

1. Name of the register	Laboratory register (<i>Laboratoriorekisteri</i>)
2. Data controller	Fimlab Laboratoriot Oy PO Box 66 FI-33101 Tampere
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 laboratory register is, on a case-by-case basis or depending on the sub-register, either the delivery of an agreement concluded with the customer, compliance with the data controller's statutory obligations, the customer's consent, the performance of duties to pursue public interest, or the pursuit of the data controller's legitimate interests.</p> <p>Fimlab Laboratoriot Oy uses the register for the following purposes:</p> <ul style="list-style-type: none"> • Diagnostics, laboratory tests and results and their storage, and enabling of follow-up tests • Hospital blood banks • Treatment of the patient • Compilation of statistics and reporting on laboratory operations, invoicing and planning of laboratory operations • Validation of the operation of systems and equipment supporting laboratory operations, if necessary • Collection of statutory information and its transfer to national registers • Scientific research • Management of equipment used in the Diabetes Self-Monitoring Service • Monitoring and development of the organisation's operations and processes as well as quality control • Duties based on the data controller's rights and obligations • Execution of laws and regulations on private health care activities • Internal training of healthcare personnel and students and using anonymised register data to produce training material <p>The logical laboratory register contains the following sub-registers with their respective privacy policies:</p> <ul style="list-style-type: none"> • Assisted reproduction laboratory patients • Flow cytometer archive

	<ul style="list-style-type: none"> • Pathology images • Patient negotiations • Stored genetics samples • Stem cell laboratory register • Coagulation disorder register • Microbiology sequencing core register <p>Fimlab acts as the data controller for various client organisations, with regard to laboratory operations, pursuant to its agreements with these organisations. Fimlab also has private patients (who pay for their tests themselves) as customers.</p>
5. Data content of the register	<p>The following personal data may be collected of the data subject:</p> <ul style="list-style-type: none"> • Patient's name and social security number • Public contact details • Health information • Laboratory test information, e.g. time of processing, result, statement • Referral information, e.g. requesting unit, desired sampling time, necessary preliminary information, treatment unit • Sample number • Sampling and sample processing information, e.g. time, location, sampler • Blood products administered and the time of administration • Information on patient communications • Quality control • Sample materials examined or photos thereof • Family information related to haemostasis tests <p>A detailed list of the personal data stored in the register may be requested from the Data Protection Officer (tietosuoja@fimlab.fi).</p>
6. Regular sources of data	<p>The data stored in the personal data register is obtained from the referral from the sending health care treatment unit and directly from the patient or their representative, the company staff (data generated through own activities), laboratory information systems, laboratory equipment, the company's subcontractors and decentralised sampling operators and production systems, client organisations' patient information systems and personal data registers, and client organisation personnel requesting information and participating in consultations.</p>
7. Recipients of data	<p>The following types of data in the laboratory register may be disclosed:</p> <ul style="list-style-type: none"> • Data may be disclosed to the EBMT register in the Netherlands with the patient's or their legal representative's or guardian's written consent • With the patient's explicit consent, patient data in Fimlab's registers may be disclosed to e.g. a private physician

	<ul style="list-style-type: none"> • At the request of certain client organisations, laboratory data is transferred to the Patient Data Repository of the Kanta services • Laboratory test requests to subcontractors are sent to subcontractors' production data systems according to agreement • The client organisation's physicians have a technical viewing access to another organisation's laboratory test information with the patient's consent • Scientific research groups may be disclosed data either with the data subject's explicit consent, the data controller's written permission or the Finnish Institute for Health and Welfare's written permission • Necessary statutory disclosure of data to authorities, e.g. communicable disease data to the Finnish Institute for Health and Welfare
8. Transfer of data outside the EU or EEA	<p>In principle, personal data in the register is not transferred outside the EU or EEA.</p> <p>In order to ensure the technical maintenance of the analytics equipment of certain laboratories and compliance with obligations concerning the data controller, the equipment/system supplier has access to personal data stored in the equipment/system in question from outside the EU or EEA. Individual, more rare tests may also be sent to a subcontracting laboratory outside the EU or EEA for analysis. In this case, the transfer of data to third countries is secured by a country-specific EU decision on the adequacy of data protection, the data subject's explicit consent or appropriate protective measures.</p>
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 stored in the register is erased when the legal basis for their 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>

	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.
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 data has been collected from a minor; • 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>
13. Right to restriction of processing (Article 18)	<p>Insofar as mandatory legislation does not prevent or restrict the restriction of processing of data, 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 they are required by the data subject for

	<p>the establishment, exercise or defence of legal claims.</p> <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>
14. Right to withdraw consent (Article 7)	<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>
15. Right to data portability (Article 20)	<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>
16. Right to lodge a complaint with a supervisory authority (Article 77)	<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>