Beamex Data Processing Agreement (DPA)

(multi-language version)

This document contains the Beamex Data Processing Agreement ("DPA") in multiple languages. In case of any discrepancies or inconsistencies between the language versions, the English version shall prevail.

Data Processing Agreement (EN)

1. Introduction, Purpose and Application

This Data Processing Agreement ("**DPA**") is applied as part of the commercial agreement ("**Agreement**") to the processing of personal data carried out by a Beamex legal entity specified in the offer, order confirmation or Agreement, such as Beamex Oy Ab or any of its subsidiaries ("**Processor**") in connection with providing digital or other services ("**Services**") to the customer who is a contracting party in the Agreement as well as the data controller of such personal data ("**Controller**"), which Services are described in more detail in the Agreement concluded by and between the Processor and the Controller.

This DPA is an integral and inseparable part of the Agreement between the parties. All terms used in this DPA, but not defined, have the same meaning as they have in the Agreement. If there is a conflict between the Agreement and this DPA, the terms of the DPA take precedence.

2. Definitions

"**Controller**" means the natural person or legal entity, authority, agency or other body mentioned in this DPA, which alone or jointly with others defines the purposes and means of personal data processing.

"**Data Protection Law(s)**" means the Data Protection Act (1050/2018) and the EU General Data Protection Regulation (2016/679) with amendments and replacement regulations as well as other valid and applicable data protection legislation and instructions and binding regulations of data protection authorities.

"**Data Subject**" means an identified or identifiable natural person whose Personal Data is Processed on the basis of this DPA.

"**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is considered to be a natural person who can be directly or indirectly identified especially on the basis of identification information such as name, social security number, location information, online identification information or one or more physical, physiological, genetic, psychological, economic, cultural or social factors characteristic of him or her.

"**Personal Data Breach**" means a data security breach event resulting in the accidental or illegal destruction, loss, alteration, unauthorized disclosure or access to personal data transferred, stored or otherwise processed.

"**Processing**" means the function or functions that are applied to Personal Data or data sets containing Personal Data in connection with the provision of Services, either using automatic data processing or manually, such as collecting, storing, organizing, structuring, storing, modifying or changing, searching, querying, using, transferring data , distributing or otherwise making them available, matching or combining, limiting, deleting or destroying the information.

"**Processor**" means the natural person or legal entity, authority, agency or other body mentioned in this DPA that Processes Personal Data on behalf of the Controller.

"**Standard Contractual Clauses**" means the Standard Contractual Clauses (EU) 2021/914 as of 4 June 2021. Any reference made to the Standard Contractual Clauses shall refer to the Standard Contractual Clauses, which includes the parties' selection on certain Modules and optional clauses as well as Appendix I to II in this DPA. In addition, the parties agree that the use of Subprocessors shall be governed by Clause 9, Option 1 of the Standard Contractual Clauses.

"**Subprocessor**" means a natural person or legal entity in a contractual relationship with the Processor, who processes Personal Data as a subcontractor of the Processor as part of performing Services for the Controller.

3. Scope of Processing and Processing Activities

Pursuant to this DPA such Personal Data is processed, for which the Controller acts as the sole data controller.

The Processor Processes Personal Data (i) in accordance with Data Protections Laws and the terms of this DPA to fulfill the obligations described in the Agreement; and (ii) in compliance with the written instructions given by the Controller from time to time, unless otherwise required by the Data Protection Laws applicable to the Processor. The Processor may not process Personal Data for any of its own purposes or hand it over to third parties, unless this DPA allows it. The Processor must notify the Controller if it considers or suspects that the Controller's written instructions violate the Data Protection Laws. Unless otherwise stipulated in this DPA or its appendices, the Processor may Process Personal Data only for the duration of the Agreement.

The Controller (i) undertakes to comply with the obligations in accordance with the Data Protection Laws applicable to it in the Processing of Personal Data; and (ii) is responsible for the fact that it, as the sole data controller, has the right to Process Personal Data and that it has fulfilled its obligation to inform the Data Subjects and/or received (or will receive) all the consents required by the applicable Data Protection Laws from the Data Subjects for the Processor to Process Personal Data on behalf of the Controller in accordance with this DPA.

More detailed information about the Processing, such as the nature of the processing, types of Personal Data and groups of Data Subjects, are described in **Appendix 1**. The appendix can be updated if changes occur in the Processing.

However, the Controller acknowledges and accepts that as part of providing the Services to the Controller, the Processor has the right to use information related to the operation, support or use of the Service or obtained in connection with it for its legal and legitimate internal business purposes, such as (i) invoicing the Service based on usage or number of users, (ii) delivery of the Service and for managing the provision thereof, (iii) for the functional and technical development of the Service, (iv) for compliance with applicable laws (including responding to official requests), (v) for ensuring the security of the Service, and (vi) for preventing fraud and abuse or reducing risks. To the extent that such information is Personal Data, the undertakes that: (a) it will process such Personal Data in accordance with the applicable Data Protection Laws and only for purposes that are compatible with the objectives described in this section; and (b) it does not use such Personal Data for any other purpose or disclose it to third parties, unless it has first anonymized the data so that the Controller or no other person or entity can be identified from the data.

4. Subcontractors and Subprocessors

The Processor has the right to use Subprocessors in the Processing. Upon request, the Processor must provide the Controller with more information about the Subprocessors it uses. If the Processor makes significant changes to its Subprocessors it must notify the Controller in writing. The Controller has the right to prohibit the use of a specific Subprocessor for a justified reason. If the Controller prohibits the use of a particular Subprocessor and it is not reasonably possible to transfer the tasks of that Subprocessor to anyone else, including to the Processor, the Processor has the right to terminate the DPA and end the Processing. The Controller is not entitled to any compensation solely on the basis that the Processing ends and the DPA has been terminated due to the Controller prohibiting the use of a specific Subprocessor.

The Processor must enter into a written agreement with each Subprocessor, which contains the terms and conditions required by the Data Protection Laws and essentially similar types of obligations as the Processor has under this DPA. The Processor is responsible for the Subprocessors it uses, just as it is for its own actions.

5. Data Security

The Processor must implement appropriate technical, physical and organizational measures to ensure a high level of security in the Processing of Personal Data by the Processor and to protect Personal Data from unauthorized or illegal processing and from unintentional loss, destruction, damage, change or transfer. When evaluating the necessary measures to guarantee the level of security, the instructions of the Controller, the latest technology and implementation costs, the nature, scope, context and purposes of the Processing, as well as the risks to the rights and freedoms of natural persons, which vary in probability and severity, must be taken into account.

Applicable measures may be, for example: (i) pseudonymization and encryption of personal data; (ii) the ability to guarantee the continuous confidentiality, integrity, availability and fault tolerance of the systems and services; (iii) the ability to quickly restore the availability of Personal Data and access to Personal Data in the event of a physical or technical failure; and (iv) the procedure for regularly testing, examining and evaluating the effectiveness of technical and organizational measures to ensure the security of the Processing. The Processor must take measures to ensure that every natural person working under the Processor who has access to Personal Data processes it only in accordance with the instructions of the Controller, unless otherwise required by applicable Data Protection legislation. The Processor is responsible, in accordance with its own policies, for taking backups of the data and files of the Controller in its possession and for checking their functionality.

Without limiting the requirements and obligations described above, the Processor must always implement at least the technical and organizational information security measures which essentially correspond to the measures described in **Appendix 2**.

6. Confidentiality

The Processor must ensure, to the extent reasonably possible, that only those persons acting on its behalf who have a need to access the information in order to fulfill the purpose of this DPA have access to the Personal Data, and that the persons who have the right to process the Personal Data are committed to complying with the obligation of confidentiality or are subject to the appropriate statutory obligation of confidentiality.

7. International Data Transfers

7.1 Transfers allowed

The processor may transfer to a country outside the European Union or the European Economic Area. The processor must always comply with the conditions and requirements of the Data Protection Laws when transferring data to countries outside the European Union or the European Economic Area, such as using standard contract clauses published by the EU Commission applicable to data transfer.

7.2 Processors in the EEA and the Controller outside the EEA

If the Processor is located inside the EEA and the Controller outside the EEA, the transfer of Personal Data shall be governed by Module 4 of the Standard Contractual Clauses which are incorporated herein by reference and form an integral part of the DPA. The Controller enters into the Standard Contractual Clauses as "data importer" and Processor as "data exporter".

For the purposes of the Standard Contractual Clauses:

a) the module four shall apply;
b) the optional docking clause, Clause 7, shall apply;
c) in Clause 11, the optional language is to be deleted;
d) in Clause 17, the substantive laws of Finland shall apply;
e) in Clause 18, disputes shall be resolved before the district court of Helsinki, Finland; and
f) the Annexes of the Standard Contractual Clauses shall be populated with the information set out in the DPA, including its appendices.

If and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement or the DPA regarding the transfer of Personal Data from Controller to Processor, the Standard Contractual Clauses shall prevail to the extent of such conflict.

If the Processor is located within the EEA and commissions a Subprocessor located outside the EEA, the Processor shall enter into the Standard Contractual Clauses (Module 3) with such Subprocessor. Any further onward transfer of Personal Data must comply with the applicable Module of the Standard Contractual Clauses.

8. Personal Data Breaches and Reporting Obligations

The Processor must notify the Controller of all real or suspected Personal Data breaches without undue delay after becoming aware of the breach.

The Processor must provide the Controller with all available information about the Personal Data Breach, which the Controller may need to fulfill its own investigation and reporting obligations. The Processor can later supplement the information if it does not have comprehensive information about the violation immediately available. The Processor must otherwise assist and cooperate with the Controller in the investigation of the Personal Data Breach and in possible matters related to notifications to authorities and interested parties. The Processor must also take the necessary reasonable follow-up measures to mitigate the adverse effects of the Personal Data Breach, repair the violation or breach that has occurred, and prevent future violations. The Processor may not comment on the Personal Data Breach to third parties, especially media representatives, without express written consent and instructions from the Controller, unless otherwise required by Data Protection Laws.

Unless otherwise required by the Data Protection Laws or the order of the competent authority, the Controller makes the final decision at its own discretion on whether the Personal Data Breach must be notified to the authorities or other parties involved, and on the possible way to make such notifications. If the Processor reports a Personal Data Breach to the authorities or other interested parties, they must be approved in advance by the Controller.

9. Documentation and Auditing Rights

A party has the obligation to make available to the other party all the required information and documents that are necessary for demonstrating compliance with this DPA and the Data Protection Laws.

At the request of the Controller, the Processor must also allow audits of the Processing, Services, information security measures and the Processor's information systems and processes, and participate at reasonable intervals to such audits for the purpose of ensuring compliance with this DPA and the Data Protection Laws. Such audits may be carried out no more than once a year, unless there is a justified reason to assume that the Processor does not comply with the DPA or the Data Protection Laws. Audits may also include visits to the Processor's offices or other physical premises. The audit is carried out during normal working hours and in such a way that it does not unnecessarily disturb the Processor's operations. Each party is responsible for its own costs related to the audit. The Processor must be notified of planned audits at least fifteen (15) days before the intended audit. Information about the Processor's activities obtained by the Controller during the audit is confidential.

10. Assisting the Controller

The Processor must, at the request and expense of the Controller, reasonably assist the Controller in complying with the obligations data controllers have in accordance with the Data Protection Laws. The duty to assist applies in particular to the following matters:

10.1 Access to Personal Data

Insofar as the Personal Data is not available directly through the Services, the Processor shall, upon request, provide the Controller with the data in question. If the information is available in electronic form, it must also be delivered to the Controller in that form.

10.2 Fulfillment of Data Subjects' rights and requests from the supervisory authority

The Processor must notify the Controller without delay: (i) of all requests, complaints or notifications made by the supervisory authority or other competent authority; and (ii) from any requests received directly from the Data Subject, related to the fulfillment of the data subject's rights. The Processor may respond directly to the request only if the Controller has given permission and instructions to do so in advance. If the Controller so requests, the Processor must reasonably assist the Controller in responding to official requests and in fulfilling the data subject's rights according to the Data Protection Legislation.

10.3 Data protection Impact Assessment

If the Processor becomes aware that the planned Processing would cause a high risk in terms of the rights and freedoms of a natural person, it must inform the Controller of this and, if necessary, assist the Controller in carrying out an impact assessment regarding data protection.

10.4 Correction, Deletion and Restriction of Personal Data

The Processor must either (i) offer the possibility to correct, delete or limit the processing of Personal Data through the functions of the Service or (ii) correct, delete or limit the processing of Personal Data in accordance with the instructions of the Controller.

11. Term and Termination

11.1 Entry Into Force and Termination

Unless otherwise agreed, this DPA enters into force at the same time as the Agreement and remains valid as long as the Processor Processes the Controller's Personal Data in connection with the provision of its Services. Regardless of the termination of the DPA, the provisions of the DPA, which are of such a nature that they are intended to remain in force regardless of the termination of the Agreement, remain in effect regardless of the termination of the DPA.

11.2 Returning or Deleting Personal Data at the End of Processing

Upon termination of the DPA, the Processor must, at the Controller's choice, either delete all Personal Data Processed on behalf of the Controller or, alternatively, return all Personal Data to the Controller and delete existing copies, unless the Data Protection Laws or other regulation (e.g. ISO 17025) require retention of Personal Data. In that case, the Processor has the right to keep the Personal Data in accordance with the requirements of the law, without otherwise continuing the Processing of the Personal Data and still complying with the confidentiality obligations described in this DPA. The return or deletion of personal data must be carried out without undue delay after the Controller's request. If the Controller has not given any instructions regarding the deletion or return of Personal Data, the Processor may on its own initiative delete the Personal Data in its possession when twelve (12) months have passed from the end of the DPA. The Processor must return the Personal Data in a commonly used, data-secure electronic format or in another format agreed upon by the parties.

12. Other Terms

12.1 Changes

All changes to this DPA must be agreed in writing between the parties. For the sake of clarity, it is stated that the written instructions given by the Controller from time to time to carry out the Processing of Personal Data are not considered to be changes to this DPA.

12.2 Responsibilities and Liability

If the Data Subject suffers damage due to a violation of the Data Protection Laws, the responsibility of the Controller and the Processor for the damage is determined in accordance with Article 82 of the EU General Data Protection Regulation (2016/679). Each party is responsible for possible administrative fines imposed by the supervisory authority on the basis of a violation of the Data Protection Laws. A party's liability for damages to the other party based on a breach of contract of this DPA is a total maximum amount that corresponds to the VAT-free service fees paid on the basis of the Agreement for the six (6) months preceding the submission of the first claim for damages. In other respects, the terms of limitation of liability that may be contained in the Agreement between the parties or its appendices also apply to this DPA. Unless otherwise expressly stated herein, a party is not liable to the other for any indirect, consequential, incidental, special or punitive damages (including any damages for business interruption and loss of use, data, sales, revenue or profit), which are specifically excluded.

12.3 Applicable Law and Dispute Resolution

Regarding the applicable law and the resolution of disputes, the terms of the Agreement between the parties are followed, unless the Data Protection Laws states otherwise. If the Agreement does not state applicable law or contain dispute resolution terms, the DPA shall be governed by the substantive laws of the Processor's domicile.

