

1. Name of the register	Customer organisations' reporting users ("Asiakasorganisaatioiden raportointikäyttäjät")
2. Data controller	Fimlab Laboratoriot Oy PO Box 66 33013 Fimlab
3. Contact person in register-related matters and Data Protection Officer appointed by the organisation	Merja Maijala Data Protection Officer tel.: +358 3 311 75259 email: tietosuoja@fimlab.fi
4. Purpose of and legal basis for processing personal data	<p>The basis for the processing of personal data stored in the register for customer organisations' reporting users is, depending on the report in question, either the delivery of an agreement concluded with the customer, a legitimate interest concerning the management of the customer relationship, compliance with the data controller's statutory obligations or the customer's explicit consent.</p> <p>The data controller uses the register to manage users reporting customer organisation information and to identify users.</p>
5. Data content of the register	<p>The following customer data may be collected of the data subject:</p> <ul style="list-style-type: none"> • Name • Social security number • Email address • Number of the ID card for regulated social welfare and healthcare professionals • Employer and role on report • User ID validity
6. Regular sources of data	<p>Regular sources of data consist of data provided by the customer themselves or a representative of the organisation.</p> <p>For purposes of screening reporting, data is also obtained from the Digital and Population Data Services Agency when the customer uses the Suomi.fi identification service.</p>
7. Recipients of data	The data in the register is not disclosed outside the organisation.
8. Transfer of data outside the EU or EEA	Personal data in the register is not transferred outside the EU or EEA.

9. Retention period	<p>The data collected in the register is stored only for as long as and to the extent necessary for the original or appropriate purposes for which the personal data was collected. Personal data referred to in this privacy policy is stored for as long as the data controller uses it for the purposes specified in section 4. Personal data stored in the register is erased when the legal basis for its processing ceases to apply.</p>
10. Principles of protection	<p>Appropriate technical and organisational measures have been taken to ensure the information security of the register and the confidentiality, integrity and accessibility of the personal data collected.</p> <p>Manual material is stored in an archive and in laboratory facilities controlled with access control and/or a locking system. Electronic material is protected securely so that it can only be accessed from the organisation's intranet. The access rights to the organisation's information systems and files are based on personal access rights, the use of which is controlled.</p> <p>Databases are maintained by the IT service provider. Fimlab Laboratoriot Oy's guidelines on data security and data privacy are observed in the storage of data.</p>
11. Right to access and rectify data (Article 15 and 16)	<p>The data subject shall have the right to know which of their personal data have been stored in the register. The request to access data or have data rectified is submitted by sending a written request to the Data Protection Officer (tietosuoja@fimlab.fi). After submitting their request, the data subject must identify themselves at the data controller's service point in order to verify the identity of the applicant in accordance with the data controller's instructions or, alternatively, the data controller may require the data subject to provide any necessary additional information to verify the applicant's identity due to the delicacy of the data requested.</p>
12. Right to erasure (Article 17)	<p>The data subject shall have the right to obtain from the controller the erasure of personal data concerning them without undue delay if</p> <ul style="list-style-type: none"> • the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed; • the data subject withdraws their consent on which the processing is based, and where there is no other legal ground for the processing; • the personal data has been unlawfully processed; or • the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject. <p>The request to have data erased is submitted by sending a written request to the Data Protection Officer (tietosuoja@fimlab.fi). After submitting their request,</p>

	<p>the data subject must identify themselves at the data controller's service point in order to verify the identity of the applicant in accordance with the data controller's instructions or, alternatively, the data controller may require the data subject to provide any necessary additional information to verify the applicant's identity due to the delicacy of the data requested.</p> <p>Despite the request to have data erased, the data controller may be entitled to continue the processing personal data stored in the register based on a legal reason under Article 17(3) of the General Data Protection Regulation.</p>
<p>13. Right to restriction of processing (Article 18)</p>	<p>The data subject shall have the right to obtain from the controller restriction of processing if</p> <ul style="list-style-type: none"> • the accuracy of the personal data is contested by the data subject; • the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use instead; • the controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims. <p>The request to restrict the processing of data is submitted by sending a written request to the Data Protection Officer (tietosuoja@fimlab.fi). After submitting their request, the data subject must identify themselves at the data controller's service point in order to verify the identity of the applicant in accordance with the data controller's instructions or, alternatively, the data controller may require the data subject to provide any necessary additional information to verify the applicant's identity due to the delicacy of the data requested.</p>
<p>14. Right to withdraw consent (Article 7)</p>	<p>The data subject shall have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p>
<p>15. Right to data portability (Article 20)</p>	<p>The data subject shall have the right to receive the personal data concerning them, which they have provided to the data controller in a structured, commonly used and machine-readable format, and have the right to transmit this data to another controller, if possible. This right shall apply to personal data that has been processed automatically and based on consent or for the purpose of implementing an agreement. After submitting their request, the data subject must identify themselves at the data controller's service point in order to verify the identity of the applicant in accordance with the data controller's instructions or, alternatively, the data controller may require the data subject to provide any necessary additional information to verify the applicant's identity due to the delicacy of the data requested.</p>

<p>16. Right to lodge a complaint with a supervisory authority (Article 77)</p>	<p>The data subject shall have the right to lodge a complaint with a supervisory authority if the data subject considers that the processing of personal data relating to them infringes the General Data Protection Regulation.</p>
--	--