



1a Controller	Name Financial Stability Authority (Business ID 2683902-3)
	Address Työpajankatu 13, PO Box 70, FI-00581 Helsinki
	Other contact information Tel. +358 295 253 500, rahoitusvakausvirasto@rvv.fi
1b Controller's representative	Name Tuija Taos, Director General
	Address Työpajankatu 13, PO Box 70, FI-00581 Helsinki
	Other contact information
2 Contact information of the data protection officer	Name Tanja Jyrkönen, Records Management Specialist
	Address Työpajankatu 13, PO Box 70, FI-00581 Helsinki
	Other contact information Tel. +358 295 253 513, tanja.jyrkonen(a)rvv.fi
3 Name of the personal data file system	Financial Stability Authority's Customer and Stakeholder Register, whose data subjects are depositors, employees of credit institutions, representatives of partners, service providers and other authorities as well as other persons who contact the Authority.
4 Purpose of processing personal data and legal basis for processing	<p>The main purpose of the personal data contained in the Customer and Stakeholder Register is to discharge the Financial Stability Authority's statutory official duties and to handle the Authority's administrative matters.</p> <p>The personal data contained in the Customer and Stakeholder Register are used for the following purposes:</p> <ul style="list-style-type: none">• crisis resolution planning and crisis management preparation• use of deposit guarantee scheme in a payout situation and preparation for this• providing information, particularly in deposit guarantee matters• management of administrative matters, such as procurement and registry activity• cooperation with authorities, such as cooperation bodies. <p>The personal data contained in the personal data file system are processed, as a rule, on the following legal grounds:</p> <ul style="list-style-type: none">• Processing of personal data is necessary to comply with the statutory obligation of the controller. The Financial Stability Authority acts as Finland's national resolution authority as well as the authority responsible for the deposit guarantee (Section 2 of the Act on the Financial Stability Authority). An authority must provide appropriate channels for service (Sections 7-8 of the Administrative Procedure Act) and keep a record of the matters it takes for consideration (Section 18 of the Act on the Openness of Government Activities, Sections 5-6 of the Decree on the Openness of Government Activities and on Good Practice in Information Management).• Processing of personal data is necessary to implement an agreement to which the

	<p>data subject is a party or a representative thereof.</p> <ul style="list-style-type: none"> • Processing of personal data is based on consent (visiting the Authority's website).
5 Data content of personal data file system and categories of personal data	<p>The personal data file system contains the following personal data on the data subjects:</p> <ul style="list-style-type: none"> • contact information and identification information such as first name, last name, email address, postal address, telephone number, personal identity code, citizen's account identifier, time stamps • other information provided by contact persons • website cookies. The website does not collect information about users, rather it collects information to improve accessibility, such as visitors' browser setting on whether use of cookies is permitted, and the start time and length of visits.
6 Data sources	<p>Data are mainly received from the data subjects themselves or an organisation representing them, from deposit banks or from the Suomi.fi Web Service.</p>
7 Profiling or automated decision-making	<p>None.</p>
8 Data recipients	<p>The recipients of personal data are the third parties, controllers and personal data processors to whom personal data contained in the personal data file system are transferred or disclosed.</p> <p>The public documents referred to in the Act on the Openness of Government Activities (621/1999) are made available upon request, in accordance with the requirements of Section 13 and Section 16 of the Act. Confidential data are made available and disclosed only 1) with the consent of the person concerned, 2) to the person concerned, 3) based on a legal right.</p> <p>Data may only be disclosed within the limits required and permitted by valid legislation or with the consent of the controller to the following entities:</p> <ul style="list-style-type: none"> • system suppliers and server maintainers, such as the Government ICT Centre Valtori • other public authorities.
9 Transfer of data outside the EU or the European Economic Area	<p>Not transferred.</p>
10 Personal data storage period	<p>The data collected for the personal data file system are stored only for as long as and to the extent necessary with respect to the original or compatible purposes for which the personal data have been collected.</p> <p>The personal data covered by this privacy statement are stored and erased as follows:</p> <ul style="list-style-type: none"> • email messages current year + 1 year • compilations of credit institutions' employees and other stakeholders' representatives: data are updated as necessary and at least once per year • other forms of storage and record entries: in accordance with the Financial Stability Authority's information management plan.