13. Appendices

This DPA consists of this document and the attachments listed below:

- Appendix 1: Description of processing operations
- Appendix 2: Technical and organizational information security measures

Appendix 1 to DPA (and where applicable, to Standard Contractual Clauses)

A. LIST OF PARTIES

Data exporter:

Name: Beamex Oy Ab

Address: Ristisuonraitti 10, 68600 Pietarsaari, FINLAND

Activities relevant to the data transferred under these Clauses: Beamex is a technology company manufacturing and providing calibration equipment, software and related services and support to its industrial customers. The data importer is a customer of Beamex and user of Beamex's digital services, which this DPA concerns.

Role (controller/processor): processor

Data importer(s):

Name: the name stated in the commercial agreement concluded with Beamex Oy Ab.

Address: as stated in the commercial agreement.

Activities relevant to the data transferred under these Clauses: The data importer is a customer of Beamex using Beamex's digital services.

Role (controller/processor): controller

Processor's essential Sub-Processors at the time of concluding the DPA:

a) **Microsoft Datacenter Netherlands B.V.** As Beamex Oy Ab subscribes to Azure cloud services (PaaS) - West Europe under the terms of the Microsoft Product Terms site, the data processing and security terms are defined in Microsoft Online Services Data Protection Addendum (DPA).
b) **Bjorkstrom Oy Ab** – domiciled in Finland, processing activities include development and deployment of LOGiCAL.

B. DESCRIPTION OF TRANSFER/PROCESSING

	Beamex Digital Services and Cloud Software (e.g. LOGiCAL)	Other Beamex Services (e.g. software support, data migration, system integration)
Categories of data subjects whose personal data is transferred:	Primarily such employees or subcontractors of the controller that use and perform calibrations with Beamex calibration equipment, which results are then stored in the Beamex calibration software.	Primarily such employees or subcontractors of the controller that use and perform calibrations with Beamex calibration equipment, which results are then stored in the Beamex calibration software.
Categories of personal data transferred:	Especially name, job title, employer's name as well as data relating to the activities the person has performed with Beamex's calibration equipment.	Especially name, job title, employer's name as well as data relating to the activities the person has performed with Beamex's calibration equipment.
The frequency of the transfer:	Data is transferred both on a continuous and as needed to provide the service(s) basis.	As needed.
Nature of the processing:	Providing user rights to Beamex calibration software to the controller and storing calibration data in the software of the calibrations the controller's employees and subcontractors have performed.	Provision of helpdesk, support and maintenance services to Beamex's customers, as well as the provision of migration and integration services related to software products, during which the processing of personal data may occur.
Purpose(s) of the data transfer and further processing:	Use of Beamex calibration software for storing calibration results.	To enable the use of Beamex's products, their implementation, and/or their operation in conjunction with other systems.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	The duration of the commercial agreement and as long as the controller uses the Beamex digital services.	The duration of the commercial agreement and as long as Beamex processes the data as a data processor for the purposes.
COMPETENT SUPERVISORY AUTHORITY:	Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) Street address: Lintulahdenkuja 4, 00530 Helsinki, FINLAND Switchboard: +358 29 566 6700, Registry: +358 29 566 6768 www.tietosuoja.fi	

Appendix 2 to DPA (and where applicable, to Standard Contractual Clauses)

A description of the technical and organizational measures that the Processor must implement in addition to the general obligations mentioned in the DPA to ensure an appropriate level of data security.

Area	Plans and practices
Microoft Azure (PaaS)	**Beamex LOGiCALand Beamex Sync services are built on Azure (PaaS). Microsoft Service trust portal lists all relevant business continuity (ISO22301) and ISMS (ISO27001 and other 27000 series) certifications, reports, documents etc., at address https://servicetrust.microsoft.com/viewpage/ISOIEC**
Premises and physical security	**Access to premises**. The Processor limits access to its premises with personal ID cards (RFID). Access rights to different areas within the premises are granted based on rights defined by the management and supervisors. Certain special areas may have enhanced measures of protection and access control. Guests have access only to public premises (lobby, cafeteria, restrooms) and move in the Processor's premises only with a host. **Alarm systems and guarding of facilities.** Guarding of premises is outsourced to a professional security company. The premises have industry standard alarm systems, including alarms for unauthorized access, laboratory condition monitoring, cooling/temperature of the ICT data centers, air conditioning system alarms and fire alarm systems. The company's Manager of Technical Services is responsible for the technical maintenance of the access monitoring and alarm systems. The employees have been trained or have available instructions on how to operate in various alarm or crisis situations, certain situations may be practiced on a regular basis.
Personnel, organization and information security management	**Personnel security.** Employment agreements signed with employees contain an industry standard confidentiality clause. In certain special situations additional confidentiality agreements may be signed (e.g. specific projects and/or information). The employees are also required to follow any guidelines or policies the Processor may have, including without limitation those relating to business ethics, privacy and information security. **Training and guidelines.** A compulsory information security training is part of every new employee's onboarding program. Additional general or specific information security training is organized for the employees from time to time. Management, supervisors, system owners, access control and other responsible persons are trained for contents of the Processor's information security policy and its future revisions. Many of such persons also participate in risk management and business continuity planning reviews, training and/or exercises. Specific guidelines for employees may exist in various areas, such as work email, remote access and remote work, tools and software as well as managing files, documents and records. **Management, monitoring, reviews and audits.** The assessment of information security and business continuity risks is part of the company's quality system audits. Separate risk assessments, inspections and development plans are made on the basis of findings, identified risks and always in connection with new development projects or planning system/facilities/process changes. External experts, peer reviews or audits are utilized when possible or necessary for the assessment of the technical information security level. The company's ICT function manages the framework for information security and is responsible for many practical and technical information security measures. ICT is represented in the company's management team.
Business continuity	The Processor maintains plans and measures for business continuity and disaster recovery.
Third parties, subcontractors, processors and subprocessors	**Background and contracts.** Background of third parties, subcontractors and subprocessors is checked as considered appropriate and necessary before entering into a business relationship. Third party partners are contractually bound by confidentiality obligations. Written data processing agreements (or annexes) are concluded with such partners that are considered as data processors or subprocessors of the Processor. If and when relevant, training or instructions may be provided to third parties employed by the Processor on topics relating also to information security. **IT procurement.** Computers, mobile devices, systems and software are procured primarily by the IT function. License information is registered and stored by the IT as well.

Beamex internal data, servers and networks	**Access control and authentication.** The Processor uses industry standard measures to authenticate persons and users, limit access (as well as to prevent unauthorized access) to systems, software, files and data. Two-factor authentication is primarily required when logging into the network from a remote connection. The aim is to primarily use domain single sign-on in the applications. Passwords must be at least 8 characters long, but 14-character strong passwords containing special characters, numbers and capital letters are preferred. Access to certain files may also be restricted to system, folder, and document-specific access right restriction. **Email.** Guidelines to email communications exist. Special email security issues need to be considered when sending or receiving confidential information. The connection between the email server and terminal device (computer, telephone, tablet, etc.) is encrypted. **Files and databases.** Various practices are in place for storing data in the cloud. Saving important data to a local computer hard drive is not recommended. Servers and systems in the Processor's own on-premises are used for saving sensitive or highly confidential information. Separate guidelines and practices exist for storing and managing records requiring filing and archiving or version and lifecycle management. Sharefile is the primary tool for delivering confidential information to third parties in a secure way. Microsoft Office365 is widely used for storing and sharing especially such documents that are used in teamwork (excluding very sensitive or highly confidential information). **Remote connections.** Supervisors define the need for devices, software and remote connections for mobile work. Secure client VPN or Citrix/XenApp with two-factor authentications required for remote work. Mobile devices are password/code protected and when applicable, MDM controlled. Separate policies may exist for mobile work and storing files and records in the cloud. **Networks, servers and IT infrastructure.** Data networks are segmented into separate sub/virtual networks. Appropriate tools and/or services are used for their traffic monitoring, prevention of penetration and observation as well as AV monitoring. Certain data connections and critical network edge components are duplicated. The aim is to arrange either duplication or a back-up device for all the critical components to mitigate so-called single point of failure (SPOF) risks in data networks, servers, storages and other critical systems. An own storage is maintained for critical device spare parts and components. The electricity supply for certain critical systems and devices are backed up by an uninterrupted electricity supply (UPS) system. High Availability (HA) storage systems, storage mirroring or some other fault-tolerant systems considered for critical information systems may be used. Regular image/system back-ups are performed on virtual servers, production systems and some other computers in critical use, in accordance with the applicable standard operating procedure. System back-ups are implemented in other objects according to case-specific consideration and risk assessment. **Back-up policy.** The Processor has various back-up plans and measures for the purpose of data and systems recovery. The plans and measures may vary depending on the importance of the data and system. The Processor has a separate standard operating procedure for backups of data and information systems. **Malicious software.** The Processor maintains firewalls as well as antivirus, anti-malware, spam filtering and other similar technical measures to detect, prevent and protect against external cyber attacks, unauthorized access and installation of malicious software to its data, systems, networks and devices.

[End of DPA.]

数据处理协议 (ZH)

1.介绍、目的和应用

本数据处理协议（“**DPA**”）作为商业协议（“**Agreement**”）的一部分，适用于由在报价、订单确认或协议中指定的 Beamex 法律实体进行的个人数据处理，例如 Beamex Oy Ab 或其任何子公司（“**Processor**“），与提供数字或其他服务（“**Services**”）相关。向作为协议的合同方以及该个人数据的控制者（“**Controller**”）的客户提供的服务在处理者与控制者之间签订的协议中有更详细的描述。

本数据处理协议（DPA）构成双方之间协议不可分割且不可分离的一部分。本数据处理协议（DPA）中使用但未定义的所有术语具有与本协议相同的含义。
如果本协议与本数据处理协议（DPA）存在冲突，则以数据处理协议（DPA）的条款为准。

2.定义

控制者是指本数据处理协议中提到的自然人或法人、权威机构、代理机构或其他机构，单独或与他人共同定义个人数据处理的目的和方式。

数据保护法是指数据保护法案（1050/2018）和欧盟通用数据保护条例（2016/679），包括修订和替代法规，以及其他有效和适用的数据保护立法、指令和数据保护机构的具有约束力的规定。

数据主体是指在本数据处理协议 (DPA) 基础上处理其个人数据的已识别或可识别的自然人。

个人数据是指与已识别或可识别的自然人相关的任何信息；可识别的自然人被认为是可以直接或间接识别的自然人，特别是基于诸如姓名、社会安全号码、位置信息、在线识别信息或一个或多个物理特征等识别信息。, 生理的，遗传的，心理的，经济的, 他或她特有的文化或社会因素。

个人数据泄露是指导致个人数据意外或非法被销毁、丢失、篡改、未经授权披露或访问的数据安全事件，这些数据被传输、存储或以其他方式处理。

处理 是指在提供服务时，对个人数据或包含个人数据的数据集应用的功能，可以通过自动数据处理或手动方式进行，例如收集、存储。, 组织、结构化、存储、修改或更改, 搜索、查询、使用、传输数据, 分发或以其他方式提供、匹配或组合、限制、删除或销毁信息。

处理者是指在本数据处理协议中提到的代表控制者处理个人数据的自然人或法人、机构、机关或其他组织。

标准合同条款 指的是 2021年6月4日生效的标准合同条款（欧盟）2021/914。凡提及标准合同条款之处，均指本数据处理协议（DPA）中所载的标准合同条款，其中包括双方对某些模块和可选条款的选择以及本协议 DPA 中的附录一至附录二。 此外，双方同意，使用次级处理商应受标准合同条款第 9 条，选项 1 的管辖。

子处理者是指与处理者有合同关系的自然人或法人，作为处理者的分包商处理个人数据，以执行控制者的服务。

3.处理范围和处理活动范围

根据本数据处理协议（ DPA），处理此类个人数据时，控制方作为唯一的数据控制方。

处理者处理个人数据 (i) 根据数据保护法律和本 DPA 的条款履行协议中所述的义务；以及 (ii) 除非适用于处理方的数据保护法律另有要求，否则应遵守控制方不时给出的书面指示。除非本数据处理协议（DPA ）允许，否则处理方不得出于自身任何目的处理个人数据或将其转交给第三方。如果处理者认为或怀疑控制方的书面指示违反数据保护法律，则处理者必须通知控制方。除非本数据处理协议（DPA）或其附录另有约定，否则处理者只能在协议期限内处理个人数据。

控制器 (i) 承诺在处理个人数据时遵守适用于其数据保护法律的义务；以及 (ii) 作为唯一的数据控制方，其有权处理个人数据，并且已履行通知数据主体的义务，和 / 或已获得（或将获得）适用数据保护法要求的数据主体同意，以便处理方根据本 DPA 代表控制方处理个人数据。

有关处理的更详细信息，例如处理的性质、个人数据的类型和数据主体的群体，已在**附录 1** 中描述。
如果在处理过程中发生变化，可以更新附录。
但是，控制方承认并接受，作为向控制方提供服务的一部分，处理方有权出于其合法和合法的内部业务目的使用与服务的运营、支持或使用相关的信息，例如 (i) 根据使用情况或用户数量对服务开具发票，(ii) 服务的交付和管理其提供，(iii) 服务的功能和技术开发，(iv) 遵守适用法律（包括回应官方请求），(v) 确保服务的安全，以及 (vi) 防止欺诈和滥用或降低风险。如果此类信息是个人数据，则承诺 : (a) 按照适用的数据保护法律处理此类个人数据，并且仅出于与本节所述目的相符的目的 ; (b) 不将此类个人数据用于任何其他目的或披露给第三方，除非其事先已对数据进行匿名化处理，以便从数据中识别控制者或其他个人或实体。

4.分包商和次级处理商

处理者有权在处理中使用次级处理商。根据要求，处理者必须向控制方提供有关其使用次级处理商的更多信息。如果处理者对其次级处理商作出重大变更，则必须以书面形式通知控制方。 控制方有权出于正当理由禁止使用特定的次级处理商。如果控制方禁止使用特定的次级处理商，并且该次级处理商的任务不可能合理地转让给任何其他人，包括处理者，则处理者有权终止该数据处理协议（DPA）并结束处理。仅在处理结束且该数据处理协议（DPA）已终止（因为控制方禁止使用特定次级处理商）的情况下，控制方无权获得任何赔偿。

处理者必须与每个次级处理商签订书面协议，其中包含数据保护法律要求的条款和条件以及与处理者在本数据处理协议（DPA）下所承担的义务基本类似的类型。处理者对其所使用的次级处理商负责，就像处理者对其自己的行为负责一样。

5.数据安全

处理者必须采取适当的技术、物理和组织措施，以确保处理者处理个人数据时的高度安全，并保护个人数据免受未经授权或非法处理以及意外丢失、破坏、损坏、更改或传输。在评估确保安全水平的必要措施、控制方的指示、最新技术和实施成本时，, 处理的范围、背景和目的，以及对自然人权利和自由的风险，这些风险的可能性和严重性各不相同, 必须予以考虑。

