish to receive electronic official communications in one or more digital mail services or in the Suomi.fi Messages user interface. Accordingly, a public administration client's personal data would not be processed by such service providers unless the public administration client has taken the relevant digital mail service into use by registering for the service and selecting that service provider's viewer application for receiving electronic communication from authorities.

Documents and messages related to the service of documents, and thus, the associated personal data, would nevertheless be stored centrally in the messaging service managed by the Digital and Population Data Services Agency, which would operate as a so-called backend service, thereby significantly reducing the risks to the protection of personal data and the confidentiality of communications arising from processing by other actors. On the other hand, for this reason, the backend service would be in an increasingly critical position with regard to ensuring the protection of personal data and the confidentiality of communications, which may, in turn, increase the risk of, for example, personal data breaches, including unauthorised access to confidential messages and thus also to personal data, as well as difficulties in exercising data subjects' rights. Access to personal data could, for example, be prevented as a result of a malfunction in the backend service, or personal data could be destroyed or lost unintentionally due to a failed update.

The risk of adverse effects on the protection of personal data can be reduced by ensuring the protection of personal data and lawful processing throughout the processing chain. The protection of personal data is ensured, first and foremost, by agreeing on the processing of personal data between the actors in the manner required by data protection legislation throughout the processing chain. In addition, the risks arising from the processing of personal data would be assessed before processing is initiated, and, where necessary, a data protection impact assessment in accordance with data protection legislation would be carried out. The actors must also implement technical and organisational measures commensurate with the risks arising from the processing. The Digital and Population Data Services Agency, as the controller of the Suomi.fi Messages service as a whole, bears primary responsibility for

ensuring that the risks arising from the processing of personal data within the Suomi.fi Messages service as a whole have been appropriately assessed and that the necessary measures have been taken to minimise those risks.

Agreements concerning the processing of personal data can also reduce risks to the protection of the confidentiality of communications in relation to private digital mail service providers. Third parties could gain access to confidential messages and their contents, for example, via digital mail service providers involved in service-of-documents procedures due to inadequate access control or information security. However, the technical and organisational measures required in the agreement on the processing of personal data can reduce the risk of third parties gaining access to confidential messages related to service of documents received by public administration clients from authorities. In addition, the actors would be obliged to comply, for example, with the information security requirements set out in Chapter 4 of the Information Management Act, which concern, inter alia, access rights management and the security of data transfer, thereby further reducing the risk of unauthorised access to confidential messages.

The risks to the protection of personal data and the confidentiality of communications are also reduced by the fact that the Digital and Population Data Services Agency, as the service producer of the Suomi.fi Messages service, ensures a high level of information security and data protection for the service. Contingency planning for the service have been designed taking into account the criticality of the service and the Digital and Population Data Services Agency's statutory obligation to provide the service. In addition, the Digital and Population Data Services Agency already has established processes in place for information security, data protection, preparedness, and continuity management. As large volumes of personal data already pass through the Suomi.fi Messages service, the service is already critical in terms of ensuring the protection of personal data and the confidentiality of communications. The proposed amendment would therefore only slightly increase the already significant importance of the Suomi.fi Messages service with regard to the protection of personal data and the confidentiality of communications.

On the other hand, the protection of the confidentiality of communications could be compromised in situations where a public administration client uses a digital mailbox jointly with another user or where the client's login credentials for the digital mail service fall into the wrong hands, in which case messages could be accessed without justification via the public administration client's own digital mailbox. However, a public administration client using a digital mailbox can reduce the risk of unauthorised access by taking particular care of their login credentials for the digital mail service. Risks related to the use of a shared digital mailbox can be reduced primarily through the functionalities of digital mail services but, ultimately, also by the public administration client choosing not to use a shared digital mailbox for receiving service of documents from authorities.

4.2.3 Social effects

4.2.3.1 Impact on public authorities

The proposed amendments are not deemed as having significant effects on the procedures or operational processes of authorities using Suomi.fi Messages. User organisations of Suomi.fi Messages would continue to send the same service-of-documents notifications and other messages to the messaging service as at present. In the future, messages would be transmitted from the messaging service acting as a backend service via an interface to the service that the

user has indicated they use and that is recorded in the Suomi.fi Messages user register. Authorities obliged to use support services under section 5 of the Support Services Act would remain obliged to use Suomi.fi Messages, even though service-of-documents notifications sent to the Suomi.fi Messages backend service could also be displayed in other digital mail services in the future. In order to derogate from the obligation to use the service, an authority would have to apply for an exemption in accordance with the procedure and conditions laid down in Section 7 of the Support Services Act. It would not be possible to derogate from the obligation to use the service solely in respect of other digital mail services; any application for an exemption would concern Suomi.fi Messages and all services connected to it.

The proposal may have effects on user organisations due to a potentially increased need for customer service and guidance. Sending organisations must be able to guide and advise message recipients to the correct service also in situations where the customer has chosen to read service-of-documents notifications from authorities via a private digital mail service.

The legislative proposal would give rise to new tasks for the Digital and Population Data Services Agency related to the development of the messaging service, particularly during the initial phase of connecting private digital mail services to the messaging service. These technical aspects related to service development are described in more detail in section 4.2.3.2. In the future, the Digital and Population Data Services Agency could, by contract, also agree with another service provider on the performance of the task of providing a viewer application. However, the transfer of tasks to other service providers would not mean that the task of providing the Suomi.fi Messages viewer application would be transferred away from the Digital and Population Data Services Agency but, rather, that it would be made possible for viewing access to be provided also by other service providers.

The number of tasks related to the drafting and administration of contracts is assessed to be low. The Digital and Population Data Services Agency would have certain tasks related to cooperation between service providers connected to the backend service and to the management of disruption situations. The Digital and Population Data Services Agency would also have the right to supervise the activities of service providers. Tasks related to the viewers of other service providers are assessed to be manageable within the Digital and Population Data Services Agency using the resources already in place for the provision of Suomi.fi Messages.

The Finnish Transport and Communications Agency (Traficom) would also continue to have responsibilities related to the supervision of digital mail services, as provided for, inter alia, in the Cybersecurity Act. The proposed amendments would have no impact on the Finnish Transport and Communications Agency’s current supervisory duties or its need for resources.

The legislative proposal would have positive effects on public administration clients’ services with public authorities. In the future, public administration clients would have the opportunity to influence which electronic service they use to receive electronic service-of-documents notifications and other messages from authorities. Many may, for example, consider services provided by private service providers to be more versatile or easier to use than Suomi.fi Messages. For such individuals, the accessibility of public services could improve to a small extent.

4.2.3.2 Information society and data protection

The proposal is assessed to have a positive impact on people as consumers using communication networks, communication services, and digital services. As a result of the proposal, public administration clients would have better opportunities to receive and read electronic messages and documents sent to them by both private actors and authorities through a single service. Public administration clients would also be able to choose through which digital mailbox they wish to read service-of-documents notifications from authorities and the related messages. As a result of the changes proposed in the proposal, users of digital mailboxes would also be able to switch digital mail service providers more easily, as service-of-documents notifications from authorities would, thanks to the backend service, also be available in another service provider's digital mailbox without the need for separate data transfers. End users would therefore not, in this respect, be tied to the first service provider they choose, but could switch service providers as needed without unreasonable effort related to data transfer.

The proposal would increase consumers' and recipients of service-of-documents notifications —citizens and businesses alike—freedom of choice and would make receiving digital mail from authorities simpler, more user-oriented and smoother. This is assessed as encouraging and facilitating the uptake of digital mail services and the preference for electronic official communications instead of paper letters. This may also be encouraged by the fact that, as a result of the proposed changes, digital mail users may gain a better user experience when using electronic mailboxes, as services provided by service providers may enable functionalities that are not available in Suomi.fi Messages. In addition, the ability to choose and switch service providers easily may encourage private digital mail service providers to compete through new functionalities and service quality, thereby improving consumers' position as users of services. A better and smoother user experience in receiving electronic service-of-documents notifications from authorities may encourage individuals and organisations to make broader use of digital services in other areas of life as well.

On the other hand, as a result of the changes in the proposal and the entry of new actors, public administration clients who communicate electronically with authorities may find it challenging to understand the overall structure of electronic official communications. Public administration clients may therefore need more support in the introduction and use of electronic official communications. The impacts of the challenges potentially faced by these public administration clients on the smoothness of electronic services with authorities can be mitigated through joint coordination and communication among all actors involved in the overall system, carried out in cooperation with stakeholders. In addition, it should be noted that the use of private digital mail services is always based on the public administration client's voluntary choice and active decision.

The proposal is also assessed as having effects on companies producing digital services. These effects are discussed in more detail in the context of business impacts in section 4.2.3.4.

Receiving electronic service-of-documents notifications and related messages from authorities as well as electronic messages from private actors primarily through a single digital mailbox creates better opportunities for authorities and other actors to reach their customers electronically and to offer increasingly high-quality electronic services and more opportunities for electronic services. This may therefore encourage authorities and other organisations to make increasing use of electronic channels for services and communications. Allowing public administration clients to also use other digital mail services for receiving service-of-

documents notifications and other messages from authorities is assessed as having an effect that speeds up the flow of information and promotes the development of digital mail services. The proposed legislative amendments may increase the customer base of private digital mail service providers and thereby contribute to the creation of opportunities for new innovations in digital mail services. This, in turn, may also benefit the development of authorities' services. Therefore, it can be assessed that the proposed amendments generally promote the development of the information society.

Including private digital mail services in the delivery of authorities' service-of-documents notifications as well as the construction of the Suomi.fi Messages backend service system will generate costs, particularly in the initial phase of operations, which are detailed in section 4.2.1. The costs of delivering authorities' electronic service-of-documents notifications will therefore increase compared to the model in which all notifications are delivered exclusively through Suomi.fi Messages. Authorities would, however, still not need to pay for the delivery of electronic notifications via the Suomi.fi Messages backend system, and the resulting costs would be covered by the operating expenses allocated to the Digital and Population Data Services Agency.

In addition to the impacts on the information society, the proposal is assessed to have effects on data protection and the allocation of responsibilities for the processing of personal data within the Suomi.fi Messages system as a whole. User organisations sending messages and documents to the Suomi.fi Messages backend service would continue to act as data controllers with respect to the content of the messages and documents they send. The Digital and Population Data Services Agency, as the provider of the Suomi.fi Messages service and backend service, also continues to act as a data processor with respect to the messages sent by user organisations and, indirectly, their content. The inclusion of private digital mail service providers introduces new actors into the delivery of authorities' electronic service-of-documents notifications via Suomi.fi Messages and the associated processing of personal data. Private digital mail service providers would act as data processors with respect to the notifications and their content, and the Digital and Population Data Services Agency would use private digital mail service providers to display notifications on behalf of the user organisations acting as data controllers. In this respect, private digital mail service providers would act as sub-processors vis-à-vis the Digital and Population Data Services Agency for the display of notifications. The processing of personal data carried out by the Digital and Population Data Services Agency and, where applicable, the processing carried out by private digital mail service providers as sub-processors, is based on the legal grounds for processing personal data set out in section 2.3.2.

The Digital and Population Data Services Agency would act as the data controller with respect to personal data accumulating from the functionalities of Suomi.fi Messages and its backend service. Private digital mail service providers would act as data processors in this context, as they would have no right to collect or manage their own permit or contact information registers. Personal data processing carried out by private digital mail service providers in their services beyond the scope described above is governed by the privacy terms of the respective private digital mail services. According to Article 28(2) of the GDPR, a data processor may not engage another data processor without the prior specific or general written authorisation of the data controller. Where written prior authorisation is required, the data processor must inform the data controller of any planned changes concerning the addition or replacement of other data processors, thereby giving the data controller the opportunity to object to such changes.

According to Article 28(3) of the GDPR, the processing of personal data must be governed by a contract or other legal act under Union or Member State law that is binding on the data processor with respect to the data controller, specifying the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects, and the data controller's obligations and rights. According to Article 28(4) of the GDPR, where a data processor engages another data processor to carry out specific processing activities on behalf of the data controller, in accordance with the agreement or Union law or some other legal document as referred to in the Member State's legislation, the same data protection obligations apply to the other data processor in question as thoseconfirmed in the contract or other legal document referred to in Paragraph 3, in particular providing sufficient guarantees that appropriate technical and organisational measures will be implemented so that the processing meets the requirements of this Regulation. If the other data processor does not comply with its data protection obligations, the original data processor remains fully responsible for ensuring that the second data processor meets its obligations toward the data controller.

Accordingly, personal data processing agreements must be concluded between both user organisations and the Digital and Population Data Services Agency and between the Digital and Population Data Services Agency and private digital mail service providers. If a user organisation acting as a data controller is unable to agree with the service provider on the processing of personal data or the sub-processors to be used, it must apply for an exemption from its obligation to use the service in accordance with section 7 of the Support Services Act.

As a result of the changes in the proposal, service-of-documents notifications processed in the Suomi.fi Messages service would also be handled in the digital mail services of private digital mail service providers, as actors with an agreement with a service provider would display the authorities' notifications and related messages in their digital mail services via a viewer application provided through an interface built into the Suomi.fi Messages backend service. The messages of an individual user, including their content and any relevant attachments, would be retrieved from the Suomi.fi Messages backend service at the user's request and stored in the private digital mail service only temporarily for the duration of a single session, unless the user explicitly and voluntarily indicates, on a per-message basis, that they wish to save that message in the private digital mail service as well. All documents and messages would be stored and retained centrally in the messaging service operating in the backend service. In the proposed model, responsibility for the secure transmission of authorities' service-of-documents notifications would rest with the Digital and Population Data Services Agency as the producer and maintainer of the messaging service, and with private digital mail service providers as displayers of documents via their viewers. This would not, however, alter the sender organisation's responsibility for ensuring the delivery or information security of the notifications.

Personal data contained in authorities' service-of-documents notifications and the related messages would therefore be processed both in private digital mail services and in the backend service maintained by the Digital and Population Data Services Agency. Some of this personal data may be classified as confidential information, special categories of personal data referred to in Article 9 of the General Data Protection Regulation (such as health data), or data concerning criminal convictions and offences. The data may also otherwise be sensitive and may partly include personal data of vulnerable data subjects, such as children or the elderly. Private actors participating in the electronic delivery of authorities' documents would also have access to the Suomi.fi Messages backend service's user and contact information register in connection with their role assisting public administration functions. Personal data

processing could be extensive if public administration clients widely adopt private digital mailboxes for receiving notifications and if an increasing number of sending organisations adopt Suomi.fi Messages. This would increase both the volume of personal data processed in the Suomi.fi Messages backend service and in private digital mail service providers, as well as the number of data subjects involved. Accordingly, there would, in principle, be a large number of data subjects and personal data being processed.

