

1. Name of the register	Fimlab's customer register (<i>Fimlabin asiakasrekisteri</i>)
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 customer register is, depending on the sub-register or on a case-by-case basis, 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 logical register for the following purposes:</p> <ul style="list-style-type: none"> • Maintenance of customer relationships, information of customers of Fimlab's operations and reminding customers of the data controller's services • Processing of customer feedback and surveying customer satisfaction • Marketing, direct marketing, opinion or market research, advertising, and targeting of marketing, services and communications at customers • Profiling and targeting of marketing measures and customer communications as well as provision of more individualised content in our digital services • Guest management • Fimlab Forum's communications • Compilation of statistics, reporting, planning and monitoring, invoicing and debt collection and other tasks necessary for the enforcement of the rights and obligations of the data controller • Development and production of the data controller's own organisation and its services, processes and products • Training of customer service staff, development of the quality of customer service and ensuring of legal protection • The data controller's own scientific research • Collection of personal data needed for remote testing and mailing of sampling sets • Sending of laboratory examination results to the customer by SMS • Relaying of laboratory examination results to the customer <p>The customer can choose which messages they will receive, and</p>

	<p>they may refuse marketing targeted at them.</p> <p>The logical customer register contains the following consent-based sub-registers with their respective privacy policies:</p> <ul style="list-style-type: none"> • Fimlab Forum's customer register • Fimlab's marketing register • Mobile register • The logistics of remote testing for STDs • Fimlab's guest management register • Customer register of the Fimlab mobile application
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 • Public contact details • Age • Photo (guest management) • Profiling information • Information on the provision of targeted measures and their results • Occupation/title • Customer's choice of marketing communications to be received • Start and end of the customer relationship and the related agreements and consents • Employer information and the related contact details • Contact history • Information on interests given by the data subject • Other information necessary for contacting the customer or targeted marketing • Consents to marketing and marketing bans • Marketing history • Customer's choice of marketing communications to be received • Revision history of the aforementioned information • Complaints filed by the customer • Customer relationship management history • Fimlab products and services used • Classification of the person participating in remote testing • Telephone number for SMS results
6. Regular sources of data	<p>Regular sources of data consist of data provided by the customer themselves or a representative of the organisation and generated in connection with customer service and the services used.</p> <p>Personal data is collected in connection with newsletter subscription and registration for various services, marketing campaigns and competitions through cookies or by other similar means,</p>

	<p>with the data subject's consent. Data may be collected and updated from Fimlab's information systems, when the data subject registers for services and uses services, and from social media related to the data collector's operations.</p> <p>The register on the logistics of remote testing for STDs also obtains data from the Digital and Population Data Services Agency when the customer uses the Suomi.fi identification service.</p>
7. Recipients of data	The data stored in the register is not disclosed to third parties. Data may be disclosed to authorities based on individualised requests.
8. Transfer of data outside the EU or EEA	In principle, personal data in the register is not transferred outside the EU or EEA. An exception to this rule is Google Analytics, which is used to process cookies on Fimlab's website in the USA. Data is transferred to the USA according to the Data Privacy Framework.
9. Retention period	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.
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)	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,

	<p>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>12. Right to erasure (Article 17)</p>	<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, 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</p>

	based on consent before its withdrawal.
15. Right to data portability (Article 20)	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.
16. Right to lodge a complaint with a supervisory authority (Article 77)	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.