适用的措施可能包括，例如： (i) 匿名化和加密个人数据； (ii) 能够保证系统和服务的持续保密性、完整性、可用性和容错性； (iii) 在发生物理或技术故障时，快速恢复个人数据可用性和访问个人数据的能力；以及 (iv) 定期测试、审查和评估技术和组织措施有效性的程序，以确保处理的安全。除非适用的数据保护法另有要求，否则处理者必须采取措施确保在处理者处工作的每个有权访问个人数据的自然人仅根据控制方的指示处理个人数据。处理者有责任根据自己的政策对其持有的控制方数据和文件进行备份，并检查其功能。

在不限制上述要求和义务的情况下，处理者必须始终实施至少与**附录 2** 中所述措施基本相对应的技术和组织信息安全措施。

6.保密性

在合理可行的范围内，处理者必须确保只有代表其行事且需要访问信息以实现本数据处理协议（DPA）目的的人员才能访问个人数据，并且确保有权处理个人数据的人员应承诺遵守保密义务或受适当的法律保密义务的约束。

7.国际数据传输

7.1 允许传输

处理者可能会将数据传输到欧盟或欧洲经济区以外的国家/地区。在向欧盟或欧洲经济区以外的国家传输数据时，处理者必须始终遵守数据保护法的条款和要求，例如使用欧盟委员会发布的适用于数据传输的标准合同条款。

7.2 欧洲经济区内的处理者和欧洲经济区以外的控制方

如果处理者位于欧洲经济区内，而控制方位于欧洲经济区外，则个人数据的传输应受标准合同条款模块 4 的管辖，这些标准合同条款以引用方式并入本协议，并构成该数据处理协议（DPA）不可分割的组成部分。控制方作为 “数据进口方” 和处理者作为 “数据出口方” 签署标准合同条款。

就实现标准合同条款目的而言：

a) 应适用第四模块；
b) 应适用可选的对接条款，即第 7 条；
c) 在第 11 条中，可选语言应予以删除；
d) 第 17 条，应适用芬兰的实质性法律；
e) 第 18 条，争议应在芬兰赫尔辛基地方法院解决；以及
f) 标准合同条款的附录应填写数据处理协议（DPA）约定的信息，包括其附录。

如果标准合同条款与本协议或数据处理协议（DPA）中有关从控制方向处理者传输个人数据的任何条款相冲突，则标准合同条款应以此类冲突的程度为准。

如果处理者位于欧洲经济区内并委托位于欧洲经济区外的次级处理商，则处理者应与该次级处理商签订标准合同条款（模块 3）。任何进一步的个人数据传输必须符合标准合同条款的适用模块。

8.个人数据泄露和报告义务

处理者必须在知晓所有实际或可疑的个人数据泄露后立即通知控制方。

处理者必须向控制方提供其所拥有的有关个人数据泄露的所有信息，控制方可能需要这些信息来履行自己的调查和报告义务。如果处理者没有立即获得有关违规的全面信息，则处理者可以稍后补充信息。除此之外，处理者必须协助并与控制方合作调查个人数据泄露以及与向当局和利益相关方通知相关的可能事项。处理者还必须采取必要的合理跟进措施，以减轻个人数据泄露的不利影响，修复已发生的违规或泄露，并防止未来违规。未经控制方明确书面同意和指示，处理者不得就个人数据泄露事件向第三方（尤其是媒体）发表任何评论，但数据保护法律另有要求的除外。

控制方自行最终决定是否必须向当局或其他相关方通知个人数据泄露，以及如何进行此类通知，但数据保护法律或主管当局的命令另有要求的除外。如果处理者向当局或其他利益相关方报告个人数据泄露，必须事先获得控制方的批准。

9.记录和审计权限

一方有义务向另一方提供证明遵守本数据处理协议（DPA）和数据保护法律所需的所有必要信息和文件。

根据控制方的要求，处理者还必须允许对处理、服务、信息安全措施以及处理者的信息系统和流程进行审计，并以合理的时间间隔参加此类审计，以确保遵守本数据处理协议（DPA）和数据保护法律。此类审计每年不得超过一次，除非有正当理由认为处理者未遵守本数据处理协议（DPA）或数据保护相关法律。审计还可能包括访问处理者的办公室或其他实体场所。审计在正常工作时间内进行，且审计方式不得对处理者的运营造成不必要的干扰。各方应自行承担与审计相关的费用。必须在计划审计前至少十五（15）天通知处理者计划的审计。控制方对审计期间获得的有关处理者活动的信息负有保密义务。

10.协助控制方

处理者必须根据控制方的要求，但由控制方支付费用，合理协助控制方履行控制方根据数据保护法律所承担的义务。协助义务尤其适用于以下事项：

10.1 访问个人数据

如果个人数据无法直接通过服务获得，处理者应根据要求向控制方提供相关数据。如果信息是以电子形式存在，则必须以该形式提供给控制方。

10.2 履行数据主体的权利和来自监管机构的请求

处理方必须立即通知控制方：(i) 监管机构或其他主管机构提出的所有请求、投诉或通知；以及 (ii) 直接从数据主体收到的与数据主体权利履行相关的任何请求。只有在控制方事先给予许可和指示的情况下，处理者才能直接响应请求。如果控制方要求，处理者必须合理协助控制方回应官方请求并履行数据主体根据数据保护法的权利。

10.3 数据保护影响评估

如果处理者发现计划中的处理会给自然人的权利和自由带来高风险，则必须通知控制方，并在必要时协助控制方进行数据保护影响评估。

10.4 个人数据的纠正、删除和限制

处理者必须：(i) 提供通过服务功能更正、删除或限制个人数据处理的可能性，或 (ii) 根据控制方的指示纠正、删除或限制个人数据的处理。

11.有效期和终止

11.1 生效和终止

除非另有约定，否则本数据处理协议（DPA）与协议同时生效，只要处理者在提供服务时处理控制方的个人数据，该协议（DPA 就一直有效。无论本数据处理协议（DPA）的终止情况如何，数据处理协议（DPA）的条款本质上都应在协议终止后仍然有效，而不管数据处理协议（DPA）的终止情况如何。

11.2 处理结束时返回或删除个人数据

在本数据处理协议（DPA）终止后，处理者必须根据控制方的选择删除代表控制方处理的所有个人数据，或者将所有个人数据返还给控制方并删除现有副本，除非数据保护法律或其他法规（例如 ISO 17025）要求保留个人数据。在这种情况下，处理者有权根据法律要求保留个人数据，而无需以其他方式继续处理个人数据，并且仍遵守本数据处理协议（DPA）所述的保密义务。个人数据的返还或删除必须在控制方提出请求后立即进行。如果控制方尚未就删除或返还个人数据给出任何指示，则处理者可在本数据处理协议（DPA）结束后十二（12）个月后主动删除其持有的个人数据。处理者必须以常用、数据安全的电子格式或双方约定的其他格式返还个人数据。

12.其他条款

12.1 变更

本数据处理协议（DPA）的所有更改必须在双方之间以书面形式达成一致。为清楚起见，数据控制方不时给出的执行个人数据处理的书面指示不被视为对本数据处理协议（DPA）的更改。

12.2 责任和义务

如果数据主体因违反数据保护法律而遭受损害，则应根据欧盟通用数据保护条例（2016/679）第 82 条确定控制方和处理者对损害的责任。每一方应对监管机构因违反数据保护法而可能施加的行政处罚负责。一方因违反本数据处理协议（DPA）合同而向另一方承担的损害赔偿责任的总额上限为在提交首次损害赔偿申请前六（6）个月根据协议支付的不含增值税服务费。在其他方面，双方协议或附件中可能包含的责任限制条款也适用于本数据处理协议（DPA）。除非本文另有明确规定，否则一方对另一方的任何间接、后果性、附带，特殊或惩罚性损害（包括业务中断和使用损失、数据损失、销售损失、收入损失或利润损失），特别是被排除在外的情况。

12.3 适用法律和争议解决

关于适用法律和争议解决，除非数据保护法律另有规定，否则应遵守双方之间的协议条款。如果协议未约定适用法律或包含争议解决条款，则数据处理协议（DPA）应受处理方所在地的实质法律管辖。

13.附录

本数据处理协议（DPA）由本文件和以下所列附件组成：

- 附录 1：处理操作的说明
- 附录 2：技术和组织信息安全措施

数据处理协议（DPA）附录 1（以及适用的标准合同条款）

A. 各方名单

数据输出方：

名称：Beamex Oy Ab

地址：Ristisuonraitti 10, 68600 Pietarsaari, FINLAND

与根据这些条款传输的数据相关的活动：贝美克斯是一家技术公司，为其工业客户制造和提供校准设备、软件及相关服务和支持。数据进口方是贝美克斯的客户，也是本数据处理协议（DPA）涉及的贝美克斯数字服务的用户。

角色（控制方 / 处理者）：处理者。

数据进口方：

名称：与 Beamex Oy Ab 签订的商业协议中约定的名称。

地址：如商业协议中所述。

与根据这些条款传输的数据相关的活动：数据进口方是使用贝美克斯数字服务的贝美克斯客户。

角色（控制方 / 处理者）：控制方。

签署数据处理协议（DPA）时处理者的主要次级处理商：

a) **微软数据中心荷兰有限公司**由于 Beamex Oy Ab 根据微软产品条款网站的规定订阅了西欧的 Azure 云服务 (PaaS)，因此数据处理和安全条款在微软在线服务数据保护附录 (DPA) 中进行了定义。
b) **Bjorkstrom Oy Ab** – 注册于芬兰，处理活动包括 LOGiCAL 的开发和部署。

B. 传输 / 处理说明

	贝美克斯数字服务和云软件（例如 LOGiCAL）	其他贝美克斯服务（例如软件支持、数据迁移、系统集成）
传输个人数据的数据主体的类别：	主要是使用贝美克斯校准设备进行校准的控制方的员工或分包商，然后将结果存储在 贝美克斯校准软件中。	主要是使用贝美克斯校准设备进行校准的控制方的员工或分包商，然后将结果存储在 贝美克斯校准软件中。
传输的个人数据的类别：	尤其是姓名、职位、雇主姓名以及与个人使用贝美克斯校准设备执行活动相关的数据。(注意：470 与471内容完全一样)	尤其是姓名、职位、雇主姓名以及与个人使用贝美克斯校准设备执行活动相关的数据。(注意：470 与471内容完全一样)
传输频率：	数据传输既是持续进行的，也会根据需要进行，以提供服务。	如有需要。
数据处理的性质：	向控制方提供贝美克斯校准软件的用户权限，并将校准数据存储在控制方员工和分包商执行校准的软件中。	为贝美克斯客户提供服务台、支持和维护服务，以及与软件产品相关的迁移和集成服务，在此期间可能涉及个人数据的处理。
数据传输和进一步处理的目的：	使用贝美克斯校准软件存储校准结果。	使贝美克斯的产品能够与其他系统结合使用、实施和 / 或运行。
个人数据的保留期限，或者如果无法保留，则确定该期限的标准：	商业协议的期限以及控制方使用贝美克斯数字服务的期限。	商业协议的期限以及贝美克斯作为数据处理方处理数据的期限。
主管监管机构：	数据保护专员办公室 (Tietosuojavaltuutetun toimisto) 街道地址：Lintulahdenkuja 4，00530 Helsinki，芬兰 总机：+358 29 566 6700，注册处 :+358 29 566 6768 www.tietosuoja.fi	

数据处理协议（DPA）附录 2（以及适用的标准合同条款）

除了数据处理协议（DPA）提到的一般义务外，处理者还必须实施的技术和组织措施的描述，以确保适当的数据安全水平。

区域	计划和实践
Microoft Azure (PaaS)	**Beamex LOGiCAL 和 Beamex Sync 服务基于 Azure (PaaS) 。微软服务信任门户列出了所有相关的业务连续性（ISO22301）和信息安全管理体系（ISO27001 及其他 27000 系列）认证、报告、文件等，地址为 https://servicetrust.microsoft.com/viewpage/ISOIEC**
场所和物理安全	**进入场所**处理者通过个人身份证 (射频识别（RFID）) 来控制对其场所的准入。根据管理层和主管定义的权限授予对场所内不同区域的访问权限。某些特殊区域可能采取增强的保护和访问控制措施。访客只能进入公共场所（大堂、餐厅、卫生间），并且只能在主人的陪同下进入处理者的场所。 **报警系统和设施防护。**场所保安外包给专业保安公司。场所设有行业标准报警系统，包括未经授权进入的报警、实验室状况监控、信息和通信技术数据中心的冷却 / 温度、空调系统报警和火灾报警系统。公司的技术服务经理负责门禁监控和报警系统的技术维护。员工均已接受相关培训，或者已经获取在各类警报或危机情况下如何操作的说明，某些情况下可以定期开展演练。
人员、组织和信息安全管理	**人员安全。**与员工签署的雇佣协议包含行业标准保密条款。在某些特殊情况下，会签署额外的保密协议（例如特定项目和 / 或信息）。员工还必须遵守处理者可能拥有的任何指南或政策，包括但不限于与商业道德、隐私和信息安全相关的指南或政策。 **培训和指南。**强制性信息安全培训是每位新员工入职计划的一部分。不时为员工组织额外的通用或特定信息安全培训。管理层、主管、系统所有者、访问控制和其他负责人已接受有关处理者信息安全政策培训，上述政策未来如有修订，也会有相应培训。此类许多人员还参与风险管理和业务连续性规划审查、培训和 / 或练习。关于员工的具体指南可能存在于多个方面，例如工作邮箱、远程访问和远程办公、工具和软件以及文件、文档和记录管理。 **管理、监控、审查和审核。**信息安全和业务连续性风险评估是公司质量体系审核的一部分。风险评估、检查和开发计划是根据发现、识别的风险单独制定的，并且始终与新的开发项目或计划系统 / 设施 / 流程变更相关联。在可能或必要的情况下，使用外部专家、同行评审或审核来评估技术信息的安全水平。公司的 ICT 职能部门管理信息安全框架，并负责许多实际和技术信息的安全措施。ICT 在公司的管理团队中设有代表。
业务连续性	处理者维护业务的连续性和灾难恢复的规划和措施。
第三方、分包商、处理者和次级处理商	**背景信息和合同。**在建立业务关系之前，根据需要检查第三方、分包商和次级处理商的背景。第三方合作伙伴受保密义务合同上的约束。与被视为处理者的数据处理方或次级处理商的合作伙伴签订书面数据处理协议（或附件）。如果相关，可以向处理者雇佣的第三方提供与信息安全相关的培训或指导。 **IT 采购。**计算机、移动设备、系统和软件主要由 IT 职能部门采购。许可证信息也由 IT 部门进行登记和保存。