Extensive processing, which partly involves special categories of personal data, confidential information, or the personal data of vulnerable data subjects, increases the risk of adverse effects on the rights and freedoms of data subjects. In addition, personal data would be processed by multiple actors in a broader processing environment, which inherently increases the potential attack surface, both technically and organisationally, and thus the risk that personal data could be subject to, for example, data breaches or other security incidents. This could result, inter alia, in the disclosure of confidential information, psychological harm to data subjects, or the potential misuse of personal data. In particular, the large-scale storage of data processed in the Suomi.fi Messages service outside the service constitutes a significant data protection risk. The involvement of multiple actors in the processing of personal data may also increase the risk that personal data could be processed unlawfully, for example, for purposes other than those pre-defined, or that personal data could be accessible to a broader group of actors than strictly necessary.

The likelihood of adverse effects on data protection is mitigated, in part, by the fact that private digital mail service providers would, as noted above, act as data processors for the display of authorities' service-of-documents notifications and would therefore be contractually bound to process personal data under the supervision of the data controllers solely for the limited purpose immediately necessary to assist with public administration functions. From this perspective, the processing of personal data associated with Suomi.fi Messages by private digital mail service providers would be relatively limited and carried out in accordance with the instructions of the data controller, thereby reducing the service providers' discretion in deciding data protection measures. In addition, private digital mail service providers would, under contract, be obliged to implement technical and organisational measures appropriate to the risk arising from personal data processing, which further ensures that the processing of personal data is carried out lawfully. The risk of personal data security breaches is further reduced by the fact that private digital mail service providers with an agreement would be obliged not only to implement appropriate technical and organisational measures to protect personal data, but also to comply with other applicable security requirements. For example, the actors would be subject to security requirements applicable under the eIDAS Regulation and the security requirements set out in Chapter 4 of the Information Management Act.

The data protection risks for data subjects are also significantly mitigated by the fact that information retrieved from authorities' messages via the Suomi.fi Messages backend service would not be permanently stored in private digital mail services. Instead, data would be stored temporarily in the private digital mail service only for the duration of a single session and would be retrieved for display in the service only at the user's request each time. After this, the private digital mail service provider would be obliged to immediately delete all related data. As is currently the case, the data would remain permanently stored and retained centrally in the Suomi.fi Messages backend service administered by the Digital and Population Data Services Agency. With the entry of private digital mail service providers into the service-of-documents notification process, an increasing number of organisations and citizens may adopt Suomi.fi Messages, resulting in a growing volume of messages and personal data processed

by Suomi.fi Messages. Suomi.fi Messages may, to some extent, appear increasingly attractive as a target for data breaches or other cyberattacks.

The transmission of authorities' messages through private digital mail service providers would also be dependent on the operation of the Suomi.fi Messages backend service. Accordingly, under the proposed changes, the operational reliability and continuity management of the service have even greater significance for the delivery of authorities' service-of-documents notifications and for ensuring data protection. Due to the centralised backend service, the Digital and Population Data Services Agency also has a heightened obligation to maintain a high level of information security and data protection for the service. Data protection risks arising from the centralised backend service are mitigated by the fact that the Digital and Population Data Services Agency, as the provider of the Suomi.fi Messages service, ensures a high level of information security and data protection, and that the service meets the standards required under the Act on Information Management. Contingency planning for the service has been designed taking into account the criticality of the service and the Digital and Population Data Services Agency's statutory duty to produce it. In addition, the Digital and Population Data Services Agency already has established processes in place for information security, data protection, preparedness, and continuity management. The operational reliability and security of the Suomi.fi Messages backend service are therefore already of major importance, considering the number of service users and the types of personal data processed in Suomi.fi Messages. In addition, the importance of the service in this respect would increase even if the proposed changes concerning the primacy of electronic communication in public administration (HE 124/2025 vp) enter into force as proposed. Accordingly, the data protection risks inherent in the Suomi.fi Messages service would increase slightly as a result of the proposed changes.

In the model in the proposal, risks to the protection of personal data and privacy may arise, for example, if authorities' documents or confidential information were accessed without authorisation by another person through digital mailboxes. For instance, confidential information could inadvertently be disclosed to another user of a shared digital mailbox, or a digital mailbox user's login credentials or authentication devices could fall into the hands of an unauthorised person. However, the user can mitigate these risks by carefully safeguarding their login credentials and authentication devices and keeping them confidential. Data protection risks associated with the use of shared digital mailboxes can primarily be reduced through the functionality of the digital mail services themselves, but ultimately also by ensuring that public administration clients do not use shared digital mailboxes to receive authorities' service-of-documents notifications.

Provided that the measures outlined above to mitigate data protection risks are implemented, the adverse data protection impacts resulting from the proposed changes are assessed as being of recognised severity but unlikely to occur. A detailed and precise risk assessment is not possible at this stage, as all the specifics of the personal data processing and, for example, the technical and organisational safeguards to be implemented are not yet known. Accordingly, this assessment is based on a general-level analysis. Data controllers must, in any case, independently assess the risks arising from processing before commencing any processing activities.

4.2.3.3 Impact on authorities' information management

The proposal would have an impact on authorities' information management and related processes. Under current legislation, authorities are already broadly required to use the

Suomi.fi Messages service, and the Digital and Population Data Services Agency, as the producer of the messaging service, is responsible for the technical transmission of messages between the authority and the Suomi.fi service, as well as for the retention of transmitted messages. Going forward, user organisations' messages could, at the user's request, also be delivered from the Suomi.fi Messages backend service to viewers provided by private actors. The proposed change would thus introduce new user interfaces to the messaging service, which would take on the nature of a backend and storage service for authorities' messages. It would remain the responsibility of the Digital and Population Data Services Agency to provide the Suomi.fi Messages user interface as a single viewer application, even if the task of providing the viewer has been delegated to another actor. For the Digital and Population Data Services Agency, the most significant changes would relate to the amendments proposed to the Support Services Act concerning the delivery of notifications from the backend service to public administration clients. Services of those providers with whom the Digital and Population Data Services Agency has agreed to delegate the task of providing the viewer application would be integrated into the messaging service, enabling users to read received notifications and other messages from the service of their choice. The Digital and Population Data Services Agency would assume new responsibilities to perform technical tasks necessary to enable private digital mail service providers to connect to the system.

The proposed changes are not expected to have a significant impact on the tasks or responsibilities of authorities sending messages. The primary impact on sender authorities' operations relate to processes for ensuring the delivery of notifications, in which the sender authorities will, as required by their needs, have to take into account from which digital mail service each notification has been accessed. However, tasks related to this will mainly be handled by the Digital and Population Data Services Agency.

Under the proposed changes, responsibilities and obligations related to information management would become more distributed and divided among multiple actors. Private digital mail service providers participating in the display of authorities' notifications would, in this respect, be subject to the Information Management Act and would be required to organise information management and ensure information security in displaying notifications in accordance with the Information Management Act and other applicable legislation, such as the Cybersecurity Act. In addition, some responsibilities for incident management would be transferred to private digital mail service providers. As a result of the proposed changes, the Digital and Population Data Services Agency would no longer have as significant an ability to independently impact information management for the Suomi.fi Messages service as it does under the current system.

With the introduction of new actors, the point at which new information is generated within the messaging service would shift. Information regarding the delivery of a message to the service used by a public administration client, its opening, and, for the purposes of verifiable communication, its acknowledgment as received, would, for users of private digital mail providers, be generated within the respective digital mail service rather than in the service administered by Digital and Population Data Services Agency. The methods of generating this information would, however, remain largely similar to the current system.

The proposal would not affect data controller responsibilities, as described in section 4.2.3.2; the primary responsibility for data management would continue to lie with the user organisations. Other service providers offering viewers would act as sub-processors under the Digital and Population Data Services Agency, which serves as the data processor, and user organisations would need to approve their use. The proposal could have an impact on the

information security of the messaging service, as viewers of providers with which the service provider has agreements would be integrated into the service. However, in an agreement on the transfer of a task concerning the provision of a viewer, the service producer could require, for example, compliance with data security requirements that are commensurate with the communications service provider. The agreement could, for example, require the service provider to demonstrate at regular intervals that its viewer application meets the requirements set for it. In the case of private digital mail services, which, as described in Chapter 2.5.2.3 above, would as a rule be the case for providers of viewer applications, they would be understood as trust services referred to in the eIDAS Regulation , and the information security requirements in the eIDAS Regulation and cybersecurity regulation would apply to them as well.

The data would not be stored in viewers for longer than a single user session, and the service providers offering them would not, in principle, have the right to read messages sent to or by natural persons or companies using the service. If the user organisation were to consider that the viewer applications of service producers with an agreement with the service provider would not be sufficiently secure, it should apply for an exemption from its obligation to use the messaging service on the basis of an information security exemption.

4.2.3.4 Impact on companies

The amendments suggested in the proposal would enable private operators to participate in the display of electronic notifications from public authorities using viewers. The proposal is therefore expected to have a significant impact on companies providing private digital mail services and other operators offering digital services who might be interested in displaying authorities' electronic notifications and related messages through their services.

To date, there are two competing private digital mail service providers operating in the Finnish market, through which authorities' notifications may have been delivered to public administration clients using these services. However, authorities have not, to any significant extent, used private digital mail services in their notification procedures. This may partly be due to the fact that executing notifications constitutes a public administration task, and there has previously been no legal provision allowing the assignment of this task to private digital mail service providers in accordance with Section 124 of the Constitution. Additionally, the delivery of notifications via private digital mail services has so far operated on the basis that the sending authority has concluded a separate agreement with one or more private digital mail providers for the transmission of messages.

Under the proposal, private digital mail providers could, based on an agreement with the messaging service producer, participate in displaying authorities' notifications via a viewer application. The changes proposed in the proposal would regulate the participation of private digital mail providers in displaying notifications clearly in accordance with Section 124 of the Constitution, thereby clarifying their role in the delivery of authorities' electronic notifications and creating better conditions for conducting business based on digital mail services in the context of official communication. In addition, the proposed regulation creates conditions for new digital business opportunities. The regulation could thus also generate new revenue possibilities for these operators. Better conditions for conducting business and developing new digital business models foster competition among companies in the digital mail market, as this could encourage businesses to develop, for example, better and more innovative services, new functionalities, and various value-added services to attract end users and sending organisations to their services. Increased competition is likely to create opportunities for new innovations.

Competition is further supported by the fact that, under the proposed changes, it would be somewhat easier for new operators to access the market, as they could display authorities' notifications in principle from all sending organisations using Suomi.fi Messages without requiring separate agreements for delivering notifications with the sending organisations. This gives new operators slightly better opportunities to establish a foothold in the market without a large end-user base. In addition, all operators would be governed by clear statutory rules regarding the possibility of participating in authorities' electronic notification procedures and the conditions for doing so, ensuring, in this respect, equal competitive conditions. The opportunities for new operators, particularly small and medium-sized enterprises, to enter the digital mail market could, however, be somewhat limited by the requirement for operators to meet general functional and cybersecurity-related requirements. Small and medium-sized enterprises may have more limited resources to meet the required obligations.

The effects of the regulation proposed in the draft have been assessed in light of EU competition and state aid rules (Treaty on the Functioning of the European Union (TFEU), Articles 106 and 107) as well as national legislation on competition neutrality (Competition Act (948/2011), Chapter 4a). According to Article 106(1) of the TFEU, in the case of public undertakings and undertakings to which Member States grant special or exclusive rights, Member States shall neither enact nor maintain in force any measure contrary to the rules contained in the Treaties, in particular to those rules provided for in Article 18 and Articles 101 to 109. Under Article 107(1) of the TFEU, any aid granted by a Member State or through State resources in any form whatsoever which distorts or threatens to distort competition by favouring certain undertakings or the production of certain goods shall, in so far as it affects trade between Member States, be incompatible with the internal market.

During the preparation of the proposal, these questions were assessed in relation to whether the display of authorities' official notifications constitutes economic activity. Competition and state aid rules apply to undertakings, i.e., units engaged in economic activity, regardless of their legal form or mode of financing. Any activity consisting in offering goods and services on a market is an economic activity. The question whether a market exists for certain services may depend on the way those services are organised in the Member State concerned and may thus vary from one Member State to another. Moreover, due to political choice or economic developments, the classification of a given activity can change over time. What is not an economic activity today may become one in the future, and vice versa. (Commission Notice on the notion of State aid as referred to in Article 107(1) of the Treaty on the Functioning of the European Union (2016/C 262), paragraphs 12–13)

Competition and state aid rules do not apply when public authority is being exercised. From the perspective of competition and state aid law, an entity may be deemed to act by exercising public power where the activity in question forms part of the essential functions of the State or is connected with those functions by its nature, its aim and the rules to which it is subject. Generally speaking, unless the Member State concerned has decided to introduce market mechanisms, activities that intrinsically form part of the prerogatives of official authority and are performed by the State do not constitute economic activities. In so far as a public entity exercises an economic activity which can be separated from the exercise of public powers, that entity acts as an undertaking in relation to that activity. In contrast, if that economic activity cannot be separated from the exercise of public powers, the activities exercised by that entity as a whole remain connected with the exercise of those public powers and therefore fall outside the notion of undertaking. (Commission Notice 2016/C 262, paragraphs 17–18)

If a Member State has decided to introduce market mechanisms, and an activity is to be regarded as economic in nature, Chapter 4a of the Finnish Competition Act on competition neutrality also applies. Chapter 4a of the Competition Act regulates the powers of the Finnish Competition and Consumer Authority to monitor and safeguard equality of competition between public and private economic activities. According to section 30b of the Competition Act, Chapter 4a does not apply if the procedure or structure of the activity follows directly from legislation, or if applying it would prevent the performance of a task that is essential to citizens' welfare, safety, or another comparable public interest.

The authorities' obligation to serve official notifications is regulated in the Administrative Procedure Act and electronic notifications are regulated in the Act on Electronic Services. The electronic notification procedure concerns the exercise of public administration functions, as it is a statutory procedure that forms an essential part of administrative procedure. The messaging service intended for implementing electronic notifications, and the authorities' obligation to use the service, are regulated in the Support Services Act. This proposal would regulate the possibility for private digital mail operators to display official notifications using a viewer application provided by private digital mail operators and the conditions for doing so. The display of electronic notifications in the user interface is an essential part of carrying out the notification procedure, as it makes the notification available and readable to the recipient. It is therefore an auxiliary task closely linked to a public administration function, forming part of the public administration duties assigned to the service producer.

Since the electronic notification procedure and the display of notifications are part of a public administration function, which under section 124 of the Constitution is primarily the responsibility of authorities, these activities are, by their nature, related to tasks typical of public authority. Under the provisions on service of notifications in the Administrative Procedure Act and the Act on Electronic Services, these functions are also related to the State's core tasks, including the rules applicable to them. The activities are also related to core state functions in terms of their objectives, as their purpose is to fulfil the authority's obligation to provide notifications—a central element of administrative proceedings and a prerequisite for exercising the right of appeal. Accordingly, from the perspective of EU competition and state aid law, the electronic notification procedure and the display of notifications constitute an exercise of public authority and are not economic activities subject to the application of EU competition and state aid rules.

