This document is meant to answer some of the most common questions about the other documents you have received. If there are any discrepancies between this document and any other document you have received, the information presented in the other documents shall prevail over the information presented in this documents. In any case, this document is not part of any contract between you and LaaS Company, but only provided to you for convenience purposes.

You must, of course, carefully read and accept all of the documents before accessing and using the service.

What documents did I receive and why?

LaaS License and service agreement

This is the main contract between you and LaaS Company.

Terms of Use

Before using or accessing the service, every user needs to accept our Terms of Use.

Handover of customer data

This document describes some special handling of your Users' data. Most importantly it specifies that we do not give you the Users' individual answers to surveys such as the Employee experience survey. We do this to maintain the Users' trust and to allow them to answer truthfully.

Data Processing Agreement (DPA)

This document sets out the conditions under which we may process your personal data on your behalf. It is required because you are the **data controller** and LaaS company acts as the **data processor** as per EU General Data Protection Regulation (GDPR). Executing a Data Processing Agreement is a mandatory requirement stipulated by the GDPR.

Common questions

Transfer of data outside the EU

This clause is in our documentation for our future development and possible changes to our processing infrastructure. Currently, all customer data storage and processing is carried out inside the EU.

However, our deployment is in Google Cloud. For these services, data transfer would be carried out in accordance with the GDPR by using the Google Workspace EU Model Contract Clauses.

If this is not acceptable to you, we offer an option to opt out of all data processing outside the EU, with the understanding that some future functionality may not be available to you. We can add this restriction to the DPA.

HR LAAS LICENSE AND SERVICE AGREEMENT

1 Application and other contractual terms

This Agreement is applied to Leadership-as-a-Service (LaaS) services (hereinafter "**Service**") provided by Leadership as a Service Company Oy (hereinafter "**Supplier**") to its Customers over data network.

In this Agreement Customer shall have the meaning of a legal entity (such as company or organization) which subscribes the Service and is duly incorporated in a country located in Europe. The Service is not available for entities located outside Europe.

By using or accessing the Service, the Customer agrees to be bound by this Agreement. If you are entering into this Agreement on behalf of a company, organisation or another legal entity, you are agreeing to the terms of this Agreement for such entity and represent that You have the authority to bind such entity to this Agreement. If you do not have such authority, or you do not agree with this Agreement, you must not accept this Agreement and you may not access nor use the Service.

The content of the Service is determined in the service description and the prices for the Service are presented in Supplier's then valid price list.

In case of any discrepancies between contractual documents, the following order of precedence shall be applied:

1. This Agreement
2. Terms of Use
3. Handover of Customer data
4. Data Processing Agreement
5. Service description
6. Price list

If the Service contains any software or software components manufactured or provided by third parties, the Customer agrees to accept and comply with such license and service terms of such third parties in addition to this Agreement. Unless otherwise agreed in writing, the terms and conditions primarily applied to open source software and standard software are the respective terms and conditions concerning such software. Such software are described in the service description.

2 Service and Use of the Service

Supplier shall provide the Service through network. The software is installed in a server operated by Supplier, its subcontractor or a third party. The Service is used via Internet or other data connection.

Supplier shall have the right to provide the Service in a way it sees most suitable as well as to use licensors and subcontractors for the provision of the Service. Supplier shall have the right to change and amend working practices, equipment, data connections, software used for the provision of the Service as well as other system parts of, or related to, the Service and to change its licensors and subcontractors.

Subject to the terms of this Agreement, Supplier hereby grants to Customer a limited, non-exclusive, non-transferable, revocable right of use (license) to the Service in accordance with this Agreement for the duration of the Agreement.

In order to use and access the Service, the Customer must give adequate and verifiable information to Supplier upon accessing to the Service. The Customer is responsible for accuracy of the information provided to Supplier. The Customer is responsible for any use of the Service occurring under its access rights or supervision.

The Service does not include data connections or capacity, or other equipment, software or security or protection systems for using the Service (hereinafter "**Prerequisites**"), which the Customer shall separately acquire in its own expense. The Customer is responsible for such Prerequisites, including configurations and settings, and effects thereof to the Service.

Use of the Service may require installation of interface or software to the Customer's equipment. Such interface or software enables use of the Services on the Customer's equipment.

The Customer may use the Service for its own internal business use. The Customer shall not have the right to resell or distribute the Service, or to use it part-time with others or as a basis of service center.

The Customer must comply with all applicable laws and regulations when using the Service.

The Customer must ensure that every user complies with the Terms of Use.

The Customer is responsible for any and all direct and indirect expenses that may result from the use of the Service.

Use of the Service occurs on the Customer's risk and liability. Supplier is not responsible for any information, material, products or other services provided by third parties through the Service.