<p>11 Personal file data system's protection principles</p>	<p><i>Manual material</i> Manual material is processed by trained personnel in locked premises corresponding to the security level of the data concerned. All Financial Stability Authority personnel are subject to, at minimum, a basic background check.</p> <p><i>Digitally processed material</i> The data of the personal data file system is protected from unauthorised viewing, modification and destruction. Protection is based on user authorisation management, technical protection of databases and servers, physical protection of premises, access control, data traffic protection and data backups.</p> <p>The right to access and process data is granted on the basis of working tasks. Access to the system is based on personal identification credentials. Administrative controls are used to supervise the appropriateness of activity.</p>
<p>12 Right to inspect and rectify data</p>	<p><i>Right to receive information</i> Data subjects have the right to receive information about what data are collected, for what purposes the data are used, what the legal basis of the processing of data is, and to whom data is disclosed.</p> <p><i>Right to inspect data</i> Data subjects have the right to inspect what data concerning them have been saved in the personal data file system. An inspection request can be made to the controller's data protection officer (see Section 2 of this privacy statement).</p> <p><i>Right to rectify inaccurate data</i> Data subjects have the right to request that the controller rectifies without undue delay inaccurate personal data concerning them. If data subjects contest the accuracy of personal data, they can request that processing of the data is restricted for a period enabling the controller to verify the accuracy of the personal data.</p> <p>Taking into account the purposes of the processing, data subjects have the right to have incomplete personal data completed. Data subjects are primarily responsible themselves for notifying the controller of any changes in personal data or of any deficiencies in the data. The controller is responsible for the immediate correction of errors it notices itself.</p>
<p>13 Right to erasure of data</p>	<p>Data subjects have the right to have erased personal data concerning them without undue delay where one of the following grounds applies:</p> <ul style="list-style-type: none"> • the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. • the data subject withdraws the consent on which the processing is based, and where there is no other legal grounds for the processing. • the personal data have been unlawfully processed. • the personal data must be erased for compliance with a legal obligation in Union or Member State law. <p>Data do not need to be erased, despite a request to do so, where the controller has the right to process the data for the establishment, exercise or defence of legal claims.</p>
<p>14 Right to restriction of processing</p>	<p>Data subjects have the right to the restriction of processing where one of the following applies:</p> <ul style="list-style-type: none"> • the processing of the personal data is unlawful, in which case the controller is, in principle, obliged to erase the data, but the data subject opposes the erasure of the personal data and requests a restriction (discontinuation) of their use instead • the controller no longer needs the personal data for the purposes of the processing,

	<p>but they are required by the data subject for the establishment, exercise or defence of legal claims.</p> <p>Where a data subject has requested a restriction of processing, such personal data can (with the exception of storage) only be processed with the data subject's consent OR for the establishment, exercise or defence of legal claims OR for the protection of the rights of another natural or legal person OR for reasons of important public interest of the Union or of a Member State.</p>
<p>15 Right to withdraw consent and right to object</p>	<p>Data subjects have the right to withdraw their consent to processing at any time. The withdrawal of consent shall not affect the lawfulness of the processing carried out prior to the withdrawal of consent.</p> <p>There is no right to object where the processing of personal data is based on an agreement and is necessary for its implementation or where processing is necessary to fulfil a statutory obligation.</p> <p>Data subjects have the right to object to the processing of their personal data where the processing of the personal data is based on the controller's legitimate interest.</p>
<p>16 Right to data portability</p>	<p>Where processing is based on consent or an agreement:</p> <ul style="list-style-type: none"> • Data subjects have the right to receive the personal data concerning them that they have provided to a controller in a structured, commonly used and machine-readable format and have the right to transfer those data to another controller. • Data subjects have the right to have the data transferred directly to another controller where this is technically feasible and is not unreasonable for the controller. Exercising this right must not adversely affect the rights and freedoms of others.
<p>17 Exercising of rights</p>	<p>Requests relating to a data subject's rights can be addressed to the controller's data protection officer (Section 2 of this privacy statement).</p>
<p>18 Right to appeal to supervisory authority</p>	<p>Data subjects have the right to appeal to the supervisory authority if they consider that the processing of personal data concerning them violates data protection regulations. The national supervisory authority in Finland is the Office of the Data Protection Ombudsman.</p>