The responsibilities and tasks of private digital mail operators involved in the authorities' electronic notification process will expand significantly under the proposed amendments, as these private operators will carry out tasks that assist in the performance of public administration functions. Performing and initiating a task that assists in a public administration function will impose administrative burdens and, thus, costs on private digital mail operators and any other actors participating in the authorities' electronic notification process as proposed in the proposal. Administrative burden arises from meeting the conditions required to carry out the task, such as fulfilling functional and technical requirements, and the associated administrative procedures. For example, the technical specifications and requirements for the new interface enabling the display of notifications are estimated to require significant changes to the existing IT systems of private digital mail operators in order to ensure interoperability with the new interface. In addition, private digital mail operators must adapt their message structures to align with the Suomi.fi Messages backend service, as the data structure and technical implementation of messages and their attachments in the backend service differ from those in private digital mail services.

Beyond the specific requirements related to initiating the activity, operators must also comply with any new obligations imposed by other legislation applicable to the task assisting a public administration function. Private digital mail operators are themselves responsible for ensuring the proper execution of notifications in accordance with the Support Services Act and the terms specified in the agreement with the service provider. Moreover, general administrative legislation also directly applies to the activities of private digital mail operators in this context. As a result, responsibilities and obligations under, for example, the Information Management Act, relating to information security and the organisation of information management, will apply directly to private digital mail operators. The activities of private digital mail operators in this context would also be subject, for example, to the obligations under the Digital Services Act regarding digital support and accessibility, as well as provisions on official liability. In addition, general principles of good administration, such as the obligation to provide guidance under Section 8 of the Administrative Procedure Act, would apply to private operators when they are performing a task that assists a public administration function. The proposed changes may also increase the need for customer support in the services of providers performing this task, as well as contacts to the providers' customer service, which in turn may increase the administrative burden and costs for the service providers.

In order for operators to perform a task that assists a public administration function and comply properly with the new statutory requirements and responsibilities that apply, it is expected that they will need to modify their operational processes and possibly also their organisational structures. Furthermore, private digital mail operators' information systems may need to be modified so that the operators can comply with the obligations imposed by the new applicable regulations, such as confidentiality requirements. Incorporating the requirements of the new applicable regulation into processes, practices, information systems, and business operations generally will result in costs for the companies. At present, it is not known how well private digital mail operators currently meet, for example, the minimum information security requirements under Chapter 4 of the Information Management Act, nor how significant the changes will be in terms of their incident management processes, protection of data transfers, or logging practices.

The proposal would have a minor positive effect overall on companies and organisations using the messaging service, as such users could, like other public administration clients, choose which viewer application to use to display notifications. After this, notifications sent by the authorities to the company and delivered to the messaging service would also be available to read in the private digital mail services selected by the company.

4.2.3.5 Impacts on the Internal Market

The service provided by private digital mail operators can be considered a service within the meaning of Directive (EU) 2015/1535 of the European Parliament and of the Council laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services. Furthermore, some of the requirements included in the proposed regulation can be considered, in part, as rules on services, as referred to in the Directive. Such rules on services would, for example, be included in the proposed Sections 8 h and 8 i. Since compliance with the rules on services would be mandatory for service providers and would affect the provision of the service, the measures constitute technical regulations within the meaning of the Directive. Including provisions considered technical regulations in national legislation is justified, because the proposed regulation concerns assigning a task that assists a public administration function to a private party. This requires, in addition to other requirements set out in the Constitution, that the matter is regulated by law. The starting point

is that all matters essential for performing the public administration function are clearly set out in the law assigning the task.

Directive (EU) 2015/1535 requires that any legislative proposal containing technical regulations be notified to the Commission before such provisions are adopted into national legislation. The Commission and other Member States then have the opportunity to comment on the proposal within three months of the notification. If the Commission or another Member State submits, within the prescribed time limit, a detailed opinion stating that the planned measure may result in obstacles to the free movement of services within the internal market, the adoption of the proposal must be postponed by an additional month. The notification procedure carried out and its outcome are described above in section 1.2.

The service provided by private digital mail operators can also be considered a service falling within the scope of Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (hereinafter "Services Directive"). Chapter II of the Services Directive (Articles 5–8) sets out provisions on the simplification of procedures. The provisions of this chapter apply to all services falling within the scope of the Directive and to all procedures and formalities necessary for the establishment and operation of the service activity. The proposed regulation takes into account the requirements laid down in Chapter II, as necessary. For example, the requirement in Article 5(1) of the Services Directive to simplify the procedures and formalities applicable to access to a service activity and to the exercise thereof has been considered, inter alia, by abandoning a heavier permit procedure for starting a service operation, which had been proposed during preparation (the permit procedure is discussed in more detail later in section 5.1). In part, the requirements of Chapter II of the Services Directive concern the authority responsible for implementing the proposed regulation later on and other parties.

Chapter III of the Services Directive (Articles 9–15) sets out rules on the freedom of establishment of service providers. The provisions of the chapter apply to all requirements regarding the establishment of a service provider. Under the proposed regulation, a private digital mail operator must meet certain requirements and enter into an agreement with the authority before it can begin offering a viewer application. Under the Services Directive, such a procedure can be considered a licensing system within the scope of the Directive (Article 4(6) and Recital 39 of the Services Directive). Article 9(1) of the Services Directive sets out the conditions that must be met for a Member State to make compliance with a licensing system a condition for starting or carrying out a service activity. This point requires that the licensing system must not discriminate against any service provider, that the need for the licensing system must be justified by an overriding reason relating to the public interest, and that the intended objective cannot be attained by a less restrictive measure, particularly because ex post monitoring would occur too late to have any real effect.

The agreement template suggested in the proposal is considered to meet the conditions set out in Article 9(1) of the Services Directive, firstly, because it treats service providers in the same way regardless of the Member State in which they are established. All service providers that meet the requirements laid down in the law would, on the basis of the agreement, be entitled to provide a viewer application for the messaging service. Secondly, the agreement template is justified by an overriding reason relating to the public interest, which includes general security, the protection of service recipients, and consumer protection, since the agreement template aims to ensure the high quality, safety, and functionality of the services. Thirdly, these objectives cannot be achieved by a less restrictive measure, as service providers must meet certain requirements, such as regarding functionalities and data security, to achieve the

objectives. The proposed model would ensure that all service providers meet the same requirements and offer services at least at a specified level of quality and safety. In this way, for example, consumers can be confident that all service providers meet certain quality criteria. A defined minimum quality level would also encourage service providers to develop additional services and features, which would further serve the interests of consumers. With regard to the objectives, ex post monitoring would occur too late to have any real effect, since, for example, a data breach or problems with the availability of an important document could negatively affect the objectives within a short period after the breach or the issue occurs.

According to Article 10(1) of the Services Directive, a licensing system must be based on criteria that determine the scope of discretion of the competent authorities, in a way that ensures the discretion is not exercised arbitrarily. According to point 2 of the same article, the criteria must be non-discriminatory, justified by an overriding reason relating to the public interest, proportionate to the public interest objective in question, clear and unambiguous, objective, generally known in advance, and open and accessible. In the proposed regulation, the criteria imposed on service providers as a condition for concluding the agreement can be considered non-discriminatory, since service providers are treated equally regardless of the Member State in which they are established. The criteria are justified by the same overriding reasons relating to the public interest as the agreement template itself, and these objectives could not be achieved by a less restrictive measure for the reasons set out above. The criteria are limited to what is strictly necessary to protect service recipients and consumers. The criteria are also clear and unambiguous, as their meaning would be explained in the section-by-section justifications. The criteria are objective, reflecting general conditions for commencing operations, similar to conditions set elsewhere in legislation for other activities. The criteria are also generally known in advance, open, and accessible, since they would be laid down in law and the terms of the agreement would be publicly available.

The proposed regulation does not contain any of the prohibited requirements set out in Article 14 of the Services Directive. However, the proposed regulation could potentially include conditions referred to in Article 15(2) of the Services Directive. Pursuant to Article 15(3) of the Services Directive, the conditions referred to in paragraph 2 must be non-discriminatory, justified by an overriding reason relating to the public interest, and proportionate.

Since section 8 h of the proposed regulation would require that the legal entity acting as a service provider possesses the necessary financial capacity to perform the task, this could be regarded as a requirement concerning ownership of share capital within the meaning of Article 15(2)(c) of the Services Directive. Furthermore, because section 8 h would require that the legal entity acting as a service provider has the necessary personnel to perform the task, this requirement could be considered a minimum number of employees requirement within the meaning of Article 15(2)(f) of the Services Directive. The proposed regulation might also include a requirement referred to in Article 15(2)(d) of the Services Directive, whereby the commencement of a certain service activity is allowed only for certain service providers due to the particular nature of the activity. This is because the proposed regulation would apply solely to private operators engaged in a specific type of activity who meet requirements relating, for example, to reliability and financial capacity. These requirements included in the proposed regulation can be considered non-discriminatory, justified by an overriding reason relating to the public interest, and proportionate for the same reasons as those set out above regarding the agreement template. Moreover, it should be noted that since the proposed regulation concerns the delegation of a public administration task to a private entity as referred to in the Constitution, the regulation must specify which tasks may be delegated to the private party and under what conditions. Requirements regarding general operating

conditions or the eligibility and reliability assessment of the operator cannot be left solely to the agreement.

Pursuant to Article 15(7) of the Services Directive, Member States must notify the Commission of new rules in their national legislation that lay down the requirements referred to in paragraph 2 as well as the justifications for those requirements. The Commission may make the submitted requirements known to other Member States. Submitting the requirements does not prevent Member States from adopting the provisions. The Commission examines within three months of the notification whether the provisions are compatible with Union law and, if necessary, adopts a decision urging the Member State to refrain from adopting or to repeal the provisions.

Other key provisions of Chapter III of the Services Directive have also been taken into account in the proposed regulation. For example, Article 10(6) of the Services Directive requires that, except in the case of the granting of an authorisation, any decision from the competent authorities, including refusal or withdrawal of an authorisation, shall be fully reasoned and shall be open to challenge before the courts or other instances of appeal. Under the proposed regulation, the service provider would, in principle, be required to conclude contracts with all service providers who notify the service provider of their willingness to carry out the task and meet the statutory requirements. The agreement would be an administrative agreement. According to section 20(1)(4) of the Administrative Judicial Procedure Act (808/2019), an administrative court handles as an administrative litigation any case concerning an administrative contract. Partially, Chapter III of the Services Directive also includes requirements that the competent authority must take into account when implementing an authorisation system. In this context, the competent authority must also consider the provisions of the Finnish Act on the Provision of Services (1166/2009). The Act on the Provision of Services relates to the national implementation of the Services Directive and, based on its preparatory works, also applies to a private entity performing a public administration task (HE 216/2009, p. 54).

Chapter IV of the Services Directive (Articles 16–21) regulates the free movement of services. This chapter concerns cross-border provision of services, i.e., cases where the service provider is not established in the Member State in which it provides services. According to Article 16(1) of the Services Directive, Member States shall not make access to or exercise of a service activity in their territory subject to compliance with any requirements which are not non-discriminatory, necessary, and proportionate. Article 16(2) of the Services Directive sets out requirements that Member States may not impose on a service provider established in another Member State. However, under Article 16(3) of the Services Directive, the Member State to which the provider moves shall not be prevented from imposing requirements with regard to the provision of a service activity where they are justified for reasons of public policy, public security, public health, or the protection of the environment and are consistent with the above principles. The requirements set out in the proposed section 8 h are justified on the grounds of public security, as the requirements imposed on service providers ensure a minimum level of security and functionality for a nationally critical service in light of the participation of private operators. The requirements are also non-discriminatory and proportionate for the same reasons as discussed above regarding the agreement template.

Pursuant to Article 39(5) of the Services Directive, Member States must submit to the Commission the national requirements whose application could fall within the scope of the third subparagraph of Article 16(1) and the first sentence of Article 16(3) of the Services Directive, together with the related justifications. The Commission may make the submitted

requirements known to other Member States. Submitting the requirements does not prevent Member States from adopting the provisions. The notification procedure carried out pursuant to Articles 39(5) and 15(7) of the Services Directive is described above in section 1.2.

Procedures falling within the scope of the Services Directive also fall within the scope of Regulation (EU) 2018/1724 of the European Parliament and of the Council establishing a single digital gateway providing access to information, procedures, and assistance and problem-solving services, and amending Regulation (EU) No 1024/2012 (the SDG Regulation). The provisions of the SDG Regulation complement the requirements of the Services Directive. Procedures under the Services Directive must be provided entirely electronically in accordance with Article 6 of the SDG Regulation, and the information concerning the procedures must meet the quality requirements set out in Article 10 of the SDG Regulation. In addition, procedures under the Services Directive must comply with Articles 13, 24, and 25 of the SDG Regulation. The competent authority must take the above SDG Regulation requirements into account when implementing procedures under the Services Directive.

5 Other options for implementation

5.1 Alternatives and their impacts

During the preparation, foreign solutions for organising the use of digital mail systems for official communications have been examined. Among the foreign solutions reviewed, as described below in section 5.2, is a model used in Sweden in which messages are delivered to separate public or private digital mail services for reading and storage, without the messages passing through or being stored in a centralised state infrastructure. In that model, the state infrastructure for delivering digital mail is primarily intended to route official digital mail to the correct addresses. During the existence of the infrastructure in Sweden, challenges related to this model have been identified, such as dependence on the services of private actors and the decentralisation of official message delivery across different channels despite the infrastructure. The Swedish Digital Agency (Myndigheten för digital förvaltning, Digg) has therefore proposed that digital mail be organised in a manner similar to the model used in Denmark. For the reasons mentioned above, the preparatory work concluded that it is not appropriate to implement private digital mail providers' participation in the delivery of official notifications according to the Swedish model.

During the preparation, one implementation option that was considered was a licensing model, in which the display of official notifications in service providers' viewer applications would be based on a licensing procedure. In this model, the authority would grant a license, upon application, to connect a viewer application to the messaging service if the conditions for granting the license were met. The model would therefore include a licensing procedure for offering a viewer application and a licensing authority responsible for the new task of granting and managing licenses. However, the licensing model would entail significant administrative burden, not only for private actors but also for the licensing authority, and thus indirectly result in costs for public finances. For this reason, the preparatory work concluded that a licensing procedure would not be a cost-effective or practical way to enable the display of notifications in private digital mail services.