The Service, software, platform and use thereof are provided on an "as is" basis. Use of the Service is intended to be provided 24/7, excluding temporary service breaks, which may result from maintenance, update or correction activities or activities performed in order to ensure or restore availability, performance, recoverability, information security or management of the Service or from other similar breaks. Supplier shall have no liability for such breaks. Supplier shall inform the Customer of such breaks if it is reasonably possible.

Supplier does not warrant that:

a) the Service fulfills the Customer's demand and needs;
b) the Service is uninterrupted, timely, and free from defects; or
c) the Service may be used in so-called high risk activities, which contain the risk of death, personal injury or damage to property or environment, and Supplier assumes no liability for the use of the Service in such high risk activities.

3 Versions and Changes to the Service

Supplier shall have the right to amend functionalities of the Service, provided that this does not cause material adverse effect on use of the Service.

Supplier aims to notify, when it is reasonably possible, the Customer of any substantial changes and breaks to the Service beforehand through the Service or by other suitable manner.

4 Misuse of the Service

The Customer must use the Service in a way that does not cause interference to the Service or to other users. The Customer is liable for content and material delivered to other users and third parties through the Service as well as for content and material delivered to servers operated by Supplier or a third party. The Customer is also liable for ensuring that the equipment and contents and material the Customer is responsible for and delivered by the Customer through the Service do not cause interference to the Service and its availability, communication network, or infringe legislation or authoritative orders and recommendations and intellectual property rights of third parties.

The Customer shall not (i) sell, resell or lease the Service, unless explicitly otherwise agreed with Supplier; (ii) use the Service in order to store or transfer infringing or illegal content; (iii) cause interference or detriment to the Service; (iv) try to obtain unauthorized access to the Service or related systems or networks; (v) reverse engineer the Service and its API; or (vi) use the Service or use its API in order to develop a competing product or service, nor copy any feature, functionality, graphics or design of the Service for competing purposes.

If Supplier, governmental authority or a third party claims that such content and material have been delivered to other users or servers operated by Supplier or a third party through the Service, then Supplier shall have the right to delete such infringing content or material and prevent use of the Service by available means. The Customer is responsible for loss, alteration or delay of contents and material transmitted by abusing the Service, as well as for claims and disputes and possible damages caused by such content and material.

5 Suspension of the Service

Supplier shall have the right, without any liability, to suspend the provision or use of the Service partly or in full for the following reasons:

- Suspension is necessary for repair, update or maintenance of the Service or part thereof or to otherwise ensure usability or functioning of the Service. Supplier shall inform the Customer of such suspension beforehand if it is reasonably possible;
- Use of the Service or Prerequisites, for which the Customer is responsible for, have caused or is causing interference or disruption to the Service or other users of the Service;
- Default of payment obligation based on the Agreement despite demand for payment;
- Supplier has a legitimate reason to suspect that the Service has been used for illegal or unethical activities;
- The Customer is subject to liquidation or bankruptcy proceedings or otherwise declared insolvent; or
- The Customer or its users do not comply with this Agreement or the Terms of Use.

6 Payments

The Customer shall pay to Supplier for use of the Service as set out in Supplier's then valid price list. Prices are exclusive of Value Added Tax (VAT 0 %) and then valid VAT shall be added to the prices upon invoicing. The Customer is obliged to

pay the VAT and other possible fees under public law.

Supplier shall invoice the charges in accordance with invoicing periods determined by Supplier. Payment term is set out in Supplier's then valid price list. Interest on delayed payments is in accordance with the Finnish Interest Act. Claims concerning invoice shall be made and undisputed amounts shall be paid on the due date of the invoice at the latest. A demand for late payment shall be charged in accordance with the price list.

The Customer shall be liable for payments even if the Service is or has been used by others than the Customer itself under Customer's access rights.

7 Data Security and Data Protection

The Customer is fully responsible for complying with its respective obligations and responsibilities under the applicable data protection and other legislation.

Supplier assumes no responsibility for information security of public internet network or possible interference contained therein or other detrimental factors to the Service outside the scope of Supplier's control nor possible damages caused by them.

Supplier shall have the right to take action to prevent personal data breach and to remove interference related to data security. These actions include, without limitation, prevention of transfer and receipt of messages or removing malicious software that endanger data security from messages. Supplier shall scale such actions based on the severity of such interference and shall cease such actions immediately after grounds from them have ceased.

The Customer commits to take care of and is responsible for adequate protection of its data networks, equipment, software, as well as other Prerequisites. This includes, inter alia, the obligation to use and maintain adequate virus prevention programs and other protective measures.