贝美克斯内部数据、服务器和网络	**访问控制和身份验证。**处理者使用行业标准措施来验证个人和用户身份，限制对系统、软件、文件和数据的访问（以及防止未经授权的访问）。从远程连接登录网络时，主要需要双重身份验证。其目的是在应用程序中主要使用域单点登录。密码长度必须至少为 8 个字符，但最好使用包含特殊字符、数字和大写字母的 14 个字符的高强度密码。对某些文件的访问也可能受到系统、文件夹和文档特定访问权限的限制。 **电子邮箱。**存在电子邮箱通信指南。发送或接收机密信息时，需要考虑特殊的电子邮件安全问题。电子邮件服务器和终端设备（计算机、电话、平板电脑等）之间的连接 已加密。 **文件和数据库。**对于云端的数据存储，存在多种做法。不建议将重要数据保存到本地计算机硬盘上。处理方自有的本地服务器和系统用于保存敏感或高度机密信息。对于需要归档和存档保存或进行版本和生命周期管理的记录，存在单独的指南和实践。Sharefile 是以安全方式向第三方提供机密信息的主要工具。Microsoft Office365 广泛用于存储和共享文件，尤其是团队合作中使用的文件（非常敏感或高度机密信息除外）。 **远程连接。**主管确定移动工作所需的设备、软件和远程连接。使用远程办公所需的双重身份验证保护客户端 VPN 或 Citrix/XenApp。移动设备受到密码 / 代码保护，并在适用时受 MDM 控制。对于移动工作和在云中保存文件和记录，可能存在单独的政策。 **网络、服务器和 IT 基础设施。**数据网络分为单独的子网络 / 虚拟网络。使用适当的工具和 / 或服务进行流量监控、渗透防护与观测以及防病毒监控。某些数据连接和关键网络边缘组件采用冗余配置。目的是为所有关键组件配置冗余或备份设备，以降低数据网络、服务器、存储和其他关键系统中的所谓单点故障 (SPOF) 风险。为关键设备备件和组件建立了自有库存。有些关键系统和设备的供电由不间断电源（UPS）系统提供备份。关键信息系统可以使用高利用率 (HA) 存储系统、存储镜像或一些其他容错系统。根据适用的标准操作程序，定期对虚拟服务器、生产系统和其他一些关键用途的计算机进行镜像 / 系统备份。系统备份会根据具体情况和风险评估，在其他对象中实施。 **备份策略。**处理者拥有各种备份计划和措施，用于数据和系统的恢复。根据数据和系统的重要性，计划和措施可能有所不同。处理者对数据和信息系统的备份有单独的标准操作程序。 **恶意软件。**处理者维护防火墙以及防病毒、反恶意软件、垃圾邮件过滤和其他类似的技术措施，以检测、防止和保护其数据、系统、网络和设备免受外部网络的攻击、未经授权的访问和恶意软件的安装。

[DPA 结束。]]

Tietojenkäsittelysopimus (FI)

1. Johdanto, tarkoitus ja soveltaminen

Tätä tietojenkäsittelysopimusta ("DPA") sovelletaan osana kaupallista sopimusta ("Sopimus") henkilötietojen käsittelyyn, jota suorittaa tarjouksessa, tilausvahvistuksessa tai Sopimuksessa määritelty Beamexin oikeushenkilö, kuten Beamex Oy Ab tai jokin sen tytäryhtiöistä ("Käsittelijä"), digitaalisten tai muiden palveluiden ("Palvelut") tarjoamisen yhteydessä asiakkaalle, joka on Sopimuksen sopijapuoli sekä kyseisten henkilötietojen rekisterinpitäjä ("Rekisterinpitäjä"). Nämä Palvelut on kuvattu tarkemmin Käsittelijän ja Rekisterinpitäjän välillä solmitussa Sopimuksessa.

Tämä tietojenkäsittelysopimus on olennainen ja erottamaton osa osapuolten välistä Sopimusta. Kaikilla tässä tietojenkäsittelysopimuksessa käytetyillä termeillä, joita ei ole erikseen määritelty, on sama merkitys kuin Sopimuksessa.Jos Sopimuksen ja tämän tietojenkäsittelysopimuksen välillä on ristiriitaa, tietojenkäsittelysopimuksen ehdot ovat etusijalla.

2. Määritelmät

"Rekisterinpitäjä" tarkoittaa tässä tietojenkäsittelysopimuksessa mainittua luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

"Tietosuojalainsäädäntö" tarkoittaa tietosuojalakia (1050/2018) ja EU:n yleistä tietosuoja-asetusta (2016/679) niihin tehtyine muutoksineen ja korvaavine säädöksineen sekä muuta voimassa olevaa ja sovellettavaa tietosuojalainsäädäntöä ja tietosuojaviranomaisten ohjeita ja sitovia määräyksiä.

"Rekisteröity" tarkoittaa tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä, jonka henkilötietoja käsitellään tämän tietojenkäsittelysopimuksen perusteella.

"Henkilötiedot" tarkoittavat kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

"Henkilötietojen tietoturvaloukkaus" tarkoittaa tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy niihin.

"Käsittely" tarkoittaa toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin Palvelujen tarjoamisen yhteydessä joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, siirtämistä, levittämistä tai muuten saataville asettamista, yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

"Käsittelijä" tarkoittaa tässä tietojenkäsittelysopimuksessa mainittua luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja Rekisterinpitäjän lukuun.

"Vakiolausekkeet" tarkoittavat 4. kesäkuuta 2021 annettuja vakiolausekkeita (EU) 2021/914. Kaikki viittaukset vakiolausekkeisiin tarkoittavat vakiolausekkeita, jotka sisältävät osapuolten valinnat tiettyjen moduulien ja valinnaisten lausekkeiden osalta sekä tämän tietojenkäsittelysopimuksen liitteet I–II. Lisäksi osapuolet sopivat, että alikäsittelijöiden käyttöön sovelletaan vakiolausekkeiden lausekkeen 9 vaihtoehtoa 1.

"Alikäsittelijä" tarkoittaa luonnollista henkilöä tai oikeushenkilöä, jolla on sopimussuhde Käsittelijään ja joka käsittelee henkilötietoja Käsittelijän alihankkijana osana Palvelujen suorittamista Rekisterinpitäjälle.

3. Käsittelyn laajuus ja käsittelytoimet

Tämän tietojenkäsittelysopimuksen mukaisesti käsitellään sellaisia henkilötietoja, joiden osalta Rekisterinpitäjä toimii ainoana rekisterinpitäjänä.

Käsittelijä käsittelee henkilötietoja (i) tietosuojalainsäädännön ja tämän tietojenkäsittelysopimuksen ehtojen mukaisesti täyttääkseen Sopimuksessa kuvatut velvoitteensa; ja (ii) noudattaen Rekisterinpitäjän kulloinkin antamia kirjallisia ohjeita, ellei Käsittelijään sovellettava tietosuojalainsäädäntö toisin vaadi. Käsittelijä ei saa

käsitellä henkilötietoja mihinkään omiin tarkoituksiinsa tai luovuttaa niitä kolmansille osapuolille, ellei tämä tietojenkäsittelysopimus sitä salli.Käsittelijän on ilmoitettava Rekisterinpitäjälle, jos se katsoo tai epäilee, että Rekisterinpitäjän kirjalliset ohjeet rikkovat tietosuojalainsäädäntöä. Ellei tässä tietojenkäsittelysopimuksessa tai sen liitteissä toisin määrätä, Käsittelijä saa käsitellä henkilötietoja vain Sopimuksen voimassaoloajan.

Rekisterinpitäjä (i) sitoutuu noudattamaan siihen sovellettavan tietosuojalainsäädännön mukaisia velvoitteita henkilötietojen käsittelyssä; ja (ii) vastaa siitä, että sillä on ainoana rekisterinpitäjänä oikeus käsitellä henkilötietoja ja että se on täyttänyt velvollisuutensa informoida rekisteröityjä ja/tai saanut (tai tulee saamaan) rekisteröidyiltä kaikki sovellettavan tietosuojalainsäädännön edellyttämät suostumukset siihen, että Käsittelijä käsittelee henkilötietoja Rekisterinpitäjän lukuun tämän tietojenkäsittelysopimuksen mukaisesti.

Tarkemmat tiedot käsittelystä, kuten käsittelyn luonne, henkilötietojen tyypit ja rekisteröityjen ryhmät, on kuvattu Liitteessä 1. Liitettä voidaan päivittää, jos käsittelyssä tapahtuu muutoksia.

Rekisterinpitäjä kuitenkin ymmärtää ja hyväksyy, että osana Palvelujen tarjoamista Rekisterinpitäjälle, Käsittelijällä on oikeus käyttää Palvelun toimintaan, tukeen tai käyttöön liittyviä tai sen yhteydessä saatuja tietoja laillisiin ja oikeutettuihin sisäisiin liiketoimintatarkoituksiinsa, kuten (i) Palvelun laskutukseen käytön tai käyttäjämäärän perusteella, (ii) Palvelun toimittamiseen ja sen tarjoamisen hallinnointiin, (iii) Palvelun toiminnalliseen ja tekniseen kehittämiseen, (iv) sovellettavien lakien noudattamiseen (mukaan lukien viranomaisten pyyntöihin vastaaminen), (v) Palvelun turvallisuuden varmistamiseen ja (vi) petosten ja väärinkäytösten estämiseen tai riskien vähentämiseen. Siltä osin kuin tällaiset tiedot ovat henkilötietoja, Käsittelijä sitoutuu siihen, että: (a) se käsittelee tällaisia henkilötietoja sovellettavan tietosuojalainsäädännön mukaisesti ja vain tarkoituksiin, jotka ovat yhteensopivia tässä osiossa kuvattujen tavoitteiden kanssa; ja (b) se ei käytä tällaisia henkilötietoja mihinkään muuhun tarkoitukseen tai luovuta niitä kolmansille osapuolille, ellei se ole ensin anonymisoinut tietoja siten, ettei Rekisterinpitäjää tai ketään muuta henkilöä tai tahoa voida tunnistaa tiedoista.

4. Alihankkijat ja alikäsittelijät

Käsittelijällä on oikeus käyttää alikäsittelijöitä Käsittelyssä. Pyynnöstä Käsittelijän on annettava Rekisterinpitäjälle lisätietoja käyttämistään alikäsittelijöistä. Jos Käsittelijä tekee merkittäviä muutoksia alikäsittelijöihinsä, sen on ilmoitettava asiasta kirjallisesti Rekisterinpitäjälle. Rekisterinpitäjällä on oikeus perustellusta syystä kieltää tietyn alikäsittelijän käyttö. Jos Rekisterinpitäjä kieltää tietyn alikäsittelijän käytön eikä kyseisen alikäsittelijän tehtäviä ole kohtuudella mahdollista siirtää kenellekään muulle, Käsittelijä mukaan lukien, Käsittelijällä on oikeus irtisanoa tietojenkäsittelysopimus ja lopettaa Käsittely. Rekisterinpitäjällä ei ole oikeutta minkäänlaiseen korvaukseen pelkästään sillä perusteella, että Käsittely päättyy ja tietojenkäsittelysopimus on irtisanottu sen vuoksi, että Rekisterinpitäjä on kieltänyt tietyn alikäsittelijän käytön.

Käsittelijän on tehtävä jokaisen alikäsittelijän kanssa kirjallinen sopimus, joka sisältää tietosuojalainsäädännön edellyttämät ehdot ja olennaisesti samankaltaiset velvoitteet kuin Käsittelijällä on tämän tietojenkäsittelysopimuksen nojalla. Käsittelijä on vastuussa käyttämistään alikäsittelijöistä samalla tavalla kuin omasta toiminnastaan.

5. Tietoturva

Käsittelijän on toteutettava asianmukaiset tekniset, fyysiset ja organisatoriset toimenpiteet varmistaakseen Käsittelijän suorittaman henkilötietojen käsittelyn korkean turvallisuustason ja suojatakseen henkilötietoja luvattomalta tai laittomalta käsittelyltä sekä tahattomalta häviämiseltä, tuhoutumiselta, vahingoittumiselta, muuttamiselta tai siirrolta.Turvallisuustason takaamiseksi tarvittavia toimenpiteitä arvioitaessa on otettava huomioon Rekisterinpitäjän ohjeet, uusin tekniikka ja toteutuskustannukset, Käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit, joiden todennäköisyys ja vakavuus vaihtelevat.

Sovellettavia toimenpiteitä voivat olla esimerkiksi:

i. henkilötietojen pseudonymisointi ja salaus;
ii. kyky taata järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, saatavuus ja vikasietoisuus;
iii. kyky palauttaa nopeasti henkilötietojen saatavuus ja pääsy niihin fyysisen tai teknisen vian sattuessa; ja
iv. menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen

toimenpiteiden tehokkuutta Käsittelyn turvallisuuden varmistamiseksi.

Käsittelijän on ryhdyttävä toimenpiteisiin varmistaakseen, että jokainen Käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä vain Rekisterinpitäjän ohjeiden mukaisesti, ellei sovellettava tietosuojalainsäädäntö toisin vaadi. Käsittelijä on omien käytäntöjensä mukaisesti vastuussa hallussaan olevien Rekisterinpitäjän tietojen ja tiedostojen varmuuskopioiden ottamisesta ja niiden toimivuuden tarkistamisesta.

Rajoittamatta edellä kuvattuja vaatimuksia ja velvoitteita, Käsittelijän on aina toteutettava vähintään sellaiset tekniset ja organisatoriset tietoturvatoimenpiteet, jotka vastaavat olennaisesti Liitteessä 2 kuvattuja toimenpiteitä.

6. Luottamuksellisuus

Käsittelijän on varmistettava, siinä määrin kuin on kohtuudella mahdollista, että vain sellaisilla sen puolesta toimivilla henkilöillä, joiden on välttämätöntä päästä tietoihin tämän tietojenkäsittelysopimuksen tarkoituksen toteuttamiseksi, on pääsy henkilötietoihin, ja että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus.

7. Kansainväliset tiedonsiirrot

7.1 Sallitut siirrot

Käsittelijä voi siirtää tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolella olevaan maahan. Käsittelijän on aina noudatettava tietosuojalainsäädännön ehtoja ja vaatimuksia siirtäessään tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolisiin maihin, esimerkiksi käyttämällä EU:n komission julkaisemia, tiedonsiirtoon sovellettavia vakiolausekkeita.

7.2 Käsittelijät ETA-alueella ja Rekisterinpitäjä ETA-alueen ulkopuolella

Jos Käsittelijä sijaitsee ETA-alueen sisällä ja Rekisterinpitäjä ETA-alueen ulkopuolella, henkilötietojen siirtoon sovelletaan vakiolausekkeiden moduulia 4, joka sisällytetään tähän viittauksella ja on olennainen osa tietojenkäsittelysopimusta. Rekisterinpitäjä solmii vakiolausekkeet "tiedontuojana" ja Käsittelijä "tiedonviejänä".

Vakiolausekkeita sovellettaessa:

i. sovelletaan moduulia 4;
ii. sovelletaan valinnaista liittymislauseketta, lauseke 7;
iii. lausekkeessa 11 valinnainen teksti poistetaan;
iv. lausekkeessa 17 sovelletaan Suomen aineellista lainsäädäntöä;
v. lausekkeen 18 mukaisesti riidat ratkaistaan Helsingin käräjäoikeudessa, Suomessa; ja
vi. vakiolausekkeiden liitteet täydennetään tietojenkäsittelysopimuksessa, mukaan lukien sen liitteissä, esitetyillä tiedoilla.

Jos ja siltä osin kuin vakiolausekkeet ovat ristiriidassa minkä tahansa Sopimuksen tai tietojenkäsittelysopimuksen ehdon kanssa koskien henkilötietojen siirtoa Rekisterinpitäjältä Käsittelijälle, vakiolausekkeet ovat etusijalla tällaisen ristiriidan osalta.