During the preparation, an alternative model based on procurement by the service provider was also considered, in which the service provider would acquire the service for the viewer application from the market. However, the procurement-based model was not deemed a

suitable way to enable the display of official notifications outside the service provider's own service. The procurement model would result in the user interface being available only to one or a limited number of actors, whereas the goal is to allow the display of notifications in viewer applications for all willing actors who meet the requirements, thereby enabling users to choose which viewer application they use. In addition, the procurement model would leave the participation of private actors dependent on the service provider's procurement. In the proposed model, the service provider could enter into agreements with all private actors who meet the requirements and voluntarily express their willingness to display official notifications. The service provider itself would also continue to provide the viewer application for the messaging service, even while enabling the participation of private actors.

During the preparation, the possibility of granting the service provider regulatory authority to issue more detailed requirements was also considered. In practice, however, the service provider could incorporate equivalent requirements into the terms of the agreement drafted as proposed and agree to modify the contractual requirements if necessary. The service provider could, in a manner similar to a regulation, make the agreement terms publicly available. For this reason, the proposal does not grant the service provider separate regulatory authority.

In the course of the preparatory work, the possibility of compensating private digital mail service operators was also assessed in light of the flexibility of public finances and the competition law implications, in accordance with the basic implementation principles. Alternatives for the payment model include, in line with the basic principles set by the Ministerial working group on reforming society described in section 1.1, either providing the service free of charge from the perspective of public finances or a fixed annual budget that would be distributed among participating operators based on the service through which a user first opens each message from a public authority. The assessment concluded that, since this concerns a voluntary task assisting a public administration function, it would not be justified to pay support to the service provider for performing the task. The starting point is that the service provider delivers the service of displaying official messages as part of its business operations. Support paid to private actors would, according to the assessment, constitute state aid, which would need to meet the requirements of EU state aid rules. The assessment further notes that such support to private actors would fall under the so-called services of general economic interest (SGEI) support, i.e., SGEI or SGEI de minimis aid. Granting SGEI aid would require complex regulation and would entail administrative burdens. According to the assessment, any regulatory evaluation regarding business support for private service providers would need to be prepared as a separate project, taking into account the schedule of the Government proposal. In this context, on 11 November 2025, the Ministry of Finance informed the Ministerial working group on reforming society of the position that no state aid will be paid for the display of official notifications by private actors.

5.2 Legislation and other means in place in other countries

5.2.1 Sweden

In Sweden, citizens and businesses can choose to receive digital mail from public authorities. For sending and receiving digital official mail, the Swedish Agency for Digital Government (Myndigheten för digital förvaltning, Digg) provides a shared digital mail infrastructure (Mina meddelanden) for public authorities, enabling public actors to send digital mail to individuals and businesses. Digg is obliged to provide the infrastructure under the Ordinance on a Common Infrastructure for Digital Post for Authorities (2018:357). The ordinance regulates

the actors that may be connected to the infrastructure, the processing of personal data in connection with the infrastructure, and Digg's authority to issue regulations.

The Mina meddelanden infrastructure does not itself operate as a digital mailbox. Instead, official messages connected to the infrastructure are received and read in a separate digital mailbox service that is linked to the Mina meddelanden infrastructure. Messages also do not pass centrally through the infrastructure; rather, the actual messages are primarily stored on the service provider's servers and kept in the recipient's mailbox. The primary role of the Mina meddelanden infrastructure is thus to manage the delivery of digital messages to recipients and maintain a registry of actors connected to the infrastructure, such as citizens' digital mailboxes and their choice to receive or not receive digital official messages. Messages can only be sent through the infrastructure unidirectionally, from the authority to the recipient.

Like message recipients, public authorities are not obliged to join the Mina meddelanden infrastructure to send messages to citizens and businesses. Thus, messages can only be received in a digital mailbox via the infrastructure from public authorities that have joined Mina meddelanden as senders. Public authorities can send messages to the Mina meddelanden infrastructure either directly themselves or through an intermediary service provider. Public authorities can also send electronic messages to citizens outside the infrastructure, for example, by email or directly to a specific digital mail with which the sending authority has an agreement.

Citizens and businesses can choose which digital mail service they want to use to receive official messages via the Mina meddelanden infrastructure, provided the service is connected to the infrastructure as a digital mail provider. Digital mail providers connected to the Mina meddelanden infrastructure can display in their services the messages sent via the infrastructure by the public authorities that are part of it. To be able to connect to the Mina meddelanden infrastructure, digital mail providers must apply to Digg for authorisation to join the infrastructure and its digital mail authorisation system. The Digital mail authorisation system is a procedure maintained by Digg that enables public actors to utilise Digital mail services and electronic identification services. The authorisation system centralises the use of these services so that Digg approves service providers into the system based on predefined requirements and enters into agreements with digital mail service providers. Within the framework of the authorisation system, Digg also concludes agreements with the public authorities that send messages via the Mina meddelanden infrastructure.

Currently, citizens and businesses can choose to receive electronic official messages via the Mina meddelanden infrastructure through Digg's Min Myndighetspost service or through three private digital mailboxes, with which Digg has agreements under the authorisation system. At present, the private digital mail providers connected to the system are Kivra, Billo (for private individuals), and Fortnox (for businesses). In addition to authorities, it is also possible to receive messages in private digital mailboxes from private actors. Kivra's digital mailbox is currently the largest and leading service on the Swedish digital mailbox market in terms of user numbers. A citizen becomes part of the Mina meddelanden infrastructure and starts receiving official mail in their chosen digital mailbox once they select one of the infrastructure-connected digital mail services and indicate that they want to join the infrastructure to receive electronic official mail.

The authorisation system for digital mail services is based on the law that came into effect in Sweden at the beginning of 2024: the Act on an authorisation system for services for electronic identification and digital mail for private individuals (lag om auktorisationssystem i

fråga om tjänster för elektronisk identifiering och för digital post (2023:704)). This law regulates applications to the authorisation system, the procedure for approving service providers, as well as rectification and compensation in cases where Digg is deemed to have violated the law. Under the law, a regulation on the authorisation system for services for electronic identification and digital mail (förordning om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post (2023:709)) has been issued, which sets out Digg's role in providing the authorisation system and its authority to issue rules on fees and requirements for service providers participating in the system. In 2025, Digg issued regulations on the requirements for service providers' authorisation applications in electronic identification and digital mail services (MDFFS 2025:1) as well as regulations on charging fees for the use of electronic identification and digital mail services in the authorisation system (MDFFS 2025:2).

Since May 2025, using digital mail services via the authorisation system has been subject to fees for public actors that join the system, in accordance with Digg's regulation MDFFS 2025:2. According to this regulation, public actors must pay SEK 0.70 (excluding VAT) per message sent and made available to the recipient. The payment made by a public actor covers Digg's costs for establishing and managing the authorisation system as well as the compensation paid to service providers.

Digg pays compensation to operators providing digital mail services through the authorisation system for delivering these services. The compensation consists of two parts: a fixed fee and a variable, transaction-based fee. To receive the fixed fee, a service provider must have at least 200,001 digital messages made available per calendar year. In 2025, the maximum fixed fee that could be received was SEK 2.5 million per calendar year. To receive the variable, transaction-based fee, the digital mail operator must annually reach at least a certain number of digital messages made available. According to the guidelines in force in autumn 2025, transaction-based compensation is paid when the operator's transactions, that is, digital messages made available, reach at least 4,237,289 per calendar year. The variable, transaction-based compensation is calculated by multiplying the number of digital messages a service provider makes available by the transaction compensation factor. In autumn 2025, the factor for the variable compensation was SEK 0.59 per digital message made available.

Swedish Administrative Law (Förvaltningslag (2017:900)) does not regulate the form in which an authority communicates with an individual. Under Section 6 of the Swedish Administrative Law, the authority must ensure that communication with the individual is smooth and simple. In the processing of an administrative matter, the Service of Documents Act (Delgivningslag (2010:1932)) and the Service of Documents Ordinance (Delgivningsförordning (2011:154)) apply when service of documents must be carried out in a case pending before a court or other authority, or when service of documents must be carried out in another situation pursuant to law or other regulation. According to section 4 of the Service of Documents Act, the method of service must be chosen so that it is appropriate for the content and extent of the document and minimises costs and effort. Under the Service of Documents Ordinance, both ordinary and simplified service can be given electronically. Ordinary service under Swedish law largely corresponds to the Finnish concept of verifiable service, and simplified service corresponds to the Finnish concept of regular service. However, according to Section 17 of the Service of Documents Act, only an authority may send a document electronically in connection with ordinary notification.

In Sweden, many citizens have started using digital mailboxes. According to Digg's statistics, approximately 6.5 million citizens had a digital mailbox in use at the beginning of October

2025. At that time, approximately 290,000 companies were also using digital mailboxes, and 323 public administration actors were sending digital mail via the Mina meddelanden infrastructure. Digg estimates that in 2026, the number of citizens and businesses adopting a digital mailbox would increase to about 6.8 million.

Despite the widespread use of digital mailboxes, some challenges have been identified in the Swedish digital mail model. In public administration, digital mail is sent through different channels, as actors have joined the Mina meddelanden infrastructure, launched in 2012, slowly over the years, and not all public authorities have joined or make extensive use of it even after joining. Some public authorities have developed their own solutions for communicating with public administration clients instead of using the shared infrastructure. Additionally, many public authorities still rely heavily on traditional paper mail. Another challenge in the Swedish model is the dependence on private digital mail operators as custodians of messages. Users do not have a legal right to transfer their digital mail from one mailbox to another, as digital mail operators are not obligated to move a user's digital mail archive to another service. If a digital mail provider exits the infrastructure or ceases operations, the user cannot transfer previously received mail directly to another digital mail provider.

Digg has proposed that the Mina meddelanden infrastructure be turned into a centralised message delivery and storage service with a viewer, similar to the model used in Denmark. According to Digg's assessment, this solution would be stronger and safer than the current one for handling messages, as it would ensure data protection, long-term access to documents for individuals, and the possibility to change the digital mail service provider. The solution is also expected to support competition, thereby benefiting consumers. On behalf of the Swedish government, a study has also been conducted on the conditions for making the sending and receiving of digital government mail mandatory for recipients and sending organisations, so that society and citizens would benefit more broadly from the Mina meddelanden infrastructure. The study was published in 2024 as the SOU report Digital myndighetspost (SOU 2024:47), which proposes a new law on the use of a shared digital mail infrastructure for public authorities. So far, the report's proposal has not led to an actual legislative proposal submitted to the Swedish government.

5.2.2 Denmark

In Denmark, citizens and businesses are required to join the state-provided digital mail solution to receive official government mail. This obligation is based on the Danish Act on Digital Post from Public Senders (Lov om Digital Post fra offentlige afsendere, LBK nr 686 af 15/04/2021), which regulates the digital mail solution for government correspondence, including joining and using it. According to section 3 of the Act, the obligation applies to natural persons aged 15 or older who reside or are permanently present in Denmark, as well as legal entities with a Danish business registration number.

Exemptions from the obligation can be requested under section 5 of the Act, based on rules set by the Danish Ministry of Finance. For natural persons, these rules are established in the Regulation on the administration of Digital Post from public senders (Bekendtgørelse om forvaltning af Digital Post fra offentlige afsendere, BEK nr 2017 af 29/10/2021). The exemption of legal entities and natural persons engaged in business activities from the obligation to join is regulated in more detail in a separate regulation (Bekendtgørelse om fritagelse af juridiske enheder med CVR-nummer samt fysiske personer med erhvervsaktiviteter for tilslutning til Digital Post, BEK no. 985 of 07/08/2013). If a natural

person or legal entity is exempt from the obligation to join, they may still voluntarily join the digital mail solution under section 4 of the Act using an electronic identification certificate. In addition, Danish citizens aged 15 or older who live abroad may also voluntarily join the digital mail system. Once someone joins the digital mail solution voluntarily, they can only opt out in accordance with the legal exemptions provided in the Act.

The solution referred to in the law as Digital Post is a state-managed digital infrastructure that functions as a common electronic messaging service for government communication with public administration clients. The development, operation, maintenance, and management of Digital Post is the responsibility of the Danish Agency for Digitisation (Digitaliseringsstyrelsen). However, the Danish Agency for Digitisation does not provide the service alone. Under section 2(3) of the Act, it has delegated certain tasks related to the operation, development, and support of Digital Post to external providers.

Government messages and documents sent via Digital Post are read and received in so-called viewer applications (visningsklient), which are the user interfaces of the digital mailboxes. Citizens and companies receiving digital mail can choose which approved interface they use to read government messages sent via Digital Post. Under sections 10a and 10b of the Act on Digital Government Mail, both public authorities and private entities may provide viewer applications for displaying government messages. Both types of providers must apply for and obtain a license from the Danish Agency for Digitisation to offer a viewer application client. The obligation to apply for a license, the approval procedure, and the requirements for the license are set out in the regulation on the approval of Digital Post viewer applications and compensation for service providers of commercial viewer applications (Bekendtgørelse om godkendelse af visningsklienter til Digital Post samt kompensation for forpligtelser til offentlig tjeneste for udbydere af kommercielle visningsklienter, BEK nr 331 af 16/03/2022).

According to section 9(2) of this regulation, the approval procedure for viewer applications generally consists of three stages: basic approval, conclusion of a membership agreement, and solution approval. Under section 9(1), a public viewer application is finally approved once it has received basic approval and the Danish Agency for Digitisation and the public viewer application provider have concluded a membership agreement. Final approval for a commercial viewer application, however, additionally requires that the commercial provider has obtained solution approval granted by the Danish Agency for Digitisation. Under section 10(2) of the regulation, the membership agreement sets the obligation to meet the requirements imposed by each applicable approval. The terms of the membership agreement for commercial viewer applications can be reviewed in advance, as the Danish Agency for Digitisation has published the agreement template with annexes on its website for commercial clients joining Digital Post.

Currently, citizens and companies can choose their digital government mail interface from two public viewer applications and two commercial viewer applications. The public viewers currently are the Digital Post app developed by the Danish Agency for Digitisation, borger.dk maintained collaboratively by the state, municipalities, and regions as a digital portal for citizens' public services, and virk.dk maintained by the Danish Business Authority (Erhvervsstyrelsen) as a portal for communities. The commercial viewer applications are currently e-Boks A/S's e-Boks and Netcompany Group A/S's mit.dk. Through these commercial viewer applications, it is possible to read and receive digital mail not only from public authorities but also from private entities.

The viewers enable citizens and businesses to access official mail that has been sent and archived centrally in the Digital Post solution. The access of natural persons and legal entities to all their digital government mail in the Digital Post solution is secured by the regulation on the transfer of digital mail for natural persons and legal entities in the event of a change of provider (Bekendtgørelse om flytning af fysiske personers og juridiske enheders digitale post ved skift af leverandør, BEK nr 2010 af 15/12/2020). The regulation governs the transfer of data to another provider in situations where the current Digital Post provider, which stores citizens' and companies' digital government mail, changes. Under section 2 of the regulation, the Danish Agency for Digitisation may require the current provider to transfer data to one or more other providers or to the Danish Agency for Digitisation itself.