Supplier has the right to store and use anonymous information both disclosed by the Customer and collected by the Service in order to develop the Service and analytics and for statistical purposes, on condition that anonymous information can never be attributed (directly or indirectly) to a natural person.

8 Backup

Supplier shall take backup copies of the Customer's material in the Service and store the backups in an appropriate manner in accordance with Supplier's practices. For other parts, the Customer shall be responsible for taking backup copies of its material.

In case the Customer's material is destructed, lost, altered or damaged due to the Customer's use of the Service or the Customer has otherwise destroyed, lost, altered or damaged the Customer's material due to its own action, Supplier is entitled to charge for returning such material in accordance with its then valid price list.

9 Intellectual Property Rights

Supplier and/or its licensors own intellectual property rights to the Service and related software, platform, material, and to work related to performance of the Service and to material developed based on such work. Intellectual property rights shall not be transferred to the Customer for any part whatsoever.

Customer acknowledges that the Service may interoperate with, or use of the Service may require, software provided by third parties. For the purpose of providing the Service, Supplier shall have the right to use, amend, store as well as to disclose Customer's material and data (including personal data) to such third parties.

The Customer shall have right of use to the Service and related documents and material for the duration of the Agreement to the extent it is necessary for exploitation of the Service in its own internal activities in accordance with the Agreement.

The Customer owns intellectual property rights to its own proprietary material and data.

The Customer warrants that use of any material delivered by it to Supplier for the provision of the Service does not infringe intellectual property rights of third parties. The Customer is obliged to obtain any necessary rights and to compensate Supplier for any damages caused by infringement of intellectual property rights.

The Customer shall not remove, amend or cover copyright, trademark, and other intellectual property rights notices contained in the Service.

10 Access Rights

Supplier shall deliver access rights, passwords and other possible technical addresses and access rights to the Customer for use of the

Service for the duration of the Agreement and only for the agreed purpose of use. After the expiration or termination of the Agreement the Customer's right of use to the access rights shall expire, unless otherwise agreed or provided in mandatory legislation.

Supplier shall have the right to make amendments to the access rights if required or necessitated by orders of governmental authorities or by service, maintenance or other technical reasons. When possible, Supplier shall inform the Customer of such changes in a reasonable time before such change.

The Customer is responsible to inform Supplier immediately of any changes to its contact information.

The Customer must store the access rights, passwords and similar information carefully and in a manner that they are not exposed to third parties. The Customer shall inform Supplier without any delay if the access rights have been exposed or allegedly exposed to third parties, or if the Services has been otherwise used without authorization. The Customer is liable for any use of the Service occurring under its access rights.

11 Force Majeure

Neither party shall be liable for delay or damage caused by an impediment beyond the party's control and which the party could not have reasonably taken into account at the time of conclusion of the Agreement and whose consequences the party could not have reasonably have avoided or overcome. Such force majeure events shall include, if not proven otherwise, inter alia, new legislation or order by a governmental authority obligating a party, war or insurrection, earthquake, flood or other similar natural catastrophe, interruptions in general traffic, data communication or supply electricity, import or export embargo, strike, lockout, boycott or other similar industrial action. A strike, lockout, boycott and other similar industrial action shall also be considered, if not proven otherwise, a force majeure event when the party concerned is the target of or a party to such an action.

A force majeure event suffered by subcontractor, supplier or licensor of Supplier shall also be considered a force majeure event suffered by Supplier.

Each party shall without delay inform the other party in writing of a force majeure event and the cessation of the force majeure event.

12 Liability for Damages and Limitation of Liability

Supplier shall not be liable for any indirect damages suffered by the Customer which have been caused by use of the Service or which relate to the use thereof. In any event, Supplier's total aggregate liability towards the Customer for direct damages shall be limited to amounts paid by the Customer for the Service for a period of six (6) months preceding the occurrence of the damage.

Supplier shall not be liable for the destruction, loss, alteration or delay of the Customer's information and data files, or for any damages and expenses incurred as a result, including expenses involved in the reconstitution of information and data files.

Supplier shall not be liable for, and it shall not have obligation to compensate for, inter alia, expenses, costs, and damages caused by the following reasons and events for which the Customer is liable for and which are outside of Supplier's control:

- Prerequisites which are in responsibility of the Customer, such as data connections and capacity, equipment, software and data security;
- content and material produced by the Customer or a third party which the Customer has stored in the Service or by using the Service;
- unauthorized use of the Service or software or attempt thereof;
- costs, charges and expenses defined in right of use, license, or service terms and conditions of services and software manufactured or produced by third parties; or
- data security of public internet network or other interference or interruption to data connection network outside control of Supplier.