Jos Käsittelijä sijaitsee ETA-alueen sisällä ja valtuuttaa ETA-alueen ulkopuolella sijaitsevan alikäsittelijän, Käsittelijän on solmittava vakiolausekkeet (Moduuli 3) kyseisen alikäsittelijän kanssa. Kaikkien edelleen tapahtuvien henkilötietojen siirtojen on noudatettava sovellettavaa vakiolausekkeiden moduulia.

8. Henkilötietojen tietoturvaloukkaukset ja ilmoitusvelvollisuudet

Käsittelijän on ilmoitettava Rekisterinpitäjälle kaikista todellisista tai epäillyistä henkilötietojen tietoturvaloukkauksista ilman aiheetonta viivytystä saatuaan loukkauksen tietoonsa.

Käsittelijän on toimitettava Rekisterinpitäjälle kaikki saatavilla olevat tiedot henkilötietojen tietoturvaloukkauksesta, joita Rekisterinpitäjä saattaa tarvita omien tutkinta- ja ilmoitusvelvollisuuksiensa täyttämiseen. Käsittelijä voi täydentää tietoja myöhemmin, jos sillä ei ole välittömästi saatavilla kattavia tietoja loukkauksesta. Käsittelijän on muutenkin avustettava ja tehtävä yhteistyötä Rekisterinpitäjän kanssa henkilötietojen tietoturvaloukkauksen tutkinnassa sekä mahdollisissa viranomaisille ja asianosaisille tehtäviin ilmoituksiin liittyvissä asioissa. Käsittelijän on myös toteutettava tarpeelliset kohtuulliset jatkotoimenpiteet henkilötietojen tietoturvaloukkauksen haitallisten vaikutusten lieventämiseksi, tapahtuneen loukkauksen tai rikkomuksen korjaamiseksi ja tulevien loukkausten estämiseksi. Käsittelijä ei saa kommentoida henkilötietojen tietoturvaloukkausta kolmansille osapuolille, erityisesti tiedotusvälineiden edustajille, ilman Rekisterinpitäjän nimenomaista kirjallista

suostumusta ja ohjeita, ellei tietosuojalainsäädäntö toisin vaadi.

Ellei tietosuojalainsäädäntö tai toimivaltaisen viranomaisen määräys toisin vaadi, Rekisterinpitäjä tekee lopullisen päätöksen oman harkintansa mukaan siitä, onko henkilötietojen tietoturvaloukkauksesta ilmoitettava viranomaisille tai muille osapuolille, sekä mahdollisesta tavasta tehdä tällaiset ilmoitukset. Jos Käsittelijä ilmoittaa henkilötietojen tietoturvaloukkauksesta viranomaisille tai muille asianosaisille, Rekisterinpitäjän on hyväksyttävä ne etukäteen.

9. Dokumentointi- ja auditointioikeudet

Osapuolella on velvollisuus asettaa toisen osapuolen saataville kaikki vaaditut tiedot ja asiakirjat, jotka ovat tarpeen tämän tietojenkäsittelysopimuksen ja tietosuojalainsäädännön noudattamisen osoittamiseksi.

Rekisterinpitäjän pyynnöstä Käsittelijän on myös sallittava Käsittelyn, Palveluiden, tietoturvatoimenpiteiden sekä Käsittelijän tietojärjestelmien ja -prosessien auditoinnit ja osallistuttava kohtuullisin väliajoin tällaisiin auditointeihin tämän tietojenkäsittelysopimuksen ja tietosuojalainsäädännön noudattamisen varmistamiseksi. Tällaisia auditointeja saa suorittaa enintään kerran vuodessa, ellei ole perusteltua syytä olettaa, että Käsittelijä ei noudata tietojenkäsittelysopimusta tai tietosuojalainsäädäntöä. Auditoinnit voivat sisältää myös vierailuja Käsittelijän toimistoissa tai muissa fyysisissä tiloissa. Auditointi suoritetaan normaalin työajan puitteissa ja siten, ettei se häiritse tarpeettomasti Käsittelijän toimintaa.Kumpikin osapuoli vastaa omista auditointiin liittyvistä kuluistaan. Suunnitelluista auditoinneista on ilmoitettava Käsittelijälle vähintään viisitoista (15) päivää ennen aiottua auditointia. Rekisterinpitäjän auditoinnin aikana saamat tiedot Käsittelijän toiminnasta ovat luottamuksellisia.

10. Rekisterinpitäjän avustaminen

Käsittelijän on Rekisterinpitäjän pyynnöstä ja kustannuksella kohtuudella avustettava Rekisterinpitäjää noudattamaan tietosuojalainsäädännön mukaisia rekisterinpitäjien velvoitteita. Avustamisvelvollisuus koskee erityisesti seuraavia asioita:

10.1 Pääsy henkilötietoihin

Siltä osin kuin henkilötiedot eivät ole saatavilla suoraan Palveluiden kautta, Käsittelijän on pyynnöstä toimitettava kyseiset tiedot Rekisterinpitäjälle. Jos tiedot ovat saatavilla sähköisessä muodossa, ne on myös toimitettava Rekisterinpitäjälle kyseisessä muodossa.

10.2 Rekisteröityjen oikeuksien toteuttaminen ja valvontaviranomaisen pyynnöt

Käsittelijän on ilmoitettava Rekisterinpitäjälle viipymättä: (i) kaikista valvontaviranomaisen tai muun toimivaltaisen viranomaisen esittämistä pyynnöistä, valituksista tai ilmoituksista; ja (ii) kaikista suoraan rekisteröidyltä saaduista pyynnöistä, jotka liittyvät rekisteröidyn oikeuksien toteuttamiseen. Käsittelijä saa vastata suoraan pyyntöön vain, jos Rekisterinpitäjä on antanut siihen etukäteen luvan ja ohjeet. Jos Rekisterinpitäjä niin pyytää, Käsittelijän on kohtuudella avustettava Rekisterinpitäjää viranomaisten pyyntöihin vastaamisessa ja rekisteröidyn oikeuksien toteuttamisessa tietosuojalainsäädännön mukaisesti.

10.3 Tietosuojan vaikutustenarviointi

Jos Käsittelijä tulee tietoiseksi siitä, että suunniteltu Käsittely aiheuttaisi suuren riskin luonnollisen henkilön oikeuksien ja vapauksien kannalta, sen on ilmoitettava tästä Rekisterinpitäjälle ja tarvittaessa avustettava Rekisterinpitäjää tietosuojaa koskevan vaikutustenarvioinnin tekemisessä.

10.4 Henkilötietojen oikaiseminen, poistaminen ja rajoittaminen

Käsittelijän on joko (i) tarjottava mahdollisuus oikaista, poistaa tai rajoittaa henkilötietojen käsittelyä Palvelun toimintojen kautta tai (ii) oikaistava, poistettava tai rajoitettava henkilötietojen käsittelyä Rekisterinpitäjän ohjeiden mukaisesti.

11. Voimassaolo ja irtisanominen

11.1 Voimaantulo ja irtisanominen

Ellei toisin ole sovittu, tämä tietojenkäsittelysopimus astuu voimaan samanaikaisesti Sopimuksen kanssa ja pysyy voimassa niin kauan kuin Käsittelijä käsittelee Rekisterinpitäjän henkilötietoja Palveluidensa tarjoamisen yhteydessä.Riippumatta tietojenkäsittelysopimuksen irtisanomisesta, ne tietojenkäsittelysopimuksen määräykset, jotka ovat luonteeltaan sellaisia, että niiden on tarkoitus pysyä voimassa Sopimuksen irtisanomisesta riippumatta,

pysyvät voimassa tietojenkäsittelysopimuksen irtisanomisesta huolimatta.

11.2 Henkilötietojen palauttaminen tai poistaminen käsittelyn päättyessä

Tietojenkäsittelysopimuksen päättyessä Käsittelijän on Rekisterinpitäjän valinnan mukaan joko poistettava kaikki Rekisterinpitäjän puolesta käsitellyt henkilötiedot tai vaihtoehtoisesti palautettava kaikki henkilötiedot Rekisterinpitäjälle ja poistettava olemassa olevat kopiot, ellei tietosuojalainsäädäntö tai muu säännös (esim. ISO 17025) edellytä henkilötietojen säilyttämistä. Siinä tapauksessa Käsittelijällä on oikeus säilyttää henkilötiedot lain vaatimusten mukaisesti jatkamatta muuten henkilötietojen Käsittelyä ja noudattaen edelleen tässä tietojenkäsittelysopimuksessa kuvattuja salassapitovelvoitteita. Henkilötietojen palauttaminen tai poistaminen on suoritettava ilman aiheetonta viivytystä Rekisterinpitäjän pyynnön jälkeen. Jos Rekisterinpitäjä ei ole antanut ohjeita henkilötietojen poistamisesta tai palauttamisesta, Käsittelijä voi omasta aloitteestaan poistaa hallussaan olevat henkilötiedot, kun kaksitoista (12) kuukautta on kulunut tietojenkäsittelysopimuksen päättymisestä. Käsittelijän on palautettava henkilötiedot yleisesti käytetyssä, tietoturvallisessa sähköisessä muodossa tai muussa osapuolten sopimassa muodossa.

12. Muut ehdot

12.1 Muutokset

Kaikista tähän tietojenkäsittelysopimukseen tehtävistä muutoksista on sovittava kirjallisesti osapuolten välillä. Selvyyden vuoksi todetaan, että Rekisterinpitäjän kulloinkin antamia kirjallisia ohjeita henkilötietojen käsittelyn suorittamiseksi ei pidetä muutoksina tähän tietojenkäsittelysopimukseen.

12.2 Vastuut ja vahingonkorvausvelvollisuus

Jos rekisteröidylle aiheutuu vahinkoa tietosuojalainsäädännön rikkomisen vuoksi, Rekisterinpitäjän ja Käsittelijän vastuu vahingosta määräytyy EU:n yleisen tietosuoja-asetuksen (2016/679) 82 artiklan mukaisesti. Kumpikin osapuoli on vastuussa mahdollisista hallinnollisista sakoista, joita valvontaviranomainen on määrännyt tietosuojalainsäädännön rikkomisen perusteella. Osapuolen vahingonkorvausvastuu toiselle osapuolelle tämän tietojenkäsittelysopimuksen sopimusrikkomuksen perusteella on kokonaisuudessaan enimmäismäärä, joka vastaa Sopimuksen perusteella maksettuja arvonlisäverottomia palvelumaksuja ensimmäisen vahingonkorvausvaatimuksen esittämistä edeltävältä kuudelta (6) kuukaudelta. Muilta osin osapuolten väliseen Sopimukseen tai sen liitteisiin mahdollisesti sisältyvät vastuunrajoitusehdot koskevat myös tätä tietojenkäsittelysopimusta. Ellei tässä nimenomaisesti toisin mainita, kumpikaan osapuoli ei ole vastuussa toiselle osapuolelle mistään epäsuorista, välillisistä, satunnaisista, erityisistä tai rangaistusluonteisista vahingoista (mukaan lukien vahingot liiketoiminnan keskeytymisestä ja käytön, tietojen, myynnin, tulojen tai voiton menetyksestä), jotka on nimenomaisesti suljettu pois.

12.3 Sovellettava laki ja riitojen ratkaisu

Sovellettavan lain ja riitojen ratkaisun osalta noudatetaan osapuolten välisen Sopimuksen ehtoja, ellei tietosuojalainsäädäntö toisin määrää. Jos Sopimuksessa ei ole määritelty sovellettavaa lakia tai se ei sisällä riitojenratkaisuehtoja, tietojenkäsittelysopimukseen sovelletaan Käsittelijän kotipaikan aineellista lainsäädäntöä.

13. Liitteet

Tämä tietojenkäsittelysopimus koostuu tästä asiakirjasta ja alla luetelluista liitteistä:

- Liite 1: Kuvaus käsittelytoimista
- Liite 2: Tekniset ja organisatoriset tietoturvatoimenpiteet

Tietojenkäsittelysopimuksen liite 1 (ja soveltuvin osin vakiolausekkeiden)

A. OSAPUOLET

Tiedonviejä:

Nimi: Beamex Oy Ab

Osoite: Ristisuonraitti 10, 68600 Pietarsaari, SUOMI

Näiden lausekkeiden mukaisesti siirrettäviin tietoihin liittyvät toiminnot: Beamex on teknologiayritys, joka valmistaa ja tarjoaa kalibrointilaitteita, ohjelmistoja ja niihin liittyviä palveluita ja tukea teollisuusasiakkailleen. Tiedontuoja on Beamexin asiakas ja Beamexin digitaalisten palveluiden käyttäjä, joita tämä tietojenkäsittelysopimus koskee.

Rooli (rekisterinpitäjä/käsittelijä): käsittelijä

Tiedontuoja(t):

Nimi: Beamex Oy Ab:n kanssa solmitussa kaupallisessa sopimuksessa ilmoitettu nimi.

Osoite: kuten kaupallisessa sopimuksessa on ilmoitettu.

Näiden lausekkeiden mukaisesti siirrettäviin tietoihin liittyvät toiminnot: Tiedontuoja on Beamexin asiakas, joka käyttää Beamexin digitaalisia palveluita.

Rooli (rekisterinpitäjä/käsittelijä): rekisterinpitäjä

Käsittelijän olennaiset alikäsittelijät tietojenkäsittelysopimuksen solmimishetkellä:

a) **Microsoft Datacenter Netherlands B.V.** Azure-pilvipalvelut (PaaS) – Länsi-Eurooppa Microsoftin tuote-ehtosivuston (Microsoft Product Terms) ehtojen mukaisesti, tietojenkäsittely- ja tietoturvaehdot on määritelty Microsoft Online Services Data Protection Addendum (DPA) -asiakirjassa.

b) **Bjorkstrom Oy Ab** – kotipaikka Suomi, käsittelytoimiin kuuluu LOGiCALin kehitys ja käyttöönotto.