According to section 16 of the regulation on the approval of viewer applications, commercial providers commit, upon receiving the license for a viewer application, to fulfilling public service obligations when they provide viewer applications. The public service obligations, according to subsection 2 of that provision, consist of the requirement to offer citizens and companies a commercial viewer application that displays digital mail from public senders along with additional services, under the conditions set by the Danish Agency for Digitisation in its decision on solution approval. In the preparatory works for the Danish law on digital government mail, it has been assessed that the public service obligations imposed on commercial providers are so demanding that companies operating under normal market conditions would not offer such solutions. Approved commercial providers are thus granted, under section 17 of the aforementioned regulation, the possibility to apply for compensation for the costs incurred in providing a commercial viewer application.

The compensation paid to commercial providers upon application covers the provider's net costs in fulfilling the public service obligations. According to section 20 of the regulation on the approval of viewer applications, the compensations are distributed among the commercial viewer application providers that applied for it from the Danish Agency for Digitisation's annual appropriation. The compensations consist of a fixed portion, which is divided equally among the providers, and a variable portion, which is distributed according to each provider's share of total log-ins in Digital Post. However, a provider may in any case receive compensation only up to the amount needed to cover its net costs of fulfilling the public service obligations. Public providers of viewer applications do not have a corresponding possibility to apply for compensation.

The processing of personal data in Digital Post between sending authorities and the Danish Agency for Digitisation is regulated separately in the regulation on responsibilities, tasks, and supervision related to the processing of personal data in connection with the sending of digital mail from public senders (bekendtgørelse om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger i forbindelse med forsendelse af digital post fra offentlige afsendere, BEK nr 2019 af 29/10/2021). The regulation stipulates, among other things, that the processing and storage of personal data by the Danish Agency for Digitisation in the Digital Post solution must take place in Denmark. This is because Digital Post is subject to the Danish data protection law requirement that personal data for public administration purposes must be stored entirely or partially in Denmark (section 4(8) of the regulation). The processing of personal data related to legal persons' Digital Post mailboxes is also regulated separately by a regulation concerning responsibilities, tasks, and supervision regarding the processing of personal data contained in messages and their storage in the digital mailboxes of legal persons (bekendtgørelse om ansvar, opgaver og tilsyn i forbindelse med behandlingen af personoplysninger indeholdt i meddelelser og opbevaringen heraf i juridiske enheders digitale postkasse, BEK nr 2020 af 29/10/2021).

5.2.3 Norway

In Norway, citizens generally receive official correspondence electronically unless they have explicitly opted out. Entities registered in the business register also receive official mail electronically at their provided electronic address, but they do not have the same right to opt out of electronic official communication.

To ensure the secure delivery of digital government mail, the Norwegian Directorate for Digitalisation (Digitaliseringsdirektoratet, Digdir) has developed a national shared solution for citizens' electronic mailboxes (Digital postkasse til innbyggere, DPI). Through DPI, authorities can send digital mail to citizens centrally and securely, while citizens can receive and read digital government correspondence in mailboxes offered by commercial providers connected to DPI.

Citizens are not required to use a commercial provider's mailbox; they can choose whether to activate one. Authorities can send mail through DPI regardless of whether the recipient has a digital mailbox or which mailbox they have chosen. DPI is connected to the national register of electronic contact information and opt-outs (kontakt- og reservasjonsregisteret), which contains citizens' electronic contact information and whether they have opted out of electronic government communication. A citizen who has activated a commercial provider's digital mailbox receives a new message notification via SMS or email.

So far, the Norwegian government has agreements for receiving official correspondence in digital mailboxes with two commercial providers: eBoks AS, originally a Danish company, which offers the eBoks service, and Norges Post AS, which offers the Digipost service. Citizens can therefore choose either of these services to receive electronic government mail through DPI. Digital mailboxes offered by commercial providers can also receive electronic mail from non-government senders, such as private entities. Commercial providers linked to DPI are responsible for making government messages available and for storing them, and they are subject to specific security requirements.

Authorities sending mail through DPI pay the Norwegian Directorate for Digitalisation (Digdir) for messaging, delivery, and storage in the digital mailboxes. Transmission is charged per message, while delivery and storage are subject to a transaction-based fee calculated based on the size of the delivered messages and the number of deliveries. Digdir then distributes this compensation to the two commercial providers which it has contracted for digital mail services. Public administration organisations using DPI can also opt to use DPI's paid printing and postal service, where mail is printed, enveloped, and sent by mail to recipients who cannot or do not wish to receive mail digitally.

In addition to the commercial digital mailboxes, citizens can also receive electronic government messages through the Altinn portal maintained by Digdir. Some authorities, such as the Norwegian Tax Administration, use Altinn to send messages to citizens. Through Altinn, citizens have been able to receive digital government mail even before the national DPI solution was implemented in 2014. All Norwegian citizens have an electronic mailbox in Altinn linked to their personal identification number for receiving electronic government messages. Beyond receiving government mail, citizens can use Altinn to interact with authorities for notifications, applications, and other administrative matters. Altinn also serves as a portal for organisations: registered entities can communicate with authorities electronically, fulfil reporting obligations, handle various administrative needs, and develop services via Altinn. Like citizens, these organisations have their own mailboxes within Altinn.

The Norwegian Ministry of Digitalisation and Public Administration (Digitaliserings- og forvaltningsdepartementet) has instructed that organisations must use DPI to send mail to citizens who have chosen a digital mailbox and have not opted out of electronic government communication. This guidance is based on the ministry's digitalisation circular (Digitaliseringsrundskrivet, 25/242-1), which compiles instructions and recommendations for digitalisation in the public sector. According to the digitalisation circular, messages can still be sent to a mailbox in Altinn if the citizen has not selected a digital mailbox but has also not opted out of receiving digital government mail. For entities conducting business or other organisations with a business ID, public authorities are, according to the circular, generally required to use the Altinn mailbox to send digital mail to these recipients.

In addition to DPI, another centralised solution for digital government communication has been developed: the KS FIKS messaging platform, aimed at municipalities and other public actors. The platform is developed and maintained by KS Digital, which is managed by regional and municipal authorities. The messaging platform includes services for sending and receiving messages: SvarUt and SvarInn. Using the SvarUt sending service, municipalities and other public actors can send electronic messages directly from case management, archival, or other systems to various recipient channels, including commercial digital mailboxes or the Altinn portal. With the SvarInn receiving service, municipalities and other actors can store incoming mail directly in their case management, archival, or other systems from organisations using the SvarUt service.

Norway's government digitalisation program, På nett med innbyggerne, published in April 2012, established as a principle that citizens and businesses should receive mail from public administration in a single, secure digital mailbox. According to the report by Norway's Digitalisation Directorate, by 2019 the use of digital mailboxes through DPI had grown slowly. Public actors joined the infrastructure gradually, and citizens found it difficult to understand why they should create a new mailbox alongside the existing digital mailbox in the Altinn portal. Organisations sending messages also lacked incentives to use DPI, as it was seen as incurring additional costs and reaching fewer citizens than Altinn. The report stated that the infrastructure has not been able to fully exploit its potential, and end users cannot access all digital mail in one place; they still need to use multiple mail solutions.

The possibility of receiving government mail electronically is primarily based on Norway's Public Administration Act (Forvaltningsloven, LOV-1967-02-10). Under section 15 a of the Public Administration Act, authorities may use electronic communication when interacting with others unless otherwise provided by law or regulations issued under the law. The use of electronic communication by authorities is also regulated in the Regulation on Electronic Public Administration (eForvaltningsforskriften, FOR-2004-06-25-988). Electronic communication by authorities became the default in 2014, when a reference to electronic communication was added to section 15 a of the Public Administration Act and the requirement for the recipient's consent to send decisions and preliminary notifications electronically was removed (Lov om endringer i forvaltningsloven, LOV-2013-06-14-42). At the same time, the Regulation on Electronic Public Administration was amended to include the right to opt out as well as provisions regarding a new registry of electronic contact information and opt-outs (Forskrift om endringer i forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen, FOR-2014-02-07-102).

Under section 9 of the regulation on electronic public administration, citizens and entities not registered in the business register have the option to opt out of receiving certain official messages electronically. The right to opt out applies to electronic decisions, preliminary

notifications, and other notices that affect the person's legal status or the handling of a matter, or for which ensuring receipt by the individual is particularly important for other reasons. Opt-outs are recorded in the registry of electronic contact information and opt-outs maintained by Digdir, as set out in section 29 of the regulation. If a person has opted out of receiving electronic government mail, they will receive these messages by paper mail. A citizen will generally also receive government mail on paper if they have not provided a mobile phone number or email address when registering with the electronic public service, because delivery of electronic government mail requires the citizen to provide electronic contact information to the authorities.

Norway's Public Administration Act was comprehensively revised in 2025 and, in June 2025, the Norwegian Government approved a new law on the handling of cases in public administration (Lov om saksbehandlingen i offentlig forvaltning (Forvaltningsloven), LOV-2025-06-20-81), which replaces the previous Public Administration Act. The law is not yet in force, as it will enter into effect on a date determined by the King. The provisions on electronic public administration in section 15 a of the current Public Administration Act have mainly been transferred, with the same content, to section 10 of the new Public Administration Act.

5.2.4 Netherlands

In the Netherlands, receiving digital mail from public authorities is optional. Citizens and businesses can only receive digital mail from public authorities via digital mail solutions maintained by the state. The state provides both natural persons and legal entities with a separate digital mailbox (berichtenbox). The citizens' digital mailbox operates within the MijnOverheid service, maintained by Logius under the Ministry of the Interior and Kingdom Relations , and enables one-way communication from authorities to citizens. The digital mailbox for legal entities is maintained by the Netherlands Enterprise Agency through the Ondernemersplein portal for businesses. Legal entities can also send messages to authorities through their own digital mailbox.

The MijnOverheid service and its digital mailbox are based on the Dutch Digital Government Act (Wet van 24 maart 2023 tot algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur) and related regulations. Section 5 of the Digital Government Act stipulates that the Minister of the Interior and Kingdom Relations is responsible for designing, providing access to, maintaining, operating, and securing the general digital infrastructure, including electronic communications and the infrastructure for communicating with natural persons, businesses, and legal entities. The infrastructure for electronic communication and notifications for natural persons via the MijnOverheid service is regulated in the Decree on Digital Services Infrastructures (Regeling voorzieningen Wdo, BWBR0048167). According to section 1 of this decree, a MijnOverheid account is available to any person who is at least 14 years old, receives services from the Dutch government, has a citizen service number, and possesses or can obtain a recognised electronic identification method.

Under section 2(13) of the Dutch General Administrative Law Act (wet van 4 juni 1992, houdende algemene regels van bestuursrecht (Algemene wet bestuursrecht)), authorities and public administration clients may communicate electronically with each other, unless the law provides otherwise or a formal requirement prevents electronic communication. Authorities may also, pursuant to section 2(14) of the same law, send messages to one or more recipients electronically, provided that the recipient has indicated that they can be reached reliably in this

manner. Provisions on electronic communication in administrative matters were added to the Dutch General Administrative Law Act through the 2023 law modernising electronic administrative communication (wet van 10 mei 2023 tot wijziging van de Algemene wet bestuursrecht in verband met de herziening van afdeling 2.3 van die wet (Wet modernisering elektronisch bestuurlijk verkeer)). Under section 5(2) of the Decree on Digital Service Infrastructures, a natural person indicates that they are able to receive messages digitally in their mailbox when they activate the MijnOverheid service.

Not all authorities offer the possibility to send digital mail to citizens' mailboxes, as organisations are not required to send messages through the MijnOverheid service linked to the digital mailbox. Furthermore, according to section 5(4) of the same decree, natural persons can choose from which sending authorities they wish to receive electronic mail in their digital mailbox.

The processing of personal data in the MijnOverheid service is regulated separately in the Decree on Digital Government (Besluit digitale overheid, BWBR0037987).

5.2.5 Belgium

In Belgium, every citizen has the option to activate their own digital mailbox, eBox, into which authorities can send documents digitally. eBox is a state-managed service infrastructure through which public administration actors can communicate with natural persons and organisations with a company registration number, as well as receive messages from them. Sending digital government mail to eBox requires that the citizen has explicitly consented to electronic communication with public administration actors via eBox and has activated their digital mailbox. The digital mailbox service for natural persons is provided by the federal public service responsible for the digital agenda (le service public fédéral compétent en matière d'Agenda numérique), SPF BOSA (le service public fédéral Stratégie et Appui), through its Directorate-General for Simplification and Digitalisation. The digital mailbox service for companies is provided by the National Social Security Office (l'Office national de sécurité sociale).

The eBox infrastructure is based on the 2019 law on the electronic exchange of messages via eBox (Loi relative à l'échange électronique de messages par le biais de l'eBox, 2019040657). The law regulates the provision and use of the service, the roles in personal data processing within the service, and the participation of service providers acting as message viewers.

Citizens can receive and read government messages sent via eBox through either public or private digital portals or mail services. A user of the digital mailbox can choose from several options for the interface they wish to use, which is then connected to their eBox digital mailbox. Between the interfaces of the sending authorities and the recipients, the SPF BOSA-managed eBox infrastructure functions as a kind of message relay layer. Sending authorities connect to the eBox infrastructure either directly using an internal public administration service integrator or technical platform (document provider), or via a private service provider (document service provider). A public administration service integrator or technical platform can be the sending authority itself, or the authority can make use of SPF BOSA's Directorate-General for Simplification and Digitalisation, or another service provider, in this context. Messages are always made available to the interfaces through the public administration service integrator or technical platform, and the messages are also stored on these platforms.

Sending authorities are required to conclude an agreement on messaging via eBox with SPF BOSA's Directorate-General for Simplification and Digitalisation. Public actors providing interfaces must also sign an agreement with SPF BOSA's Directorate-General for Simplification and Digitalisation. Private actors who wish to provide access and an interface to eBox must, on the other hand, obtain permission from SPF BOSA's Directorate-General for Simplification and Digitalisation to join the infrastructure. The permission is based on Article 11 of the law governing the eBox infrastructure. Under this provision, SPF BOSA's Directorate-General for Simplification and Digitalisation may temporarily deny a service provider's authorisation and require corrective measures if the service does not comply with the conditions of the authorisation. Ultimately, the authorisation can be revoked if the service provider has not taken the necessary steps to correct deficiencies that led to the temporary denial. The requirements for private service providers' authorisation, as well as the approval process and consequences, are regulated by a royal decree concerning the conditions, procedure, and consequences for the approval of service providers for the electronic exchange of messages via eBox (Arrêté royal fixant les conditions, la procédure et les conséquences de l'agrément de prestataires de services pour l'échange électronique de messages par le biais de l'eBox, 2019013116). According to Articles 2 and 3 of the decree, private service providers' digital mailbox interfaces must, among other things, offer the mailbox functionality free of charge to users receiving messages and display all messages received in eBox in their interface without special selection or filtering.