The Customer is responsible for any unauthorized installation, use, copying, reproduction, or sharing of the Service, software, platform or parts thereof and is liable for possible costs, expenses and damages incurred to Supplier as a result thereof.

The limitation of liability stated in this Section 12 shall not be applied in case of a party's willful misconduct or gross negligence. Furthermore, limitation of liability shall not be applied to damage which the Customer has caused by any copying, transfer or use of the Service or the deliverables contrary to this Agreement or in violation of applicable legislation.

13 Validity and Termination

Agreement commences when Customer has electronically accepted to comply with this Agreement and Supplier has granted access rights to the Service.

Unless otherwise agreed in writing, the Agreement is in force until further notice, and each party shall have the right to terminate the Agreement by issuing a written notice to the other party at least one (1) month prior to the commencement of the subsequent invoicing period (as determined in the price list).

The Customer takes care of and ensures that the Customer copies or prints information it has stored to the Service as it desires and needs before termination of the Agreement. After the Agreement period Supplier shall have the right to delete information stored by the Customer into the Service and thereafter Supplier shall have no obligation to restore such information to the Customer.

If the Customer terminates the Agreement, there shall be no refund of advance payments. Charges related to implementation of the Service shall not be refunded.

14 Other Terms

Amendments to contractual terms: Supplier shall always have the right to amend this Agreement and its appendices. The amendments shall become effective on the date notified by Supplier.

Customer's invoicing and contact information: Supplier shall send invoices, notifications and other messages to address notified by the Customer in writing. The Customer shall be obliged to notify Supplier of any changes to its contact information without undue delay.

Assignment of the Agreement: The Customer shall have no right to assign the Agreement or any part thereof without Supplier's written consent. Supplier shall have the right to assign the Agreement to a company belonging to the same group of companies as Supplier, or in connection with the transfer of business operations. Furthermore, Supplier shall have the right to transfer its receivables under the Agreement to a third party.

Applicable Law and Dispute Resolution: The Agreement shall be governed by the laws of Finland (excluding its choice of law provisions). Any dispute shall be primarily solved by mutual negotiation between the parties. If the parties are unable to solve the dispute by negotiation, disputes shall be solved in the district court of Supplier's place of domicile. Alternatively the parties may agree on solving the dispute by arbitration proceedings. Nonetheless, Supplier shall always have the right to bring claims for non-payment of monetary charges to be resolved in the district court of Supplier's place of domicile.

LaaS Terms of Use

Background and Purpose

These Terms of Use ("**Terms**") govern your use of the LaaS service ("**Service**") provided by Leadership as a Service Company Oy ("**Company**"). Company and your organization ("**Your Organization**") have entered into a license agreement concerning the Service ("**Agreement**"), pursuant to which Agreement you are granted access rights to the Service. The Agreement stipulates the legal relationship between Company and Your Organization concerning the Service (such as license term, payments, warranties, liabilities, and limitations of liability). Your use of the Service is always subject to the Agreement and these Terms.

PLEASE READ CAREFULLY THE FOLLOWING TERMS. BY ACCESSING THE SERVICE OR BY USING IT IN ANY MANNER, YOU INDICATE YOUR ACCEPTANCE OF THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS OF USE, YOU MAY NOT ACCESS OR USE THE SERVICE.

PLEASE READ OUR PRIVACY POLICY (https://tuki.laas.fi/wp-content/uploads/PrivacyNotice.pdf) BEFORE USING THE SERVICE.

License Grant

Subject to these Terms and the Agreement between Your Organization and the Company, the Company grants you a limited, non-exclusive, revocable, non-transferable, revocable right to use the Service as agreed between Your Organization and the Company in the Agreement.

User Account

You need to register a user account to use the Service. You must give adequate and verifiable information to the Company upon accessing the Service. You must store the access rights, passwords and similar information carefully and in a manner that they are not exposed to third parties. You will inform the Company without any delay if the access rights have been exposed or allegedly exposed to third parties, or if the Service has been otherwise used without authorization.

Acceptable Use of the Service

When using the Service, you will abide by the applicable laws, rules and regulations, and by any usage guidelines Company may convey to you from time to time.

You must use the Service in a way that does not cause interference to the Service or other users.

You may not access or use the Service for any illegal or abusive purposes, or to develop or create a similar or competitive product or service to the Service.

You will not:

(a) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share or otherwise commercially exploit or make the Service available to any third party;
(b) modify, adapt, alter or hack the Service or otherwise attempt to gain unauthorized access to the Service or related systems and networks;
(c) use the Service in any unlawful or unethical manner, including, but not limited to, violation of any person's right to privacy;
(d) use the Service to store or transmit material or other content that infringes intellectual property right of any person or entity;
(e) attempt to decipher, decompile, reverse engineer or otherwise discover the source code of any software making up the Service;
(f) use the Service or use its API in order to develop a competing product or service, and not copy any feature, functionality, graphics or design of the Service for competing purposes; or
(g) attempt to use or use the Service in violation of these Terms.