B. KUVAUS SIIRROSTA/KÄSITTELYSTÄ

	Beamexin digitaaliset palvelut ja pilviohjelmistot (esim. LOGiCAL)	**Muut Beamex-palvelut (esim. ohjelmistotuki, tiedonsiirto, järjestelmäintegraatio)**
Rekisteröityjen ryhmät, joiden henkilötietoja siirretään:	Pääasiassa sellaiset rekisterinpitäjän työntekijät tai alihankkijat, jotka käyttävät ja suorittavat kalibrointeja Beamexin kalibrointilaitteilla, joiden tulokset sitten tallennetaan Beamexin kalibrointiohjelmistoon.	Pääasiassa sellaiset rekisterinpitäjän työntekijät tai alihankkijat, jotka käyttävät ja suorittavat kalibrointeja Beamexin kalibrointilaitteilla, joiden tulokset sitten tallennetaan Beamexin kalibrointiohjelmistoon.
Henkilötietoryhmät, joita siirto koskee:	Erityisesti nimi, tehtävänimike, työnantajan nimi sekä tiedot toiminnoista, joita henkilö on suorittanut Beamexin kalibrointilaitteilla.	Erityisesti nimi, tehtävänimike, työnantajan nimi sekä tiedot toiminnoista, joita henkilö on suorittanut Beamexin kalibrointilaitteilla.
Siirron tiheys:	Tietoja siirretään sekä jatkuvasti että tarpeen mukaan palvelun/palveluiden tarjoamiseksi.	Tarpeen mukaan.
Käsittelyn luonne:	Beamexin kalibrointiohjelmiston käyttöoikeuksien tarjoaminen rekisterinpitäjälle ja rekisterinpitäjän työntekijöiden ja alihankkijoiden suorittamien kalibrointien kalibrointitietojen tallentaminen ohjelmistoon.	Helpdesk-, tuki- ja ylläpitopalveluiden tarjoaminen Beamexin asiakkaille sekä ohjelmistotuotteisiin liittyvien migraatio- ja integraatiopalveluiden tarjoaminen, joiden aikana henkilötietojen käsittelyä voi tapahtua.
Tiedonsiirron ja myöhemmän käsittelyn tarkoitus (tarkoitukset):	Beamexin kalibrointiohjelmiston käyttö kalibrointitulosten tallentamiseen.	Mahdollistaa Beamexin tuotteiden käytön, niiden käyttöönoton ja/tai niiden toiminnan yhdessä muiden järjestelmien kanssa.
Aika, jonka henkilötietoja säilytetään, tai jos se ei ole mahdollista, perusteet, joita käytetään kyseisen ajan määrittämiseksi:	Kaupallisen sopimuksen voimassaoloaika ja niin kauan kuin rekisterinpitäjä käyttää Beamexin digitaalisia palveluita.	Kaupallisen sopimuksen voimassaoloaika ja niin kauan kuin Beamex käsittelee tietoja henkilötietojen käsittelijänä näihin tarkoituksiin.
VALVONTAVIRANOMAINEN:	Tietosuojavaltuutetun toimisto Lintulahdenkuja 4, 00530 Helsinki +358 29 566 6700 www.tietosuoja.fi	

Tietojenkäsittelysopimuksen liite 2 (ja soveltuvin osin vakiolausekkeiden)

Kuvaus teknisistä ja organisatorisista toimenpiteistä, jotka Käsittelijän on toteutettava tietojenkäsittelysopimuksessa mainittujen yleisten velvoitteiden lisäksi asianmukaisen tietoturvatason varmistamiseksi.

Alue	Suunnitelmat ja käytännöt
Microoft Azure (PaaS)	**Beamex LOGiCAL ja Beamex Sync -palvelut on rakennettu Azuren (PaaS) päälle. Microsoft Service Trust -portaali listaa kaikki asiaankuuluvat liiketoiminnan jatkuvuuden (ISO22301) ja tietoturvan hallintajärjestelmän (ISMS) (ISO27001 ja muut 27000-sarjan) sertifikaatit, raportit, asiakirjat jne. osoitteessa https://servicetrust.microsoft.com/viewpage/ISOIEChttps://servicetrust.microsoft.com/viewpage/ISOIEC**
Tilat ja fyysinen turvallisuus	**Pääsy tiloihin.** Käsittelijä rajoittaa pääsyä tiloihinsa henkilökohtaisilla henkilökorteilla (RFID). Pääsyoikeudet tilojen eri alueille myönnetään johdon ja esimiesten määrittelemien oikeuksien perusteella. Tietyillä erityisalueilla voi olla tehostettuja suojaus- ja kulunvalvontatoimenpiteitä. Vierailla on pääsy vain julkisiin tiloihin (aula, ruokala, wc-tilat) ja he liikkuvat Käsittelijän tiloissa vain isännän seurassa. **Hälytysjärjestelmät ja tilojen vartiointi.** Tilojen vartiointi on ulkoistettu ammattimaiselle vartiointiliikkeelle. Tiloissa on alan standardien mukaiset hälytysjärjestelmät, mukaan lukien hälytykset luvattomasta pääsystä, laboratorio-olosuhteiden valvonta, ICT-konesalien jäähdytys/lämpötila, ilmastointijärjestelmän hälytykset ja palohälytysjärjestelmät. Yrityksen teknisten palveluiden päällikkö vastaa kulunvalvonta- ja hälytysjärjestelmien teknisestä ylläpidosta. Työntekijät on koulutettu tai heillä on saatavilla ohjeet siitä, miten toimia erilaisissa hälytys- tai kriisitilanteissa; tiettyjä tilanteita saatetaan harjoitella säännöllisesti.
Henkilöstö, organisaatio ja tietoturvan hallinta	**Henkilöstön turvallisuus.** Työntekijöiden kanssa allekirjoitetut työsopimukset sisältävät alan standardien mukaisen salassapitolausekkeen. Tietyissä erityistilanteissa voidaan allekirjoittaa ylimääräisiä salassapitosopimuksia (esim. erityiset projektit ja/tai tiedot). Työntekijöiden on myös noudatettava kaikkia Käsittelijän mahdollisia ohjeita tai käytäntöjä, mukaan lukien rajoituksetta ne, jotka liittyvät liiketoiminnan etiikkaan, yksityisyyteen ja tietoturvaan. **Koulutus ja ohjeet.** Pakollinen tietoturvakoulutus on osa jokaisen uuden työntekijän perehdytysohjelmaa. Työntekijöille järjestetään ajoittain ylimääräistä yleistä tai erityistä tietoturvakoulutusta. Johto, esimiehet, järjestelmien omistajat, kulunvalvonnasta ja muista asioista vastaavat henkilöt koulutetaan Käsittelijän tietoturvapolitiikan sisältöön ja sen tuleviin päivityksiin.Monet tällaisista henkilöistä osallistuvat myös riskienhallinnan ja liiketoiminnan jatkuvuussuunnittelun katselmuksiin, koulutukseen ja/tai harjoituksiin. Työntekijöille voi olla erityisiä ohjeita eri aloilla, kuten työsähköpostin käyttö, etäkäyttö ja etätyö, työkalut ja ohjelmistot sekä tiedostojen, asiakirjojen ja tallenteiden hallinta. **Hallinta, valvonta, katselmukset ja auditoinnit.** Tietoturva- ja liiketoiminnan jatkuvuusriskien arviointi on osa yrityksen laatujärjestelmän auditointeja.Havaintojen, tunnistettujen riskien ja aina uusien kehityshankkeiden tai järjestelmä-/tila-/prosessimuutosten suunnittelun yhteydessä tehdään erillisiä riskiarviointeja, tarkastuksia ja kehityssuunnitelmia. Teknisen tietoturvatason arviointiin käytetään mahdollisuuksien tai tarpeen mukaan ulkopuolisia asiantuntijoita, vertaisarviointeja tai auditointeja. Yrityksen ICT-toiminto hallinnoi tietoturvan viitekehystä ja vastaa monista käytännön ja teknisistä tietoturvatoimenpiteistä. ICT on edustettuna yrityksen johtoryhmässä.
Business continuity	Käsittelijä ylläpitää suunnitelmia ja toimenpiteitä liiketoiminnan jatkuvuuden ja katastrofipalautuksen varmistamiseksi.
Kolmannet osapuolet, alihankkijat, käsittelijät ja alikäsittelijät	**Taustaselvitykset ja sopimukset.** Kolmansien osapuolten, alihankkijoiden ja alikäsittelijöiden taustat tarkistetaan tarkoituksenmukaiseksi ja tarpeelliseksi katsotulla tavalla ennen liikesuhteen solmimista. Kolmannen osapuolen kumppaneita sitovat sopimukseen perustuvat salassapitovelvoitteet. Kirjalliset tietojenkäsittelysopimukset (tai liitteet) solmitaan sellaisten kumppaneiden kanssa, joita pidetään Käsittelijän tietojenkäsittelijöinä tai alikäsittelijöinä. Käsittelijän työllistämille kolmansille osapuolille voidaan tarpeen mukaan tarjota myös tietoturvaan liittyvää koulutusta tai ohjeistusta. **IT-hankinnat.** Tietokoneet, mobiililaitteet, järjestelmät ja ohjelmistot hankkii ensisijaisesti IT-toiminto.Lisenssitiedot rekisteröidään ja tallennetaan myös IT:n toimesta.

Beamexin sisäiset tiedot, palvelimet ja verkot	**Kulunvalvonta ja todennus.** Käsittelijä käyttää alan standardien mukaisia toimenpiteitä henkilöiden ja käyttäjien todentamiseksi, järjestelmiin, ohjelmistoihin, tiedostoihin ja tietoihin pääsyn rajoittamiseksi (sekä luvattoman pääsyn estämiseksi). Kaksivaiheista todennusta vaaditaan ensisijaisesti kirjauduttaessa verkkoon etäyhteyden kautta. Tavoitteena on käyttää ensisijaisesti verkkotunnuksen kertakirjautumista (single sign-on) sovelluksissa. Salasanojen on oltava vähintään 8 merkkiä pitkiä, mutta suositeltavia ovat 14 merkin vahvat salasanat, jotka sisältävät erikoismerkkejä, numeroita ja isoja kirjaimia. Pääsy tietyihin tiedostoihin voidaan myös rajata järjestelmä-, kansio- ja asiakirjakohtaisilla käyttöoikeusrajoituksilla. **Sähköposti.** Sähköpostiviestintään on olemassa ohjeet. Erityiset sähköpostin tietoturva-asiat on otettava huomioon luottamuksellista tietoa lähetettäessä tai vastaanotettaessa. Sähköpostipalvelimen ja päätelaitteen (tietokone, puhelin, tabletti jne.) välinen yhteys on salattu. **Tiedostot ja tietokannat.** Tietojen tallentamiseen pilveen on käytössä erilaisia käytäntöjä. Tärkeiden tietojen tallentamista paikallisen tietokoneen kiintolevylle ei suositella.Käsittelijän omien toimitilojen palvelimia ja järjestelmiä käytetään arkaluonteisten tai erittäin luottamuksellisten tietojen tallentamiseen. Arkistointia vaativien tai versio- ja elinkaarihallintaa edellyttävien tallenteiden säilyttämiseen ja hallintaan on olemassa erilliset ohjeet ja käytännöt. Sharefile on ensisijainen työkalu luottamuksellisen tiedon toimittamiseksi kolmansille osapuolille turvallisella tavalla. Microsoft Office365 -ohjelmistoa käytetään laajalti erityisesti tiimityöskentelyssä käytettävien asiakirjojen tallentamiseen ja jakamiseen (pois lukien erittäin arkaluonteiset tai erittäin luottamukselliset tiedot). **Etäyhteydet.** Esimiehet määrittelevät laitteiden, ohjelmistojen ja etäyhteyksien tarpeen liikkuvassa työssä. Turvallinen asiakas-VPN tai Citrix/XenApp kaksivaiheisella todennuksella vaaditaan etätyössä.Mobiililaitteet ovat salasana-/koodisuojattuja ja soveltuvin osin MDM-hallittuja. Liikkuvaan työhön sekä tiedostojen ja tallenteiden pilvitallennukseen voi olla erilliset käytännöt. **Verkot, palvelimet ja IT-infrastruktuuri.** Dataverkot on segmentoitu erillisiin ali-/virtuaaliverkkoihin. Niiden liikenteen valvontaan, tunkeutumisen estämiseen ja havainnointiin sekä AV-valvontaan käytetään asianmukaisia työkaluja ja/tai palveluita. Tietyt datayhteydet ja kriittiset verkon reunakomponentit on kahdennettu. Tavoitteena on järjestää joko kahdennus tai varalaite kaikille kriittisille komponenteille tietoverkkojen, palvelimien, tallennustilojen ja muiden kriittisten järjestelmien ns. yhden vikapisteen (SPOF) riskien lieventämiseksi. Kriittisten laitteiden varaosille ja komponenteille ylläpidetään omaa varastoa. Tiettyjen kriittisten järjestelmien ja laitteiden virransyöttö on varmistettu keskeytymättömällä virransyöttöjärjestelmällä (UPS). Korkean käytettävyyden (HA) tallennusjärjestelmiä, tallennuksen peilausta tai jotain muuta kriittisille tietojärjestelmille harkittua vikasietoista järjestelmää voidaan käyttää. Säännölliset levykuva-/järjestelmävarmuuskopiot suoritetaan virtuaalipalvelimille, tuotantojärjestelmille ja tietyille muille kriittisessä käytössä oleville tietokoneille sovellettavan vakiotoimintamenettelyn mukaisesti. Järjestelmävarmuuskopiot toteutetaan muissa kohteissa tapauskohtaisen harkinnan ja riskiarvioinnin perusteella. **Varmuuskopiokäytäntö.** Käsittelijällä on erilaisia varmuuskopiointisuunnitelmia ja -toimenpiteitä tietojen ja järjestelmien palauttamista varten. Suunnitelmat ja toimenpiteet voivat vaihdella tietojen ja järjestelmän tärkeyden mukaan. Käsittelijällä on erillinen vakiotoimintamenettely tietojen ja tietojärjestelmien varmuuskopioinneille. **Haittaohjelmat.** Käsittelijä ylläpitää palomuureja sekä virustorjuntaa, haittaohjelmien torjuntaa, roskapostin suodatusta ja muita vastaavia teknisiä toimenpiteitä havaitakseen, estääkseen ja suojautuakseen ulkoisilta kyberhyökkäyksiltä, luvattomalta pääsyltä ja haittaohjelmien asentamiselta tietoihinsa, järjestelmiinsä, verkkoihinsa ja laitteisiinsa.

[Tietojenkäsittelysopimuksen loppu.]

Contrat de traitement des données (FR)

1. Introduction, objectif et application

Le présent contrat de traitement des données (« **DPA** ») s'applique, dans le cadre du contrat commercial (« **Contrat** »), au traitement des données à caractère personnel effectué par une entité juridique de Beamex désignée dans l'offre, la confirmation de commande ou le contrat, telle que Beamex Oy Ab ou l'une de ses filiales (« **Responsable du traitement** »), dans le cadre de la fourniture de services numériques ou autres (« **Services** ») au client, qui est partie contractante au Contrat ainsi que le responsable du traitement de ces données à caractère personnel (« **Contrôleur** »), lesdits Services étant décrits plus en détail dans le Contrat conclu entre le Sous-traitant et le Responsable du traitement.

Le présent DPA fait partie intégrante et indissociable de l'accord entre les parties. Tous les termes utilisés dans le présent DPA, mais non définis, ont la même signification que dans le contrat. En cas de conflit entre l'Accord et le présent DPA, les conditions du DPA prévalent.

2. Définitions

« Contrôleur » désigne la personne physique ou morale, l'autorité, l'agence ou tout autre organisme mentionné dans ce DPA, qui définit seule ou conjointement avec d'autres les finalités et les moyens du traitement des données personnelles.

« Loi(s) sur la protection des données » désigne la Loi sur la protection des données (1050/2018) et le Règlement général sur la protection des données de l'UE (2016/679) avec ses amendements et règlements de remplacement, ainsi que d'autres législations et instructions de protection des données valides et applicables et les règlements contraignants des autorités de protection des données.

« Personne concernée » désigne une personne physique identifiée ou identifiable dont les Données Personnelles sont traitées sur la base de ce DPA.