Currently, citizens can choose from three publicly managed interfaces: my eBox, Mijn Burgerprofiel, and IRISBox. The my eBox service is provided by the federal SPF BOSA for citizens to read electronic mail sent by authorities. A separate interface is also available for businesses (e-Box Enterprise). Mijn Burgerprofiel is a portal provided by the Flemish regional government in Flanders, where citizens can not only read their public administration digital mail but also access other government-related information. IRISBox is the portal of the Brussels regional government, offering regional and local online services. Currently, private providers connected to the eBox infrastructure include Doccle, KBC Mobile, and TrustO. Doccle is a commercial service where citizens can receive electronic mail from both companies and authorities, archive documents, and generally manage incoming documents and invoices. Its purpose is also to digitalize and centralize administrative tasks from companies and organisations into a single service. KBC Mobile is an application offered by KBC Bank to its clients, where bank customers can link their eBox and view and manage electronic messages received in eBox. TrustO is a commercial service where citizens can receive digital mail from authorities via eBox, as well as messages from other organisations and emails from private individuals.

5.2.6 Estonia

In Estonia, the model for sending and receiving digital official messages and notifications is fully managed by the state. All citizens and companies have access to a state-provided electronic mailbox (riiklik postkast) for receiving official messages and notifications through the national digital service portal eesti.ee. The eesti.ee portal and the national digital mailbox solution are managed by the Information System Authority (Riigi Infosüsteemi Amet, RIA), which operates under the Ministry of Justice and Digital Affairs (Justiits- ja Digiministeerium). The state-provided digital mailbox works through the citizen's or company's official email address ending in @eesti.ee. This official email address is linked to a citizen's Estonian personal identification code or a company's registration number in Estonia, which forms the first part of the email address.

The eesti.ee portal and the official email addresses are regulated by a decree on the management, accessibility, development, and use of the Estonian information portal eesti.ee (Eesti teabevärava eesti.ee haldamise, teabe kättesaadavaks tegemise, arendamise ning kasutamise nõuded ja kord, RT I, 29.12.2024, 10). According to section 20^1 of this decree, a public authority may deliver information to the user's official email address or phone number via the official email system. As the service provider, RIA is obligated to notify citizens and companies of incoming information to their official email address using another email address or phone number provided by the user.

State and local government authorities, as well as other public service entities, can send documents and notifications to the national digital mailbox once the recipient has activated their mailbox. Sender organisations can also notify users via text message if the user has registered a phone number in the digital mailbox. Messages can additionally be forwarded to the citizen's regular email address. Only entities that have signed an agreement with RIA are authorised to send messages to the state digital mailbox.

The management interface of the state digital mailbox solution is structured like a modern SaaS service. It consists of a user interface for the message recipient, a centralised administration system that distributes notifications and delivers emails and text messages, and an administrative interface for sending organisations. Both the user interface and the sender organisation interface can be used through RIA's infrastructure or integrated into the sending organisation's own infrastructure and self-service portal. The user interface for the digital mailbox is available via the eesti.ee website in a browser and through the Eesti app mobile application. The user interface for the digital mailbox is the eesti.ee website in a browser and the Eesti app mobile application.

In 2024, Estonia updated its state digital mailbox solution, significantly changing both the mailbox logic and the underlying systems. The new digital mailbox solution was made available to citizens in April 2024. The previous backend systems had been used for message delivery for nearly 20 years. In the future, the Estonian government intends for the state digital mailbox to be accessible through all government service portals, with all official notifications delivered via this system. So far, private digital mailbox services have not been integrated into the state model for delivering official electronic communications.

The Estonian Administrative Procedure Act (haldusmenetluse seadus, RT I, 06.07.2023, 31) governs the electronic delivery of official documents. According to section 25, administrative decisions, summonses, notifications, and other documents can be delivered to parties involved in an administrative matter electronically. If the law or regulations do not specify a particular delivery method, the authority may, under section 5(1), choose the method at its discretion. Under section 27, in electronic delivery, a document is made available in the relevant information system or via the Estonian service bus, or it can be sent by email to the concerned party. According to Estonia's Digital Agenda 2030, the state digital mailbox is intended to become the legally established main channel for delivering public administration notifications and documents, replacing paper letters.

6 Feedback

To be supplemented after the consultation procedure.

7 Provision-specific rationale

Section 2 *Definitions.* A new subsection 6 would be added to the section, according to which a "viewer application" is understood in this law as a digital service that functions as the user interface of a messaging service. In addition to a viewer application provided by the service provider, the user interface of the messaging service could also be provided by other service providers' viewer applications, if the service provider, pursuant to an agreement under section 8g, has assigned the task of providing the viewer application to them as well. Through the viewer application or applications, users would have access to the electronic notifications and other messages in their messaging service account.

Section 8f *Provision of a viewer.* Subsection 1 would regulate the basic principle that the service provider of the messaging service, currently the Digital and Population Data Services Agency, is responsible for the viewer application enabling the use of the messaging service. In practice, the service provider already carries out this responsibility by providing the Suomi.fi Messages service. The provision would clarify the scope of tasks assigned to the service provider, as in the future the user interface to the messaging service could also be provided by another actor. The service provider would be solely responsible for producing and developing the technical infrastructure behind the message exchange service, pursuant to Section 4(1) currently in force.

The service producer would be required to provide a viewer application even if it had, under a contract made pursuant to section 8g, assigned the task of providing a viewer application to another service provider or providers. In other words, the service provider would continue to be required to provide a viewer application, that is, the current Suomi.fi Messages interface, even if it had enabled the provision of a viewer application contractually to other service providers.

Subsection 2 of the section would regulate the procedure for delivering notifications and other messages received in a user's messaging service account to the service provider's viewer application. The purpose of the view opened to the message exchange service account is to allow a person using another viewer application to inspect notifications and other messages delivered by authorities to their messaging service account from the service they use.

The service producer would open the view of the user's messaging service account in the service provider's viewer application if the user had indicated that it was the viewer application they use in the register referred to in section 11. The view would be opened only temporarily for the duration of a single session. All documents and messages would be recorded and stored centrally in the backend service of the messaging service.

To enable freedom of choice, the user could indicate in the user register of the messaging service which of the services of the service providers that have entered into a contract under section 8g they wish to use as their viewer application. The user could simultaneously select multiple services they wish to use. The information would be recorded in the user register of the messaging service, and electronic notifications and other messages received in the messaging service would then be displayed in the service or services selected by the user. In addition, notifications and other messages would always be readable in the viewer application provided by the service provider.

Chapter 2b. Service provider viewer application

It is proposed that a new Chapter 2b be added to the Act, which would regulate viewer applications offered by operators other than service providers in messaging services. This chapter would provide for the conditions for the delegation of the task of assisting in a public administration task concerning the provision of a viewer application and the minimum content of the related agreement, the requirements for service providers, the supervision to which they are subject, the cooperation between them and the service provider, the response to incidents and the possibility for the user to choose the viewer application that they use.

Section 8g *Assigning the task of providing viewers to a service provider.* This section would provide for the possibility for the service provider to entrust by contract the performance of a viewer application considered to be ancillary to a public administration task also to an operator that meets the conditions laid down in section 8h. The section would satisfy the requirement set out in Section 124 of the Constitution that a public administration task may be entrusted to an entity other than an authority only by law or pursuant to law, if necessary for the proper performance of the task and without endangering fundamental rights, legal protection, or other requirements of good administration. The Constitutional Law Committee has considered that tasks assisting authorities may be transferred by agreement to entities other than authorities (PeVL 11/2006, p. 2, and PeVL 2/2018, p. 4).

Subsection 1 would provide for the competence of the service producer to entrust the task of offering a viewer application referred to in the proposed section 8f to another service provider on the basis of a contract. The amendment would therefore not transfer the task of providing a viewer application away from the service provider of the messaging service, but would only establish the legal basis for allowing another service provider to offer a viewer application on the basis of an agreement with the service provider. The service producer would, as a rule, enter into agreements with all service providers that meet the requirements and wish to provide a viewer application. All willing service providers that meet the statutory requirements could thus participate in offering the service, provided that they accept the conditions set by the service producer in the agreement. In such a situation, this would not constitute a public procurement, and the Act on Public Procurement and Concession Contracts (1397/2016) would not apply to the making of the agreements.

Subsection 2 of the section would stipulate that criminal official liability also applies to a person performing a public administration task in the employ of a service provider. The subsection also contains an informative reference to the Act on Compensation for Damages. References to criminal official liability and the Act on Compensation for Damages are necessary in order for the task to be entrusted to a private entity. The display of electronic notifications through a viewer application does not constitute the exercise of public authority, but rather the performance of a task assisting in a public administration function. The provisions of the Criminal Code on official offences are therefore not directly applicable on the basis of Chapter 40 of the Criminal Code (39/1889), but the extension of criminal official liability to public administration tasks that do not involve public authority must be enacted in special legislation, as required by the Constitutional Law Committee.

Since the task being transferred is a public administration task referred to in Section 124 of the Constitution, the service provider and its personnel must comply with the general administrative laws while performing it. The section does not, however, separately regulate the general laws applicable to the service provider and its personnel, as this is not necessary according to the practice of the Constitutional Law Committee: these laws apply even without a specific provision (PeVL 34/2010, p. 5). Based on their provisions relating to their scope, the definition of public authorities, or the language obligation of private operators, the general

administrative acts also apply to individuals carrying out public administration tasks (PeVL 42/2005 vp, p. 3/II). The obligation to comply with the general administrative laws arises directly from the law even when a contract is made between an authority and a private entity for the performance of a public administration task (PeVL 3/2009, p. 5). At a minimum, the performance of the tasks would be subject to the Information Management Act, the Act on Openness, the Digital Services Act, the Act on Electronic Services, the Administrative Procedure Act, and language legislation. Under the general requirements of non-discrimination in administration, the service provider must also ensure equal treatment of recipients of notifications.

According to Section 4 of the Act on Openness, a private entity is also considered an authority when performing a public administration task that involves the exercise of public power. In the performance of the task under this proposal, however, public power would not be exercised, and the service provider carrying out the task would therefore not fall within the definition of an authority in the Act on Openness. A document that is issued on behalf of an authority for the purpose of performing an assigned task is nevertheless regarded as an official document under Section 5 of the Act on Openness. The confidentiality obligations provided by law thus apply to a person performing the task on assignment pursuant to section 23 of the Act on Openness.

Section 8h *Requirements for the service provider*. The proposed subsection 1 would lay down requirements for the service provider. The requirements are intended to ensure the proper performance of the activity. Prior to entering into a contract, the service producer must ascertain that the service provider meets the requirements and monitor that they continue to be met throughout the duration of the contract. Similarly, the service provider must ensure that it complies with the requirements imposed on it.

Since the task being transferred involves documents containing personal data on behalf of user organisations, the user organisations, the service producer, and the service provider must be able to ensure proper information security and data protection as provided in Article 28 of the General Data Protection Regulation. For example, the service provider must implement the necessary measures to protect personal data against unauthorised access and against accidental or unlawful destruction, alteration, disclosure, transfer, or other unlawful processing. In general, under the General Data Protection Regulation, the service producer may not use data processors who do not meet the requirements set out in the regulation.

With respect to the assessment of the right to conduct business, the Enterprise Act (565/2023) shall apply.

Technical capabilities mean that the service provider must have at its disposal the data connections, information systems, and other technical resources necessary for the proper performance of the task. Technical capabilities may, for example, relate to the structure of messages, methods of data transmission, and capacity requirements. Technical requirements also include responsibility for ensuring information security. Regarding information security requirements, the rules set out in the eIDAS Regulation, the Information Management Act, and the Cybersecurity Act shall apply as described above.

Financial capabilities mean that the service provider must be solvent, that is, able to properly meet its financial obligations. The service provider’s solvency shall always be verified before entering into a contract. For example, a person or entity in bankruptcy could not act as a service provider.

Professional and operational capabilities mean that the service provider must possess professional expertise. Professional requirements apply to both the service provider as a business and to its personnel. The service provider must organise its operations so that it can properly perform the tasks assigned to it. In addition, the service provider must have sufficient personnel with the professional competence and training necessary for the proper performance of the tasks. Operational capabilities include, among other things, responsibility for ensuring proper data handling, interoperability, and compliance with other requirements set for the operation covered by the contract.

The proposed *subsection 2* would provide for an assessment of the reliability of the service provider. A service provider is not considered reliable if he or she is not currently operational, has been banned from engaging in commercial activities in the past year, has been sentenced to prison in the past five years or issued a fine in the last three years for a serious infringement of an employment relationship, business, accounting or debt legislation or regulation, and if he or she has been sentenced to imprisonment for another serious crime which can be considered to affect his or her reliability or make it manifestly inappropriate for him or her to undertake the tasks referred to in this chapter. The assessment of the service provider's reliability shall concern its persons in a controlling position as well as the personnel performing the tasks referred to in this chapter.

The assessment shall concern the service provider's persons in a controlling position as well as the personnel responsible for and performing the tasks. A person responsible for a task could, for example, be the system manager in charge of the viewer application. For the service provider, the assessment shall cover persons in a controlling position, such as members or deputy members of the board of directors or supervisory board, partners, the managing director, a shareholder exercising significant voting power in the company, or a person whose controlling position is based on a separate agreement. If any of these persons do not pass the assessment, the service provider cannot be considered reliable.

Section 8i *Agreement on the provision of a viewer application.* The proposed first subsection would regulate the content of the agreement concluded with the service provider. The section would specify the matters that must at a minimum be agreed upon in the contract. These provisions would ensure the proper performance of the service provider's tasks. The contractual transfer of public administration tasks is permitted under section 124 of the Constitution when the constitutional requirements for the delegation of the task are met and there is an appropriate statutory authorisation for concluding the agreement (PeVL 3/2009, PeVL 11/2006). In practice, the terms of the agreement would primarily be based on standard conditions prepared by the Digital and Population Data Services Agency, which would be uniform for all actors and publicly accessible.

At the beginning of the subsection, there would be an informative reference to Article 28(3) of the EU General Data Protection Regulation. That provision specifies the matters that must be included in the contract between a controller and a processor. Since European Union regulations are directly applicable, they apply as such without explicit references. Accordingly, references should generally be avoided, but for the sake of regulatory clarity, a reference would be justified in this context.

In principle, the service provider would be required to conclude contracts with all those who notify the service provider of their willingness to carry out the task and meet the statutory requirements. The agreement would be an administrative agreement. According to section 20(1)(4) of the Administrative Judicial Procedure Act (808/2019), an administrative court

handles as an administrative litigation any case concerning an administrative contract. The service producer would draft the contract terms, which would be standardized in nature and generally available prior to concluding the agreement.