Company may temporarily or permanently deny, limit, suspend, or terminate your user account, prohibit you from accessing the Service, remove your User Content and take technical and legal measures to keep you off the Service without refund, if Company determines in its sole discretion that you: (i) abused your rights to

use the Service; (ii) breached the Terms; (iii) violated any applicable law, rule, or regulation; and/or (iv) performed any act or omission which is harmful or likely to be harmful to us, or any other third party, including other users or providers of the Service.

User Content

You may upload content such as Service descriptions, images and attachments to the Service ("**User Content**").

Company may, but is under no duty to, review all uploaded Content and remove or block access to such Content, as more fully described below.

Any use of your account is subject to your sole responsibility. You will not access and use the Service (including as to upload or transmit any Content) for any illegal, harmful, fraudulent, offensive purpose or to transmit, store, display, distribute or otherwise make available Content that is infringing upon any third party rights, illegal, harmful, supportive of or promoting violence or violent extremism, advocating hatred against any person or group of people based on their race, religion, ethnicity, sex, gender identity, sexual orientation, disability, or impairment, indecent, obscene, defamatory, libelous, harassing, threatening, fraudulent, offensive, enables online gambling or inconsistent with the generally accepted practices of the Internet community, including without limitation promoting or facilitating pornography, offering or disseminating fraudulent goods, services, schemes, or promotions, spamming, make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming, and use of content or technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms or time bombs.

Privacy and Data Protection

Company processes your personal data in connection with the Service as described in Company's Privacy Policy, available at: https://tuki.laas.fi/wp-content/uploads/PrivacyNotice.pdf

Intellectual Property

Except for User Content, all rights, title and interest in and to the Service, including any intellectual property rights, whether registered or not, and any goodwill associated therewith, are owned by, or licensed to Company. Unless as expressly provided herein, these Terms do not grant you any rights to patents, copyrights, trademarks (whether registered or unregistered), trade names, trade secrets, domain names or any other rights, functions or licenses with respect to the Service and you may not use the Service for any other purpose without Company's prior, express written authorization.

Company does not claim ownership over User Content. However, you grant Company permission to use your User Content, for the purposes of providing, developing and supporting the Service.

Amendments to these Terms

The Company reserves the right to amend these Terms from time to time. The Company will notify you of the amended Terms. You need to accept the amended Terms to continue use of the Service. By continuing use of the Service after the amended Terms have taken effect, you indicate your acceptance to the amended Terms.

Handover of Customer data

An appendix to the **LAAS LICENSE AND SERVICE AGREEMENT ("Agreement")**

General

The database used in LaaS is designed so that the user's personally identifiable information is stored separately from data generated by the Users' use of the LaaS service. These datasets can be combined only by using a randomly generated identifier. This arrangement makes it possible to simply and permanently anonymize the Users' data by deleting the personally identifiable information.

After termination or expiration of the Agreement, LaaS Company will execute the deletion and anonymization operations described in this document.

Data handed over to the Customer

Some of this data is also available from the Admin user interface during normal use of the LaaS service.

- Service descriptions, including names and longer textual descriptions
- Service Provider descriptions
- The average evaluations of services by Provider
- Service order counts
- Statistical data and analysis as available in the LaaS Admin user interface

Other data, individual Users' survey responses in particular, is not handed over.

Data deleted on termination of the Agreement

This list is not comprehensive. LaaS Company is not obligated to store any Customer data after the termination of the Agreement. Some data may, due to technical reasons, be stored in backups of system caches after the termination or the expiration of the Agreement. The data in these backups and caches is removed during the normal operation of the system.

- Individual Users' Personally Identifiable Information such as their email address
- Survey responses' connections to deleted Personally Identifiable Information
- Service names and descriptions
- Service Provider names and descriptions
- Free text responses to surveys, free texts in reviews and Service Order comments
- Other textual input given by the Users.

Data stored indefinitely

NOTE: The data listed here is not published in a way that would make it possible to identify a particular Customer company. As mentioned earlier, information which would allow identification of individual users are permanently deleted upon termination or expiration of the Agreement.

The data described in this section is used to create comparison data over all LaaS Customer organizations, for example to answer questions such as "How is my company's employee satisfaction relative to other companies in the same industry?"