« Données personnelles » désigne toute information relative à une personne physique identifiée ou identifiable ; une personne physique identifiable est considérée comme une personne physique qui peut être identifiée directement ou indirectement, notamment sur la base d'informations d'identification telles que le nom, le numéro de sécurité sociale, les informations de localisation, les informations d'identification en ligne ou une ou plusieurs caractéristiques physiques, physiologique, génétique, psychologique, économique, des facteurs culturels ou sociaux qui lui sont caractéristiques.

« Violation de données personnelles » désigne un événement de violation de la sécurité des données entraînant la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé aux données personnelles transférées, stockées ou autrement traitées.

« Traitement » désigne la ou les opérations effectuées sur des données à caractère personnel ou des ensembles de données contenant des données à caractère personnel dans le cadre de la fourniture des Services, que ce soit par des moyens automatisés ou manuels, telles que la collecte, le stockage, l'organisation, la structuration, la conservation, la modification ou l'altération, la recherche, la consultation, l'utilisation, le transfert, la diffusion ou toute autre forme de mise à disposition, le recoupement ou la combinaison, la limitation, l'effacement ou la destruction des informations.

« Responsable du traitement » désigne la personne physique ou morale, l'autorité, l'agence ou tout autre organisme mentionné dans ce DPA qui traite des données personnelles pour le compte du contrôleur.

« **Clauses Contractuelles Types** » désigne les clauses contractuelles types (UE) 2021/914 en date du 4 juin 2021. Toute référence faite aux clauses contractuelles types se référera aux clauses contractuelles types, qui incluent la sélection des parties sur certains modules et clauses facultatives, ainsi qu'aux annexes I à II du présent DPA. En outre, les parties conviennent que le recours à des sous-responsables du traitement sera régi par la clause 9, option 1 des clauses contractuelles types.

« Sous-responsable » désigne une personne physique ou une entité juridique ayant une relation contractuelle avec le responsable du traitement, qui traite des données personnelles en tant que sous-traitant du responsable du traitement dans le cadre de la réalisation de services pour le responsable.

3. Portée du traitement et des activités de traitement

En vertu du présent DPA, ces données à caractère personnel sont traitées, le contrôleur agissant en tant que seul contrôleur des données.

Le responsable du traitement traite les données à caractère personnel (i) conformément à la législation en matière de protection des données et aux dispositions du présent contrat de traitement des données (DPA) afin de remplir les obligations décrites dans le contrat ; et (ii) conformément aux instructions écrites données de temps à autre par le contrôleur, sauf disposition contraire prévue par la législation en matière de protection des données applicable au responsable du traitement. Le responsable du traitement ne peut traiter les données à caractère personnel à ses propres fins ni les transmettre à des tiers, sauf si le présent DPA l'y autorise. Le responsable du traitement doit informer le contrôleur s'il considère ou soupçonne que les instructions écrites du contrôleur enfreignent les lois sur la protection des données. Sauf stipulation contraire dans le présent DPA ou ses annexes, le responsable du traitement ne peut traiter les données à caractère personnel que pendant la durée du contrat.

Le contrôleur (i) s'engage à respecter les obligations qui lui incombent en vertu des lois sur la protection des données qui lui sont applicables dans le cadre du traitement des données à caractère personnel ; et (ii) est responsable du fait qu'il dispose, en tant que seul contrôleur des données, du droit de traiter des données à caractère personnel et qu'il a rempli son obligation d'informer les personnes concernées et/ou a reçu (ou recevra) de celles-ci tous les consentements requis par les lois applicables en matière de protection des données afin que le responsable du traitement puisse traiter des données à caractère personnel pour le compte du contrôleur conformément au présent DPA.

Des informations plus détaillées sur le traitement, telles que la nature du traitement, les types de données personnelles et les groupes de sujets de données, sont décrites dans l'**annexe 1**. L'annexe peut être mise à jour en cas de changements dans le traitement.

Toutefois, le contrôleur reconnaît et accepte que, dans le cadre de la fourniture des services au contrôleur, le responsable du traitement a le droit d'utiliser les informations relatives au fonctionnement, à l'assistance ou à l'utilisation du service, ou obtenues en rapport avec celui-ci, à des fins commerciales internes légales et légitimes, telles que (i) la facturation duservice en fonction de l'utilisation ou du nombre d'utilisateurs, (ii) la fourniture du service et la gestion de celle-ci, (iii) pour le développement fonctionnel et technique du service, (iv) pour se conformer aux lois applicables (y compris pour répondre à des demandes officielles), (v) pour garantir la sécurité du service, et (vi) pour prévenir la fraude et les abus ou réduire les risques. Dans la mesure où ces informations sont des données à caractère personnel, le s'engage à : (a) traiter ces données à caractère personnel conformément aux lois applicables en matière de protection des données et uniquement à des fins compatibles avec les objectifs décrits dans la présente section ; et (b) ne pas utiliser ces données à caractère personnel à d'autres fins ou les divulguer à des tiers, à moins qu'il n'ait d'abord anonymisé les données de sorte qu'aucune autre personne ou entité ne puisse être identifiée à partir des données.

4. Sous-traitants et sous-responsables

Le responsable du traitement a le droit de recourir à des sous-responsables dans le cadre du traitement. Sur demande, le responsable du traitement doit fournir au contrôleur plus d'informations sur les sous-responsables qu'il utilise. Si le responsable du traitement apporte des modifications importantes à ses sous-responsables, il doit en informer le contrôleur par écrit. Le contrôleur a le droit d'interdire le recours à un sous-responsable spécifique pour une raison justifiée. Si le contrôleur interdit le recours à un sous-responsable particulier et qu'il n'est pas raisonnablement possible de transférer les tâches de ce sous-responsable à quiconque d'autre, y compris au responsable du traitement, le responsable du traitement a le droit de résilier le DPA et de mettre fin au traitement. Le contrôleur n'a droit à aucune compensation uniquement sur la base du fait que le traitement prend fin et que le DPA a été résilié en raison de l'interdiction par le contrôleur du recours à un sous-responsable spécifique.

Le responsable du traitement doit conclure un accord écrit avec chaque sous-responsable, qui contient les conditions générales requises par les lois sur la protection des données et des types d'obligations essentiellement similaires à ceux que le responsable du traitement a accepté en vertu du présent DPA. Le responsable du traitement est responsable des sous-responsables qu'il utilise, tout comme il est responsable de ses propres actions.

5. Protection des donnés

Le responsable du traitement doit mettre en œuvre des mesures techniques, physiques et organisationnelles appropriées pour garantir un niveau élevé de sécurité dans le traitement des données à caractère personnel par le responsable du traitement et pour protéger les données à caractère personnel contre tout traitement non autorisé ou illégal et contre toute perte, destruction, dommage, modification ou transfert involontaire. Lors de l'évaluation des mesures nécessaires pour garantir le niveau de sécurité, les instructions du contrôleur, les dernières technologies et les coûts de mise en œuvre, la nature, la portée, le contexte et les finalités du traitement, ainsi que les risques pour les droits et libertés des personnes physiques, qui varient en probabilité et en gravité, doivent être prises en compte.

Les mesures applicables peuvent être, par exemple : (i) la pseudonymisation et le chiffrement des données à caractère personnel ; (ii) la capacité à garantir en permanence la confidentialité, l'intégrité, la disponibilité et la tolérance aux défaillances des systèmes et services ; (iii) la capacité à rétablir rapidement la disponibilité des données à caractère personnel et l'accès aux données à caractère personnel en cas de défaillance physique ou technique ; et (iv) la procédure de test, d'examen et d'évaluation réguliers de l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du traitement. Le responsable du traitement doit prendre les mesures nécessaires pour garantir que toute personne physique travaillant pour son compte et ayant accès à des données à caractère personnel ne traite ces données que conformément aux instructions du responsable du traitement, sauf disposition contraire de la législation applicable en matière de protection des données. Le responsable du traitement est chargé, conformément à ses propres politiques, d'effectuer des sauvegardes des données et des fichiers du responsable du traitement dont il a la garde, ainsi que de vérifier leur bon fonctionnement.

Sans limiter les exigences et obligations décrites ci-dessus, le responsable du traitement doit toujours mettre en œuvre au moins les mesures de sécurité de l'information techniques et organisationnelles qui correspondent essentiellement aux mesures décrites à l'**annexe 2**.

6. Confidentialité

Le sous-traitant doit veiller, dans la mesure du possible, à ce que seules les personnes agissant en son nom qui ont besoin d'accéder aux informations pour atteindre l'objectif du présent contrat de traitement aient accès aux données à caractère personnel, et à ce que les personnes habilitées à traiter ces données s'engagent à respecter l'obligation de confidentialité ou soient soumises à l'obligation légale de confidentialité applicable.

7. Transferts internationaux de données

7.1 Transferts autorisés

Le sous-traitant peut transférer vers un pays en dehors de l'Union européenne ou de l'Espace économique européen. Le sous-traitant doit toujours respecter les conditions et exigences des lois sur la protection des données lors du transfert de données vers des pays en dehors de l'Union européenne ou de l'Espace économique européen, par exemple en utilisant les clauses contractuelles types publiées par la Commission européenne applicables au transfert de données.

7.2 Responsables du traitement dans l'EEE et contrôleur en dehors de l'EEE

Si le responsable du traitement est établi au sein de l'EEE et le contrôleur en dehors de l'EEE, le transfert des données à caractère personnel est régi par le module 4 des clauses contractuelles types, qui sont incorporées aux présentes par référence et font partie intégrante du contrat de traitement des données. Le contrôleur conclut les clauses contractuelles types en tant qu'« importateur de données » et le responsable du traitement en tant qu'« exportateur de données ».

Aux fins des Clauses contractuelles types :

a) le module quatre s'applique ;
b) la clause d'accueil facultative, clause 7, s'appliquera ;
c) à la Clause 11, la langue facultative est supprimée ;
d) à la Clause 17, les lois substantielles de la Finlande s'appliquent ;
e) à la Clause 18, les litiges seront réglés devant le tribunal de district d'Helsinki, Finlande ; et
f) les Annexes des Clauses contractuelles types seront complétées par les informations énoncées dans le DPA, y compris ses annexes.

Si et dans la mesure où les clauses contractuelles types entrent en conflit avec une disposition du contrat ou du DPA concernant le transfert de données à caractère personnel du contrôleur au responsable du traitement, les clauses contractuelles types prévaudront dans la mesure de ce conflit.

Si le Sous-traitant est situé dans l'EEE et mandate un Sous-traitant secondaire situé en dehors de l'EEE, le Sous-traitant conclura les Clauses contractuelles types (Module 3) avec ce Sous-traitant secondaire. Tout transfert ultérieur de Données à caractère personnel doit être conforme au Module applicable des Clauses contractuelles types.

8. Violations de données personnelles et obligations de signalement

Le responsable du traitement doit informer le contrôleur de toutes les violations réelles ou présumées de données à caractère personnel sans délai indu après avoir pris connaissance de la violation.

Le responsable du traitement doit fournir au contrôleur toutes les informations disponibles sur la violation de données à caractère personnel, dont le contrôleur peut avoir besoin pour remplir ses propres obligations d'enquête et de signalement. Le Sous-traitant peut compléter ultérieurement les informations s'il ne dispose pas immédiatement d'informations complètes sur la violation. Le responsable du traitement doit par ailleurs assister et coopérer avec le contrôleur dans le cadre de l'enquête sur la violation de données à caractère personnel et pour toute question éventuelle relative à la notification aux autorités et aux personnes concernées. Le Sous-traitant doit également prendre les mesures de suivi raisonnables nécessaires pour atténuer les effets négatifs de la Violation des données à caractère personnel, réparer la violation ou la violation qui s'est produite et prévenir les violations futures. Le responsable du traitement ne peut faire aucune déclaration concernant la violation de données à caractère personnel à des tiers, en particulier aux représentants des médias, sans l'autorisation écrite expresse et les instructions du contrôleur, sauf si les lois sur la protection des données l'exigent.

Sauf disposition contraire de la législation sur la protection des données ou de l'ordonnance de l'autorité compétente, le contrôleur prend la décision finale, à sa seule discrétion, de savoir si la violation des données à caractère personnel doit être notifiée aux autorités ou aux autres parties concernées, et de la manière possible de procéder à ces notifications. Si le responsable du traitement signale une violation de données à caractère personnel aux autorités ou à d'autres parties intéressées, celles-ci doivent être approuvées au préalable par le contrôleur.

9. Droits de documentation et d'audit

Une partie a l'obligation de mettre à la disposition de l'autre partie toutes les informations et tous les documents nécessaires pour démontrer le respect du présent DPA et des lois sur la protection des données.

À la demande du contrôleur, le responsable du traitement doit également autoriser la réalisation d'audits portant sur le traitement, les services, les mesures de sécurité des données ainsi que ses propres systèmes et processus informatiques, et participer à ces audits à des intervalles raisonnables afin de garantir le respect du présent accord

et de la législation en matière de protection des données. Ces audits ne peuvent être effectués qu'une fois par an, sauf s'il existe une raison justifiée de supposer que le sous-traitant ne respecte pas le DPA ou les lois sur la protection des données. Les audits peuvent également inclure des visites dans les bureaux du sous-traitant ou d'autres locaux physiques. L'audit est effectué pendant les heures normales de travail et de manière à ne pas perturber inutilement les opérations du sous-traitant. Chaque partie prend en charge ses propres frais liés à l'audit. Les audits prévus doivent être notifiés au sous-traitant au moins quinze (15) jours avant l'audit prévu. Les informations sur les activités du responsable du traitement obtenues par le contrôleur au cours de l'audit sont confidentielles.

10. Assistance au contrôleur

Le responsable du traitement doit, à la demande et aux frais du contrôleur, aider raisonnablement le responsable du traitement à se conformer aux obligations des gestionnaires de données conformément aux lois sur la protection des données. L'obligation d'assistance s'applique en particulier aux questions suivantes :

10.1 Accès aux données personnelles

Dans la mesure où les données à caractère personnel ne sont pas disponibles directement par le biais des services, le responsable du traitement fournira, sur demande, les données en question au contrôleur. Si les informations sont disponibles sous forme électronique, elles doivent également être remises au contrôleur sous cette forme.

10.2 *Respect des droits des personnes concernées et des demandes émanant de l'autorité de contrôle*

Le responsable du traitement doit informer sans délai le contrôleur : (i) de toutes les demandes, plaintes ou notifications formulées par l'autorité de contrôle ou toute autre autorité compétente ; et (ii) de toute demande reçue directement de la personne concernée, liée à l'exercice des droits de la personne concernée. Le responsable du traitement ne peut répondre directement à la demande que si le contrôleur a donné son autorisation et des instructions à cet effet au préalable. Si le contrôleur le demande, le responsable du traitement doit raisonnablement aider le gestionnaire à répondre aux demandes officielles et à exercer les droits de la personne concernée conformément à la législation sur la protection des données.

10.3 Évaluation de l'impact sur la protection des données

Si le responsable du traitement prend connaissance du fait que le traitement envisagé entraînerait un risque élevé en matière de droits et de libertés d'une personne physique, il doit en informer le contrôleur et, le cas échéant, l'aider à effectuer une évaluation d'impact relative à la protection des données.

10.4 Correction, suppression et limitation des données à caractère personnel

Le responsable du traitement doit soit (i) offrir la possibilité de rectifier, d'effacer ou de limiter le traitement des données à caractère personnel par le biais des fonctionnalités du service, soit (ii) rectifier, effacer ou limiter le traitement des données à caractère personnel conformément aux instructions du contrôleur.