The subsection would specify the matters that must at least be agreed upon in the contract to ensure the proper performance of the service provider's tasks. According to point 1 of the subsection, the agreement would cover the service provider's tasks other than the processing of personal data. The contract should also address the processing of personal data, but this requirement would derive directly from Article 28(3) of the EU General Data Protection Regulation. When drafting the agreement, it should be noted that the GDPR's list is not exhaustive. Thus, the contract could, for example, require the service provider to appoint a responsible person. The responsible person would train the service provider's personnel after first completing training themselves, inform staff on related issues, and otherwise act as a liaison with the service producer regarding matters necessary to ensure the personnel's adequate professional competence and the quality of operations.

According to point 2 of the subsection, the contract should specify the contract term, the commencement of operations, and the procedure for termination of the agreement before the end of the contract term.

According to paragraph 3, agreement should be reached on the requirements set for the viewer application offered by the service provider. The matter would concern the operational requirements imposed on a service provided by a private provider, such as the ability to respond to messages received through the service and to receive both ordinary and legally verifiable notifications. Since this concerns a service for which the service producer is responsible, the contract could specify in more detail the conditions under which the service producer could, if necessary, unilaterally modify the requirements set in the contract for the viewer application. Similarly, the contract could regulate the service provider's right to terminate the agreement in such a situation.

According to point 4 of the subsection, the contract should address procedures to ensure the adequate professional competence of personnel performing the tasks. Such procedures could include, for example, training or instructions provided by the service provider.

According to point 5 of the subsection, the contract should specify the retention and archiving of documents related to the operations.

With respect to information security, the requirements imposed on service providers would, in a corresponding manner to those applied to the service producer, be those set in the Cybersecurity Act for non-qualified trust service providers under the eIDAS Regulation. These information security requirements apply to service providers based on the activities they perform; therefore, it may not necessarily be required to specifically include such requirements in the contract between the service producer and the service provider. The service providers would also be subject to the information management law's Chapter 4 information security requirements to the extent that they perform the relevant task.

The responsibility of actors displaying notifications via their viewers for errors in delivering the document to be notified, such as technical errors, is generally determined according to the standard rules of tort liability. However, liability between the service producer and the service provider could be agreed differently or in more detail in the contract governing the performance of the task.

According to the proposed subsection 2, the service provider would be required to provide the service producer with the necessary evidence that the requirements referred to in section 8 h are met before the contract is concluded. The service producer could reasonably require, for example, sufficient documentation demonstrating compliance with the statutory requirements and the contractual conditions.

According to the proposed subsection 3, the service producer could terminate or cancel the contract if the service provider no longer meets the general requirements or if the service provider substantially neglects the performance of the agreed contract or otherwise violates the contract or acts essentially or repeatedly unlawfully. The provision would not prevent the contract from also including other terms regarding termination or rescission.

According to the proposed subsection 4, the service provider would be required to promptly notify the service producer of any changes in its operations that could have a material impact on the performance of the tasks entrusted to it. Such a situation could arise, for example, if the ownership structure of the service provider changes, or if the service provider that has a contract with the service producer makes significant changes to its service that would affect the practical fulfilment of the matters agreed in the contract. The service providers' obligation to report material changes would give the service producer the opportunity to assess whether the conditions set out in the contract concluded with the service provider under sections 8h and 8g are still met despite the changes, or whether the changes are such that they require termination or rescission of the contract pursuant to subsection 3.

Section 8j *Cooperation between the service producer and service providers.* The section would regulate the cooperation between service providers and the service producer. The purpose of the provision is to ensure that the service producer and all parties connected to the backend of the messaging service cooperate to ensure that authorities' electronic notifications are delivered to the correct recipients smoothly and securely. Cooperation to harmonise technical practices is necessary to guarantee technical interoperability, also as the technology related to the messaging service and digital mail services evolves. In addition to interoperability, the service producer and service providers must cooperate to ensure information security. For example, the service producer and service providers could agree on appropriate cooperation forums in which they could exchange up-to-date information regarding the operation and security of the services. The cooperation obligation under this provision would not, of course, require service producers or service providers to share trade secrets or other information in a manner contrary to competition law.

Section 8k *Disruption situations.* The section would regulate the possibility for the service producer of the messaging service and the service providers to disconnect their services from each other in the event of disruptions. If necessary, the service producer or a service provider could disconnect their information system or service from a system maintained by the other party, and vice versa. By disconnection is meant that data transfer between the systems is stopped completely or partially, depending on the severity of the disruption. Disconnection could be applied in serious disruption situations where less severe measures would not be sufficient. The service or information system causing the disruption must be reconnected without delay once it has been confirmed that it no longer causes harm. The section would not separately regulate the notification to the public regarding service interruptions of the messaging service or the viewer application, as this matter is covered by the provisions of Section 4(2) of the Digital Services Act.

Section 8l *Supervision of a service provider performing a public administration task.* The provision would regulate the authority and right of the service producer to supervise the activities of service providers in the performance of the public administration task assisting function referred to in section 8g. The service producer would have the right to carry out audits at the premises of a service provider and, without prejudice to the confidentiality provisions, provide information on documents relating to the service. In addition, the service provider must provide the service producer with the information necessary to supervise compliance with the Support Services Act. Audits should not be carried out on premises of permanent residence. Inspections of premises shall follow the procedure laid down in section 39 of the Administrative Procedure Act regarding inspections within the competence of an authority. The provision would give the service producer a general right to supervise service providers. The service producer and service provider may agree in more detail on the procedures for supervision, for example in connection with the agreement made pursuant to section 8g.

In addition to the service producer, service providers would also be supervised by other authorities under the powers granted to them elsewhere in legislation. Such supervising authorities would include, for example, the Data Protection Ombudsman with respect to compliance with provisions on the processing of personal data, and the Finnish Transport and Communications Agency (Traficom) with respect to compliance with the eIDAS Regulation, the Cybersecurity Act, the regulations issued under it, and the provisions issued pursuant to the NIS 2 Directive.

8 Entry into force

It is proposed that the Act enter into force on 1 July 2026.

9 Implementation and monitoring

The technical, functional, and administrative changes required by the proposal for Suomi.fi Messages and the procedures related to the provision of the service will be implemented as part of the Programme to Promote Primarily Digital Official Communications (VM006:00/2024) established by the Ministry of Finance. The regulation proposed in the draft allows the service provider to conclude an agreement with a service operator regarding the provision of the viewer application, but it does not obligate the service provider to complete the technical implementation by a specific date. The technical implementation of the viewer application provision task proposed in the draft is therefore unlikely to be ready by the date of entry into force of the law as proposed. The achievement of the objectives will be assessed and monitored as part of the statutory general steering duties of the Suomi.fi services under the Support Services Act.

10 Relationship to the Constitution and the legislative procedure

10.1 Protection of private life

According to section 10(1) of the Constitution, everyone’s private life, honour and inviolability of one’s premises are safeguarded. Further provisions on the protection of personal data are laid down by law. According to the practice of the Constitutional Law Committee (PeVL 51/2002 vp, p. 2/I; PeVL 6/2003 vp, p. 2/I), the scope of privacy protection secured in this subsection also partially covers the protection of personal data. Section 10 of the Constitution on the protection of private life also provides for the confidentiality of

messages. Subsection 2 of the provision establishes that the secrecy of letters, telephone calls, and other confidential messages is inviolable. The provision is both instrument- and technology-neutral, and it generally safeguards the confidentiality of all types of private communications (HE 309/1993 vp, p. 53). The provision guarantees everyone the right to confidential communication without outsiders being able to obtain information about the contents of messages sent by them or addressed to them.

The effects of the changes proposed in the government draft on the privacy and personal data protection safeguarded by section 10(1) of the Constitution relate to the exercise of the data subject's privacy rights and the secure and lawful processing of personal data. With regard to the confidentiality of messages protected under section 10(2) of the Constitution, the effects relate to the protection of confidential communications in notices received by public administration clients from authorities against third-party access. The effects of the proposal on the protection of personal data and the confidentiality of messages are described in sections 4.2.2.3 and 4.2.3.2. The changes proposed in the proposals are assessed as having a positive, albeit minor, impact on the exercise of data protection rights. At the same time, the proposed changes are also assessed as carrying a risk of adverse effects on the protection of personal data and the confidentiality of messages. The potential adverse effects would relate to possible deficiencies in information security, access control, and the lawful processing of personal data, as well as potential data breaches and other cyberattacks.

The risk of adverse effects on personal data protection and the confidentiality of messages is mitigated by agreements on the processing of personal data between all actors in the processing chain in accordance with data protection legislation. The risks arising from the processing of personal data would be assessed to the necessary extent before the processing operations commence, and the technical and organisational measures corresponding to the risk of the processing would be implemented. As the service provider of the Suomi.fi Messages backend service and the data controller for the overall system, the Digital and Population Data Services Agency would have a significant role in ensuring the protection of personal data related to the functionalities of Suomi.fi Messages. With regard to the protection of the confidentiality of messages, the risk of unauthorised access to messages related to official notifications could also be reduced through features developed by private digital mail operators, but ultimately also through actions taken by end users.

The proposal does not suggest using the national discretion contained in the (GDPR) with respect to complementary or clarifying national legislation. According to the Constitutional Law Committee, it is generally sufficient that the regulation on the protection and processing of personal data is compatible with the GDPR. The Committee considers that the protection of personal data must primarily be ensured under the GDPR and the national Data Protection Act. The enactment of special national legislation should therefore be approached cautiously and limited only to what is necessary within the scope of discretion permitted by the GDPR. However, the Committee notes that the need for special regulation must also be assessed in accordance with the risk-based approach required by the GDPR, paying attention to the threats and risks arising from the processing of data. The greater the risk that processing poses to the rights and freedoms of a natural person, the more justified detailed regulation becomes (Constitutional Law Committee Report PeVL 14/2018, pp. 4–5). Conversely, the lower the risk posed by processing, the more justified it is to adhere to general regulation.

Given that the measures presented above, and in sections 4.2.2.3 and 4.2.3.2, to reduce risks related to data protection and the confidentiality of messages would be implemented, the harmful effects arising from the proposal are, in this regard, considered to be identifiable in

terms of severity but unlikely in terms of probability. Accordingly, the risks of potential compromise to personal data protection and the confidentiality of messages are assessed overall as low. Therefore, for the provisions proposed in the proposal, there is no assessed need for national legislation complementing the General Data Protection Regulation, and the proposal is not considered to conflict with the protection of private life under section 10 of the Constitution.

10.2 Legal protection and good governance

According to section 21 of the Constitution, everyone has the right to have their case dealt with appropriately and without undue delay by a legally competent court of law or other authority, as well as to have a decision pertaining to their rights or obligations reviewed by a court of law or other independent organ for the administration of justice. The publicity of the proceedings and the right to be heard, the right to receive a reasoned decision and the right of appeal, as well as other guarantees of a fair trial and good governance, are laid down by an Act. The principles of good administration are laid down in chapter 2 of the Administrative Procedure Act.

The provision of section 21 of the Constitution must be read as a whole (HE 309/1993 vp, p. 72). The provision lists the most important elements of good administration and a fair trial, namely the publicity of proceedings, the right to be heard, the right to receive a reasoned decision, and the right to seek a review or appeal. The list is not intended to be exhaustive (PeVL 43/2021 vp, section 2). The requirement of impartiality in official activities, as well as the service principle laid down in the Administrative Procedure Act, may be linked to the requirement of appropriate handling of matters set out in subsection 1. Under the service principle in section 7(1) of the Administrative Procedure Act, dealings with and the handling of matters by an authority must be arranged so that persons dealing with the administration receive appropriate administrative services and the authority can perform its duties effectively. The service principle also includes an obligation to arrange dealings with the administration in such a way that users of digital services receive appropriate digital administrative services. In electronic dealings with the administration, the service principle is a key element when assessing the quality of electronic official activities. Legislation must not jeopardise anyone's legal protection (PeVL 5/2016 vp, p. 3). However, the provisions of section 21 of the Constitution do not preclude the enactment by law of minor exceptions to the rights safeguarded therein, provided that such exceptions do not alter the status of the relevant legal safeguard as the main rule and do not, in an individual case, jeopardise an individual's legal protection (HE 309/1993 vp, p. 74; see also, e.g., PeVL 43/2021 vp, section 2; PeVL 39/2014 vp, p. 2).

In the draft Government proposal, the effects of the proposed amendments on the legal protection guaranteed by section 21 of the Constitution and on good administration safeguarded by law relate primarily to the authority's duty of service and the effective method of service, in accordance with the service principle laid down in section 7 of the Administrative Procedure Act. The effects of the proposal on legal protection are described in section 4.2.2.2. The proposed amendments are assessed as strengthening, to a limited extent, the prerequisites for legal protection and good administration for those individuals who primarily use, for example, a service provided by a private service provider to receive their electronic messages. However, the proposal is also considered to potentially entail certain risks to the realisation of legal protection. A person should understand that choosing a viewer application and having this recorded in the service provider's user registry means that they will need to monitor the chosen service to receive electronic notifications and other messages

from authorities in the future. Otherwise, the receipt of ordinary electronic notifications of service sent by authorities in particular could be jeopardised.

Potential risks to legal protection can be mitigated through information measures, including both general communication about the changes resulting from the legislative proposal and individualised information provided when the customer makes a selection concerning the viewer application they use. As a service provider, the Digital and Population Data Services Agency is responsible for ensuring that the impact of choosing another viewer application is communicated in the Suomi.fi Messages in a sufficiently clear and understandable manner. The Digital and Population Data Services Agency and the service providers participating in the display of notifications of service could also, through communication and service design, ensure that an individual does not select a viewer application that they do not in fact use. From the perspective of legal protection risks, it is also essential that selecting a viewer other than the Suomi.fi Messages interface requires active steps by the individual and is based on their own voluntary choice. The messages would also always be stored in the background service of Suomi.fi Messages and would not be stored in other digital mail services except temporarily for the duration of a single session. In addition, the messages would always be readable in the Suomi.fi Messages user interface.

The potential risks to legal protection associated with the proposal are assessed to be minor, and they can be mitigated by the various measures described above. Accordingly, the provisions proposed in the Government proposal are not assessed to be in conflict with the guarantee of legal protection laid down in section 21 of the Constitution.

10.3 Delegation of public administration tasks to parties other than the authorities

According to section 124 of the Constitution, a public administration task may be delegated to a party other than a public authority only by an Act or by virtue of an Act, if this is necessary for the appropriate performance of the task and if basic rights and liberties, legal remedies and other requirements of good governance are not endangered. However, a task involving significant exercise of public powers can only be delegated to public authorities.