- Statistical data and analysis as available in the LaaS Admin user interface
- Answers to survey questions found in LaaS (not including questions added by the Customer) anonymized so that the respondent is not identifiable
- Service Order data and evaluations, excluding the data listed in the previous section
- The anonymized user data collected for development and improvement of the Service, such as data collected by Google Analytics or similar tools

Data handed over for research purposes during or after the validity of the Agreement

- Individual User's data can be handed over in an anonymized format for scientific research if the user has agreed to it in the settings of their LaaS profile.
- Data collected are the industry and size of the Customer, but only if they do not identify a specific LaaS Customer.

For scientific research we do NOT hand over:

- LaaS Customer's name
- Individual users' personally identifiable information (such as email address)
- The randomly generated identifier described earlier. Instead, a new random, single-use identifier is generated.
- Free text responses to surveys, free texts in reviews and Service Order comments or other textual input given by the users.

Data published

Grouped by industry, statistics on survey questions and complete surveys provided with LaaS, but only when the industry group contains at least five (5) LaaS Customers.

Statistics on survey questions and complete surveys provided with LaaS, but grouped only so that any group specified in the statistics contains at least ten (10) people.

APPENDIX 1

DATA PROCESSING AGREEMENT

1 PURPOSE OF THE AGREEMENT

This Data Processing Agreement (hereinafter "**DPA**") sets out the conditions under which the Processor may process the Controller's personal data on behalf of the Controller. This Appendix is a fundamental part of the Leadership as a Service License Agreement between the Processor and the Controller ("**Service Agreement**"). With regard to personal data incurred in connection with the service use, the Controller acts as a controller of the personal data and the Processor acts as the processor of the personal data.

2 DEFINITIONS

2.1 The concepts and definitions used in this DPA are defined below. Other terms used herein have the meaning given to them in the applicable data protection legislation.

Applicable data protection legislation shall mean applicable data protection legislation as in force from time to time, such as the General Data Protection Regulation, applicable national data protection laws and binding regulations of the data protection authorities.

Personal data shall mean personal data as defined in the applicable data protection legislation.

General Data Protection Regulation shall mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).

2.2 Parties agree to negotiate in good faith over necessary additions and complements to the terms of this DPA throughout the term of the agreement to make sure that this DPA is in line with the obligations arising from the applicable data protection legislation.

2.3 The Processor shall process personal data lawfully, with due care and diligence and in accordance with good data processing practice.

3 INSTRUCTIONS ON PROCESSING PERSONAL DATA

3.1 The Controller has the right to issue the Processor binding written instructions on processing of personal data. At the effective date of this DPA, the Controller has instructed the Processor to process personal data to fulfill the terms of the Service Agreement. The description of personal data processing is in Appendix 1. The instructions shall include at least the following information:

(i) The purpose of processing personal data
(ii) The nature of processing personal data
(iii) The retention period for personal data

(iv) The types of personal data
(v) The groups of data subjects

3.2 The Processor shall process personal data in accordance with applicable data protection legislation and written instructions issued by the Controller. If the Controller wishes to provide the Processor with supplementary instructions on processing personal data, such instructions must be delivered in writing. The instructions are binding on the Processor after the Processor has accepted them in writing. If the Processor is not able to comply with the supplementary instructions (such as technical restrictions due to standard nature of the service provided under the Service Agreement), the Parties shall then discuss how to proceed with the supplementary instructions.

3.3 The Processor shall immediately inform the Controller if, in its opinion, any instructions given by the Controller infringes the applicable data protection legislation. The Processor shall not be obligated to follow any instruction that it suspects to be unlawful.

4 APPLICABLE DATA SECURITY MEASURES

4.1 The Processor shall implement and maintain appropriate technical and organizational data security measures in respect to the personal data it processes. The purpose of these measures is to ensure lawful processing of personal data and the confidentiality, integrity, availability and resilience of the processing systems and services. Information security practices are constantly developed. The data security measures are set out in Appendix 2.

4.2 The Processor only processes personal data to the extent necessary to carry out the service defined in the Service Agreement. The supplier shall procure that all persons acting under its authority and having access to the personal data of the Controller, are under obligation of confidentiality.

4.3 The Processor shall notify the Controller of any personal data breach without undue delay. In addition, the Processor shall assist the Controller to fulfil its legal obligations in respect to documenting and informing the breach to the data subjects and the relevant supervisory authority.

5 ASSISTANCE TO THE CONTROLLER

5.1 The Processor shall assist the Controller in order for the Processor to be able to fulfil its obligations in respect to information requests related to rights of a data subject. These requests may require the Processor to assist in providing information and communicating to the data subjects, carrying out data subject's right of access, rectifying or erasing of personal data, carrying out restriction of processing of personal data or transfers of personal data from one system to another.

5.2 Taking into account the nature of processing and the information available to the service provider, the Processor shall assist the Controller to ensure that the obligations pursuant to Article 32 to 36 of the GDPR, including safety of processing data, personal data breach notification and data protection impact assessments are complied with.

5.3 The Processor is entitled to invoice the Controller according to its price list for activities and expenses related to providing assistance, data protection impact assessment support and any actions and costs caused by changes made in the Controller's instructions. The Processor shall inform the Controller in advance of any additional costs incurring.

6 SUB-PROCESSORS WHO PROCESS PERSONAL DATA

6.1 The Controller may use sub-processors for processing personal data as set forth in this agreement. The Controller has the right to be informed of the sub-processors the Controller uses for processing personal data. On the date of this DPA, the sub-processors used by the Controller are set out in an Appendix 3 to this DPA.

6.2 By this agreement, the Controller gives the Processor general prior authorization to engage sub-contractors for processing personal data. The Processor shall inform the Controller of any change in writing. A change will enter into force thirty (30) days after the Processor has informed the Controller of the change unless the Controller has informed the Processor that it objects such change on a reasonable, data protection related cause before the change. If the Controller does not approve the sub-processor, the Processor has the right to terminate this agreement with 30-day notice period.

6.3 The Processor may only use such sub-processors which are committed to complying with the obligations set forth in the GDPR, the data protection obligations of this DPA or similar obligations providing same level of data protection.

6.4 The Processor is liable for the sub-processors' acts as for its own acts and shall enter into necessary written agreements on the processing of personal data with the sub-processors.

7 DATA TRANSFERS

The Processor shall have a right to freely transfer the personal data within the European Union or the European Economic Area. The personal data may also be transferred outside the EU or the EEA following the requirements laid down in the GDPR. The Controller has the right, at any time, to receive information on the location of the personal data processing.

8 RIGHT TO AUDIT

8.1 The Controller or any auditor authorized by it shall, during the term of this DPA, have a right to conduct audits or inspections of the Processor to ensure the Processor is complying with the personal data processing obligations. The Processor shall have a right to reject a certain third-party auditor if such third party is a competitor of the Processor. The Controller shall provide the Processor a written notification of the audit at least (10) business days prior to the audit. The Controller shall serve a written notice to the Processor and the audit shall be carried out within the office hours and without interrupting the Processor's standard operations or its obligations towards any third parties.

8.2 The Processor shall make available to the Controller all information the Controller needs in order to verify the compliance with the obligations laid down for a personal data processor and assist the Controller in carrying out the audit.

8.3 The Parties shall cover their own costs associated with an audit. If an audit reveals material failure by the Processor, the Processor shall bear all costs related to identifying and correcting the failure. No indirect costs are covered.

9 DAMAGES

9.1 Each Party shall be liable for such part of imposed damages or administrative fines which correspond to the Party's confirmed liability for the overall damages imposed in the final decision of the data protection authority or a competent court.

9.2 A Party's total liability for damages to the other Party is limited to 100 per cent of the total price of the delivery, excluding VAT, during twelve (12) months preceding the damage. A Party shall not be liable for indirect damages. Indirect damages include, for example, any loss of anticipated profits or consequential damages arising from decrease or interruption of production or revenue. Limitation of liability is not applied if the damage is caused by intentional misconduct or gross negligence.

9.3 Any claim to the Processor shall be made in writing without undue delay. If the error or deficiency is discovered or could be discovered immediately, the notice must be served immediately and no later than within 14 days. If the specified claim is not served to the Processor within three months from finding the damage and no later than within one year from the personal data processing act in question, no compensation or damages will be paid by the Processor.

10 CONFIDENTIALITY

10.1 The Processor shall commit to a) keep all personal data received from the Controller confidential, b) ensure the persons entitled to process the personal data are committed to a confidentiality obligation, and c) ensure the personal data is not transferred to any third parties without prior written approval of the customer unless the service provider is obligated to express such data on the basis of mandatory provision of law or authority order. In this context, the Processor's sub-processors are not interpreted as third parties.

10.2 If a data subject or an authority makes a request concerning personal data, the Processor shall, as soon as reasonably possible, inform the Controller of such request before answering the request or performing any other measures related to the personal data. If the competent authority requires immediate answer, the Processor shall inform the request to the Controller as soon as possible after answering such request, unless otherwise provided in the mandatory provision of law.

10.3 The confidentiality obligation shall survive the termination of the DPA.

10.4 The Processor has the right to use the personal data register's data incurred based on the use of the service in an anonymized form. The Controller grants the Processor a permanent, non-transferable, non-exclusive and free-of-charge right to use this anonymized data to develop its services.