The provision emphasises that, as a main rule, the performance of public administration tasks must belong to authorities, and that such tasks may be assigned to parties other than public authorities only to a limited extent. For the purposes of determining the scope of application of the section, the decisive issue is what is meant by a public administration task. In the provision, a public administration task refers to a relatively broad range of administrative duties, including, for example, tasks related to the implementation of legislation and to decision-making concerning the rights, obligations and interests of private individuals and legal persons. By contrast, the exercise of legislative or judicial power cannot be regarded as a public administration task within the meaning of the provision. Section 124 of the Constitution covers not only the transfer of tasks that already belong to a public authority to parties other than public authorities, but also the conferral of new tasks falling within the sphere of administration on such parties (HE 1/1998 vp, p. 179/I).

The Constitutional Law Committee has not provided a precise definition of the concept of a public administration task, but instead, carries out a case-by-case assessment. In its opinion practice, the Committee has, when interpreting the concept of a public administration task, paid particular attention to the nature and characteristics of the task. Significance has also been attached to whether the task is provided for by law, as well as to whether the entity performing the task operates under the authority's powers of direction, guidance, or supervision. In addition, attention has been paid, inter alia, to the legal effects of the task and the decision-making associated with it (PeVL 53/2014 vp).

The Constitutional Law Committee has, for example, considered maritime search and rescue operations when viewed as a whole (PeVL 24/2001 vp, p. 4/I) and the overall entity formed by operative waste management tasks (PeVL 58/2010 vp, p. 4/II) to constitute public administration tasks. Despite their strong private-law characteristics, the granting of state export guarantees constitutes a public administration task (PeVL 2/2001 vp, p. 2/I). In the Committee's view, tasks relating to legal aid and guardianship, taking into account the manner in which they are organised, form a set of tasks displaying the characteristics of a public administration task even though they also emphasise considerations related to private interests and business activities. In this context, the Committee attached significance to the fact that the tasks in question constitute a statutory service task for which an authority bears organisational responsibility, and the performance of which could also be characterised as de facto administrative activity (PeVL 16/2016 vp, p. 2). Tasks assisting an authority have likewise been regarded as public administration tasks (see, e.g., PeVL 55/2010 vp, p. 2/I). By contrast, a public administration task has not been considered to be involved in impartial testing and certification based on technical expertise that did not affect an authority's competence to decide on the methods and personnel used in periodic inspections of equipment and structures (PeVL 4/2012 vp, p. 2/II), nor in certification activities whose nature had, in practice, diverged from the characteristics typically associated with public administration tasks (PeVL 16/2009 vp, pp. 2–3).

In addition, the provision of public services may be regarded as a public administration task (PeVM 9/2002 vp; HE 1/1998 vp). In such cases, the activity constitutes so-called de facto administrative activity. De facto administrative activity generally refers to actions related to the performance of an administration task that are not intended to produce direct legal effects. However, de facto administrative activity may also involve the exercise of public authority, such as issuing orders or prohibitions directed at private individuals without preceding procedural measure. The practice of the Constitutional Law Committee shows that, in certain situations, activities of a private-law nature may also be regarded as public administration tasks. A prerequisite is that such activities involve specific characteristics, such as being comparable to administrative decisions (PeVL 23/2013 vp; PeVL 57/2010 vp; PeVL 2/2001 vp).

As a starting point, the conferral of a public administration task on a party other than an authority must be provided for by law. In some cases, such as when public service tasks are transferred, the matter may, however, be regulated or decided on the basis of law. The question may concern, for example, authorisation granted by an authority or the transfer of a public administration task to a non-authority on a contractual basis in accordance with the law. Even in such cases, the competence authorising the transfer or conferral of the task must be based on law. The Constitutional Law Committee has considered that tasks assisting authorities may be transferred by contract to parties other than authorities (PeVL 11/2006 vp, p. 2).

In legislation concerning the conferral of a public administration task, it must be specified which tasks may be transferred to an external party and under what conditions. Matters such as requirements concerning the general conditions of the activity, supervision of the performance of public administration tasks, the competence and assessment of the reliability of the operator, and the criminal liability under official responsibility of those performing the tasks cannot be left to be determined solely by contract or an administrative decision.

As a rule, the further transfer of a public administration task that has been conferred on a private party, i.e. subdelegation, must be approached with caution. However, regulation allowing subdelegation was not considered problematic from the perspective of section 124 of the Constitution in a case where a private service provider could arrange the delivery of a passport to an applicant through another service provider. First, the task could be regarded as relatively technical in nature, and the arrangement required that the National Police Board had also separately approved the other service provider. In addition, the subcontractor was, by law, subject to the same quality requirements and other obligations as the original service provider. In such a case, organising the task through subcontracting could also be considered justified from the perspective of expediency. (PeVL 6/2013 vp, p. 4) The assignment of parking supervision tasks assisting authorities to private parties, based on a permit granted by the Regional State Administrative Agency, was considered expedient within the meaning of section 124 of the Constitution, since the police or municipal parking inspectors do not have sufficient resources to supervise parking on private areas, and there is deemed to be a need for activities assisting authorities (PeVL 23/2016 vp, p. 3).

Under section 124 of the Constitution, a public administration task may be assigned outside the authority apparatus only if it is necessary for the expedient performance of the task. The requirement of expediency is a legal condition, the fulfilment of which must be assessed on a case-by-case basis for each public administration task proposed to be assigned outside the authority structure. (see, e.g., PeVL 5/2014 vp, p. 3) In assessing expediency, attention must be paid not only to administrative efficiency and other internal administrative considerations but also, in particular, to the needs of private individuals and legal entities. The nature of the administrative task must also be taken into account in the assessment. Accordingly, the requirement of expediency may be more readily fulfilled for tasks related to the provision of services than, for example, when transferring decision-making authority concerning an individual’s fundamental rights.

The assignment of a public administration task to a party other than an authority must not jeopardise fundamental rights, legal protection, or other requirements of good administration. The provision also emphasises the importance of the training and expertise of persons performing public administration tasks, as well as the proper organisation of public supervision over these persons. The Constitutional Law Committee has emphasised that when administrative tasks are entrusted to a party other than an authority, the operation must, on a statutory basis, ensure compliance with the requirements of legal protection and good administration (PeVL 5/2014 vp, pp. 3–4). The requirements of legal protection and good administration primarily concern decision-making related to the public administration task. (HE 1/1998 vp, p. 179/II)

Ensuring the fulfilment of legal protection and good administration in the sense intended by section 124 of the Constitution generally requires that the general administrative laws are applied in the handling of matters and that those processing the matters act under official responsibility (PeVL 53/2014 vp, pp. 4–5). According to the Constitutional Law Committee, general administrative laws apply, based on their provisions regarding scope, the definition of

authorities, or the linguistic service obligations of private parties, also to parties outside the authority apparatus when they perform public administration tasks within the meaning of section 124 of the Constitution. For this reason, the Committee has considered that it is generally not constitutionally necessary to include a reference to general administrative laws in the legislation (see, e.g., PeVL 27/2014 vp, pp. 2–3; PeVL 42/2005 vp, p. 3/II). However, the Committee has noted that the application of broad criminal liability for official duties in the performance of a public administration task requires, in its view, an explicit provision at the legislative level (PeVL 15/2019 vp, p. 4).

The proposal includes regulation under which the Digital and Population Data Services Agency, acting as a service provider, could, by contract, assign the task of providing a viewer to another legal entity operating as a service provider. The primary service provider would be responsible, in technical terms, for integrating the other service provider's viewer into the messaging service.

Entering into a contract for the provision of a viewer would require that the service provider meets the requirements set out in section 8h. The tasks that could be transferred to a party other than an authority would be limited solely to an assisting task related to the technical implementation of electronic service of notifications, namely, making an electronic notification delivered to the messaging service's backend readable through a viewer in a user interface other than that provided by the primary service producer. The conferral of the public administration task to a party other than an authority would be based on a contract under law between the service producer and service provider. The contract would include an assessment of the service provider's ability to fulfil the prescribed requirements. In addition to the requirements set out in Article 28(3) of the General Data Protection Regulation, the law would specify minimum requirements for the content of the contract (section 8i).

The service producer would supervise the activities of the service providers (section 8l). Moreover, the Finnish Transport and Communications Agency (Traficom) would supervise the services provided by the service providers in accordance with existing regulation, particularly the provisions of the Cybersecurity Act. Other supervisory mechanisms provided by law, such as the Data Protection Ombudsman's oversight of compliance with provisions on the processing of personal data, would also apply to the activities of service providers. Regulation of private digital mail services from a supervisory perspective is described in section 2.5.2 of the proposal.

Section 8g(2) of the Act proposes that criminal liability should also apply to persons performing public administration tasks in the service of a service provider. The subsection would also contain an informative reference to the Act on Compensation for Damages. The display of electronic notifications through a viewer application does not constitute the exercise of public authority, but rather the performance of a task assisting in a public administration function. The provisions on official misconduct in the Criminal Code do not, therefore, apply directly on the basis of Chapter 40 of the Criminal Code (39/1889); rather, the extension of criminal liability for official duties to public administration tasks that do not involve the exercise of public authority must be established in special legislation. The Constitutional Law Committee has required that criminal liability for official duties also extend to public administration tasks in which public authority is not exercised (see, for example, PeVL 11/2006 vp; PeVL 3/2009 vp; PeVL 30/2012 vp).

Assigning, on a contractual basis, the task of displaying notifications via a viewer to a party other than an authority would, in part, ensure that clients of the administration have a genuine

opportunity to choose in which service they wish to receive electronic notifications from authorities. The ability to choose a service could increase the number of persons switching from notifications delivered by mail to electronic notifications, which would enhance the efficiency of notifications and administration while reducing emissions caused by notifications. Delivering electronic notifications also to private services, in accordance with the proposed regulation, would further support the development of the market for electronic message delivery and increase competition between companies. In addition, the public administration task assigned to service providers is an assisting task for the primary service provider and does not involve the exercise of public authority or decision-making. The proposed amendments would not change the basic principle that responsibility for fulfilling the duty of service under the Administrative Procedure Act would remain with the authorities. The conferral of a public administration task to a party other than an authority, as proposed, can thus be regarded as expedient in the sense required by section 124 of the Constitution.

The service provider performing the task would be required by law to be reliable and authorised to carry on business in Finland, and to have the technical, financial, professional, and operational capacity, as well as personnel, necessary to perform the task, as separately prescribed by law. The law would also provide for the criminal liability of the service provider's employees, and the service provider and its personnel would be required to comply with general administrative laws when performing the public administration task. In addition, the primary service provider would have statutory authority to supervise the performance of the assisting task by service providers and, if necessary, to carry out inspections for supervisory purposes. The conferral of this assisting public administration task to other service providers is therefore not considered to jeopardise fundamental rights, legal protection, or other requirements of good administration.

On the basis of the above considerations, the proposals may be dealt with under the ordinary legislative process.

Resolution

Based on the foregoing, the following Government Proposal is submitted to Parliament for approval:

1.

Act

Amendment to the Act on Central Government's Joint e-Service Support Services

In accordance with the decision of Parliament
a new paragraph 6, a new section 8f and a new chapter 2b are *added* to section 2 of the Act on Common Support Services for Electronic Transactions in Public Administration (571/2016) as follows:

Section 2

Definitions

For the purposes of this Act:

———————————————————————————————————————

6) *viewer* means a digital service that functions as the user interface of the messaging service.

Chapter 2 a

Messaging service

Section 8f

Provision of a viewer

The service producer shall provide a viewer to the users of the messaging service. The service producer is required to provide the viewer even if the task of providing it has also been assigned, under a contract concluded pursuant to section 8g, to another service provider or to other service providers.
The service producer shall open a view of the user's messaging service account in the service provider's viewer if the user has indicated that they use it as their viewer in the register referred to in section 11.

Chapter 2b

Service provider viewer application

Section 8g

Assignment of a task for the provision of a viewer to a service provider

The service producer may, by agreement, delegate the task of providing a viewer referred to in section 8f to another service provider.

An employee of the service provider shall be subject to the provisions on offences in office in the performance of the duties referred to in this Act. Liability for damages is regulated by the Tort Liability Act.

Section 8h

Requirements for the service provider

The service provider must be reliable and authorised to carry on business in Finland, and must have the technical, financial, professional, and operational capacity, as well as personnel, required to perform the task, as separately prescribed by law.

A service provider is not considered reliable if he or she is not currently operational, has been banned from engaging in commercial activities in the past five years, has been sentenced to prison in the past five years or issued a fine in the last three years for a serious infringement of an employment relationship, business, accounting or debt legislation or regulation, and if he or she has been sentenced to imprisonment for another serious crime which can be considered to affect his or her reliability or make it manifestly inappropriate for him or her to undertake the tasks referred to in this chapter. The assessment of the service provider's reliability evaluates a provider's leadership and the persons responsible for the tasks referred to in this chapter.

Section 8i

Agreement on the provision of viewers

In addition to what is provided in Article 28(3) of the General Data Protection Regulation, a contract concluded with the service provider must specify at least the following:

1) the service provider's tasks other than the processing of personal data;

2) the contract term, commencement of operations, and termination of the contract during its term;

3) the requirements applicable to the viewing application provided by the service provider;

4) procedures ensuring the sufficient professional competence of the personnel performing the tasks; and

5) the retention and archiving of documents related to the operations.

The contract must also set out the parties' statutory rights and obligations regarding supervision and reporting, as well as the consequences of deficiencies or omissions.

The service provider must provide the primary service provider with the necessary information to demonstrate compliance with the requirements set out in section 8 h before the contract is concluded.

The service producer may terminate or cancel the contract if the service provider no longer meets the general requirements or if the service provider substantially neglects the performance of the agreed contract or otherwise violates the contract or acts essentially or repeatedly unlawfully.

The service provider shall promptly notify the service provider of changes in its activities that may have a material effect on the performance of duties.

Section 8j

Obligation to cooperate

Service providers and the service producer shall cooperate to ensure the information security, interoperability and operation of the messaging service.

Section 8k

Disruption situations

If the messaging service, the information system used to provide it, or a viewing application connected to the messaging service causes harm to the operation or information security of the messaging service or the connected viewing application, the service producer or the service provider may disconnect their information system, service, or viewing application from a system maintained by another party. The service or information system that caused the harm must be reconnected without delay once it has been determined that no further harm will occur.

Section 8l

Supervision of a service provider performing a public administration task

The service producer supervises the performance of the public administration task referred to in section 8 g by the service providers. The service provider must provide the primary service provider with the information necessary to monitor compliance with this Act.

The service producer has the right to carry out audits at the premises of a service provider and, without prejudice to the confidentiality provisions, provide information on documents relating to the service. Audits shall not be carried out on premises of permanent residence. The inspection of premises is governed by Section 39 of the Administrative Procedure Act.

This Act enters into force on [day] [month] 20[year].

Helsinki xx xx 20xx

Prime Minister

First name Last name

Minister of ... First name Last name