11 DELETION AND RETURNING THE PERSONAL DATA

11.1 Upon termination of the Service Agreement, the Processor shall delete or return to the Controller all personal data transferred according to the agreement and delete all copies of the data. The Processor shall delete the date no earlier than thirty (30) days and no later than ninety (90) days after the termination of the Service Agreement.

12 TERM AND TERMINATION

This DPA enters into force when duly signed by both Parties and remains in force until the Processor has deleted the personal data as set forth in Section 12.1 above.

13 APPENDICES

Appendix 1: Instructions for personal data processing
Appendix 2: Technical and organizational measures
Appendix 3: Sub-processors

APPENDIX 1 – INSTRUCTIONS FOR PERSONAL DATA PROCESSING

The Processor processes the personal data in accordance with the instructions given below.

INSTRUCTIONS

The purpose of processing
The Processor carries out services to the Controller involving processing of personal data

Nature of processing
Performing and carrying out services set out in the Service Agreement

Duration of the personal data processing
Term of the Service Agreement

Personal data types
- Basic profile data such as name and email address
- Demographic data
- Data created during use of the Service such as service orders
- Device information, e.g. the user's browser version

Categories of data subjects
- Employees

Other instructions
[In case needed, provide more specific instructions for personal data processing.]

APPENDIX 2 – TECHNICAL AND ORGANISATIONAL MEASURES

- In this Appendix 2, ”System” shall mean the service defined in the Service Agreement
- The Processor shall comply with good data processing practice required by the data protection legislation, provisions concerning protecting personal data as well as instructions on the data processing provided by the Controller.
- The Processor instructs and trains necessary data security and data protection practices to employees participating in the maintenance of the Processor’s System.
- The Processor procures that all persons participating in the maintenance of the Processor’s System are committed to the confidentiality obligation set forth in the DPA.
- The Processor is responsible for taking regular backup copies and tests restoring the backup copies regularly.
- There is no direct link to databases and reverse proxy from the internet, but only via encrypted tunneling.
- Databases and backups copies thereof are located in locked up premises.
- In the System, only secured data exchange is used.
- Employees of the Processor have user rights defined based on their assignments and system specific personal user rights and passwords. The System developers are required to have 2FA identification for Google cloud services. Access rights to the servers and the database are limited to minimum.
- The Processor protects the System against security breaches and offenses and observes the safety of the System and any unlawful access attempts. The Processor shall inform the Controller of any data security breaches without undue delay.
- The Processor shall procure that data security updates of the components belonging to the System are installed regularly.

APPENDIX 3 – SUB-PROCESSORS

Sub-processor	Location of personal data	Description	Transfer mechanism
Google	EU	LaaS application deployment in Google Cloud, including its database, virtual machines and other services.	
Mailgun	EU	Used to send email to users.	

Technical Service Description

v1.2

Technical Environment
LaaS is cloud service compatible by design and implementation.

- Servers located in a Kubernetes cluster on Google Cloud
- Scalable microservice architecture
- Google Cloud SQL (PostgreSQL) database
- Multi-tenant HA environment with each client in a separate database schema
- Gitlab CI environment
- Several different login methods and options
- Client-specific login expiration times and secrets

We use existing email addresses and single sign-on links as the primary user login method. Users may also log in by linking their personal Google account with LaaS.

Azure AD or Google G Suite User Integration
We also support login using client's own Azure AD or Google G Suite authentication.

- OAuth 2.0
- Single sign-on

Other User ID Sources
As an add-on service, user integration can also be done using other user ID sources. Clients may also perform the integration independently against the LaaS API.

Data Security
Our aim is to provide our clients with system security that exceeds their expectations.

- Forced HTTPS throughout the web service
- Access rights to the servers and database limited to a minimum
- Connections between servers and database are encrypted

- No direct online connection to database and frontend servers, only secure connections through encrypted tunnels
- Developers are required to use two-factor authentication with Google Cloud

Your privacy and security are our number one priority. Our clients are free to conduct security audits to make sure that the quality of our service meets or exceeds requirements.

Data
Users' personal data is gathered, processed, and stored in accordance with the EU General Data Protection Regulation, applicable data protection legislation, and good database practices.

Data is stored in databases protected with firewalls, passwords, and other technical measures. Data is only accessible to persons whose duties require such access.

User data is provided by the data subjects themselves and gathered from our systems as the registered users use the service. The data subjects have the right to review their personal data stored in the Vincit LaaS client register, to request that any inaccuracies in their personal information be corrected, and to prohibit the use of their data.

Privacy Policy: https://laas.fi/en/privacy-policy/

For further information, please contact:
tuki@laas.fi