11. Conditions et résiliation

11.1 Entrée en vigueur et résiliation

Sauf accord contraire, le présent DPA entre en vigueur en même temps que le contrat et reste valable tant que le responsable du traitement traite les données à caractère personnel du contrôleur dans le cadre de la fourniture de ses services. Indépendamment de la résiliation du DPA, les dispositions du DPA, qui sont de nature à rester en vigueur indépendamment de la résiliation du contrat, restent en vigueur indépendamment de la résiliation du DPA.

11.2 Restitution ou suppression des données à caractère personnel à la fin du traitement

À la résiliation du présent DPA, le responsable du traitement doit, au choix du contrôleur, soit effacer toutes les données à caractère personnel traitées pour le compte du gestionnaire, soit restituer toutes les données à caractère personnel au gestionnaire et effacer les copies existantes, sauf si les lois sur la protection des données ou d'autres réglementations (par exemple, la norme ISO 17025) imposent la conservation de ces données. Dans ce cas, le sous-traitant a le droit de conserver les données à caractère personnel conformément aux exigences de la loi, sans poursuivre autrement le traitement des données à caractère personnel et tout en respectant les obligations de confidentialité décrites dans le présent contrat. La restitution ou la suppression des données à caractère personnel doit être effectuée sans délai excessif après la demande du contrôleur. Si le contrôleur n'a donné aucune instruction concernant la suppression ou la restitution des données à caractère personnel, le responsable du traitement peut, de sa propre initiative, supprimer les données à caractère personnel en sa possession douze (12) mois après la fin du contrat. Le sous-traitant doit renvoyer les données à caractère personnel dans un format électronique couramment utilisé et sécurisé ou dans un autre format convenu par les parties.

12. Autres dispositions

12.1 Modifications

Toutes les modifications du présent contrat doivent être convenues par écrit entre les parties. Par souci de clarté, il est précisé que les instructions écrites données ponctuellement par le contrôleur en vue de la mise en œuvre du traitement des données à caractère personnel ne sont pas considérées comme des modifications apportées au présent accord de traitement des données.

12.2 Responsabilités

Si la personne concernée subit un préjudice résultant d'une violation des lois sur la protection des données, la responsabilité du contrôleur et du responsable du traitement à l'égard de ce préjudice est déterminée conformément à l'article 82 du règlement général sur la protection des données de l'Union européenne (2016/679). Chaque partie est responsable des éventuelles amendes administratives imposées par l'autorité de contrôle sur la base d'une violation des lois sur la protection des données. La responsabilité d'une partie envers l'autre partie en cas de dommages-intérêts résultant d'une violation du présent contrat de traitement des données est limitée à un montant maximal correspondant au total des frais de service hors TVA payés en vertu du contrat au cours des six (6) mois précédant la présentation de la première demande de dommages-intérêts. À d'autres égards, les conditions de limitation de responsabilité qui peuvent être contenues dans le contrat entre les parties ou ses annexes s'appliquent également au présent contrat de traitement des données. Sauf mention contraire expresse dans les présentes, aucune des parties ne peut être tenue responsable envers l'autre de tout dommage indirect, consécutif, accessoire, spécial ou punitif (y compris les dommages liés à l'interruption d'activité et à la perte d'usage, de données, de ventes, de recettes ou de bénéfices), lesquels sont expressément exclus.

12.3 Droit applicable et règlement des litiges

En ce qui concerne le droit applicable et le règlement des litiges, les termes du contrat entre les parties sont respectés, sauf disposition contraire des lois sur la protection des données. Si le contrat ne mentionne pas le droit applicable ou ne contient pas de conditions de résolution des litiges, le contrat de traitement des données sera régi par les lois substantielles du domicile du sous-traitant.

13. Annexes

Le présent contrat de traitement des données se compose du présent document et des annexes énumérées ci-dessous :

- Annexe 1 : Description des opérations de traitement
- Annexe 2 : Mesures techniques et organisationnelles de sécurité de l'information

Annexe 1 au DPA (et, le cas échéant, aux clauses contractuelles types)

A. LISTE DES PARTIES

Exportateur de données :

Nom : Beamex Oy Ab

Adresse : Ristisuonraitti 10, 68600 Pietarsaari, FINLANDE

Activités liées aux données transférées en vertu des présentes clauses : Beamex est une entreprise technologique qui fabrique et fournit des équipements d'étalonnage, des logiciels et des services connexes à ses clients industriels. L'importateur de données est un client de Beamex et un utilisateur des services numériques de Beamex, qui sont concernés par le présent DPA.

Rôle (contrôleur/responsable du traitement) : responsable du traitement.

Importateur(s) de données :

Nom : le nom mentionné dans l'accord commercial conclu avec Beamex Oy Ab.

Adresse : telle qu'indiquée dans le contrat commercial.

Activités liées aux données transférées en vertu des présentes clauses : L'importateur de données est un client de Beamex qui utilise les services numériques de Beamex.

Rôle (contrôleur/responsable du traitement) : contrôleur.

Sous-traitants secondaires essentiels du sous-traitant au moment de la conclusion du DPA :

a) **Microsoft Datacenter Netherlands B.V.** Étant donné que Beamex Oy Ab souscrit aux services cloud Azure (PaaS) – Europe occidentale conformément aux conditions générales des produits Microsoft, les conditions relatives au traitement et à la sécurité des données sont définies dans l'avenant sur la protection des données (DPA) des services en ligne Microsoft.
b) **Bjorkstrom Oy Ab** – domiciliée en Finlande, les activités de traitement comprennent le développement et le déploiement de LOGiCAL.

B. DESCRIPTION DU TRANSFERT/TRAITEMENT

	Services numériques et logiciel cloud Beamex (par ex. LOGiCAL)	Autres services Beamex (p. ex. assistance logicielle, migration de données, intégration système)
Catégories de personnes concernées dont les données à caractère personnel sont transférées :	Il s'agit principalement des employés ou sous-traitants du contrôleur qui utilisent et effectuent des étalonnages à l'aide des équipements d'étalonnage Beamex, dont les résultats sont ensuite enregistrés dans le logiciel d'étalonnage Beamex.	Il s'agit principalement des employés ou sous-traitants du contrôleur qui utilisent et effectuent des étalonnages à l'aide des équipements d'étalonnage Beamex, dont les résultats sont ensuite enregistrés dans le logiciel d'étalonnage Beamex.
Catégories de données à caractère personnel transférées :	En particulier, le nom, le poste, le nom de l'employeur ainsi que les données relatives aux activités que la personne a exercées avec les équipements d'étalonnage de Beamex.	En particulier, le nom, le poste, le nom de l'employeur ainsi que les données relatives aux activités que la personne a exercées avec les équipements d'étalonnage de Beamex.
La fréquence du transfert :	Les données sont transférées à la fois en continu et selon les besoins pour fournir le(s) service(s).	Au besoin.
Nature du traitement :	Attribuer des droits d'utilisation au logiciel d'étalonnage Beamex au contrôleur et enregistrer dans ce logiciel les données d'étalonnage relatives aux étalonnages effectués par les employés et les sous-traitants du contrôleur.	Prestation de services d'assistance, de support et de maintenance aux clients de Beamex, ainsi que prestation de services de migration et d'intégration liés aux produits logiciels, dans le cadre desquels le traitement de données à caractère personnel peut avoir lieu.
Finalité(s) du transfert et du traitement ultérieur des données :	Utilisation du logiciel d'étalonnage Beamex pour le stockage des résultats de l'étalonnage.	Permettre l'utilisation des produits de Beamex, leur mise en œuvre et/ou leur fonctionnement conjointement avec d'autres systèmes.
La durée de conservation des données à caractère personnel ou, si cela n'est pas possible, les critères utilisés pour déterminer cette durée :	La durée du contrat commercial et tant que le contrôleur utilise les services numériques de Beamex.	La durée de l'accord commercial et tant que Beamex traite les données en tant que sous-traitant aux fins prévues.
AUTORITÉ DE CONTRÔLE COMPÉTENTE :	Bureau de l'ombudsman de la protection des données (Tietosuojavaltuutetun toimisto) Adresse : Lintulahdenkuja 4, 00530 Helsinki, FINLANDE Standard : +358 29 566 6700, Bureau d'enregistrement : +358 29 566 6768 www.tietosuoja.fi	

Annexe 2 au DPA (et, le cas échéant, aux clauses contractuelles types)

Une description des mesures techniques et organisationnelles que le sous-traitant doit mettre en œuvre en plus des obligations générales mentionnées dans le DPA pour garantir un niveau approprié de sécurité des données.

Zone	Plans et pratiques
Microsoft Azure (PaaS)	**Les services Beamex LOGiCALet Beamex Sync sont basés sur Azure (PaaS). Le portail de confiance des services Microsoft répertorie toutes les certifications, rapports, documents, etc. relatifs à la continuité des activités (ISO 22301) et aux systèmes de gestion de la sécurité de l'information (ISO 27001 et autres normes de la série 27000) à l'adresse** : **https://servicetrust.microsoft.com/viewpage/ISOIEC.**
Sécurité des locaux et sécurité physique	**Accès aux locaux**. Le Sous-traitant limite l'accès à ses locaux à l'aide de cartes d'identité personnelles (RFID). Les droits d'accès aux différentes zones des locaux sont accordés sur la base de droits définis par la direction et les superviseurs. Certaines zones spécifiques peuvent faire l'objet de mesures de protection et de contrôle d'accès renforcées. Les invités n'ont accès qu'aux locaux publics (lobby, cafétéria, toilettes) et ne se déplacent dans les locaux du Sous-traitant qu'avec un hôte. **Systèmes d'alarme et gardiennage des installations.** Le gardiennage des locaux est sous-traité à une société de sécurité professionnelle. Les locaux sont équipés de systèmes d'alarme conformes aux normes du secteur, notamment des alarmes en cas d'accès non autorisé, des systèmes de surveillance des conditions de laboratoire, des alarmes relatives au refroidissement et à la température des centres de données informatiques, des alarmes du système de climatisation et des systèmes d'alarme incendie. Le responsable des services techniques de l'entreprise est chargé de la maintenance technique des systèmes de contrôle d'accès et d'alarme. Les employés ont suivi une formation ou disposent de consignes sur la manière d'agir dans diverses situations d'alerte ou de crise ; certaines situations peuvent faire l'objet d'exercices réguliers.
Gestion du personnel, de l'organisation et de la sécurité de l'information	**Sécurité du personnel.** Les contrats de travail conclus avec les salariés contiennent une clause de confidentialité conforme aux normes du secteur. Dans certaines situations particulières, des accords de confidentialité supplémentaires peuvent être signés (par exemple, des projets et/ou des informations spécifiques). Les employés sont également tenus de suivre toutes les directives ou politiques que le sous-traitant peut avoir, y compris, mais sans s'y limiter, celles relatives à l'éthique commerciale, à la confidentialité et à la sécurité de l'information. **Formation et directives.** Une formation obligatoire à la sécurité de l'information fait partie du programme d'intégration de chaque nouvel employé. Des formations générales ou spécifiques supplémentaires sur la sécurité de l'information sont organisées de temps à autre pour les employés. La direction, les superviseurs, les propriétaires de systèmes, les responsables du contrôle d'accès et les autres personnes concernées reçoivent une formation sur le contenu de la politique de sécurité de l'information du sous-traitant ainsi que sur ses révisions futures. Bon nombre de ces personnes participent également à la gestion des risques et aux examens, formations et/ou exercices de planification de la continuité des activités. Des directives spécifiques pour les employés peuvent exister dans divers domaines, tels que l'e-mail professionnel, l'accès à distance et le travail à distance, les outils et les logiciels, ainsi que la gestion des fichiers, des documents et des enregistrements. **Gestion, suivi, examens et audits.** L'évaluation des risques liés à la sécurité de l'information et à la continuité des activités fait partie des audits du système qualité de l'entreprise. Des évaluations des risques, des inspections et des plans de développement distincts sont élaborés sur la base des conclusions et des risques identifiés, et toujours en lien avec de nouveaux projets de développement ou des modifications apportées au système de planification, aux installations ou aux processus. On fait appel à des experts externes, à des évaluations par les pairs ou à des audits lorsque cela est possible ou nécessaire pour évaluer le niveau de sécurité des informations techniques. La fonction ICT de l'entreprise gère le cadre de la sécurité de l'information et est responsable de nombreuses mesures pratiques et techniques de sécurité de l'information. L'ICT est représentée dans l'équipe de direction de l'entreprise.
Continuité des activités	Le sous-traitant maintient des plans et des mesures pour la continuité des activités et la reprise après sinistre.

Tiers, sous-traitants, responsables du traitement et sous-responsables du traitement	**Contexte et contrats.** Les antécédents des tiers, des sous-traitants et des sous-responsables de traitement sont vérifiés, selon ce qui est jugé approprié et nécessaire, avant l'établissement d'une relation commerciale. Les partenaires tiers sont contractuellement tenus à des obligations de confidentialité. Des contrats écrits relatifs au traitement des données (ou des annexes) sont conclus avec les partenaires considérés comme des gestionnaires de données ou des sous-gestionnaires du gestionnaire. Le cas échéant, des formations ou des instructions peuvent être fournies aux tiers employés par le Gestionnaire sur des sujets liés également à la sécurité de l'information. **Achats informatiques.** Les ordinateurs, les appareils mobiles, les systèmes et les logiciels sont principalement achetés par le service informatique. Les informations de licence sont également enregistrées et stockées par le service informatique.
Données internes, serveurs et réseaux Beamex	**Contrôle d'accès et authentification.** Le Sous-traitant utilise des mesures standard de l'industrie pour authentifier les personnes et les utilisateurs, limiter l'accès (ainsi que pour empêcher tout accès non autorisé) aux systèmes, logiciels, fichiers et données. L'authentification à deux facteurs est principalement requise lors de la connexion au réseau à partir d'une connexion à distance. L'objectif est d'utiliser principalement l'authentification unique au niveau du domaine dans les applications. Les mots de passe doivent contenir au moins 8 caractères, mais il est préférable d'utiliser des mots de passe forts de 14 caractères contenant des caractères spéciaux, des chiffres et des majuscules. L'accès à certains fichiers peut également être soumis à des restrictions de droits d'accès spécifiques au système, aux dossiers et aux documents. **Email.** Il existe des directives pour les communications par e-mail. Il convient de prendre en compte certaines questions spécifiques liées à la sécurité des e-mails lors de l'envoi ou de la réception d'informations confidentielles. La connexion entre le serveur de messagerie et le terminal (ordinateur, téléphone, tablette, etc.) est chiffré. **Fichiers et bases de données.** Différentes pratiques sont mises en place pour stocker les données dans le cloud. Il n'est pas recommandé d'enregistrer des données importantes sur le disque dur d'un ordinateur local. Les serveurs et systèmes dans les locaux du Sous-traitant sont utilisés pour enregistrer des informations sensibles ou hautement confidentielles. Il existe des directives et des pratiques distinctes pour le stockage et la gestion des documents nécessitant un classement et une archivage, ou une gestion des versions et du cycle de vie. Sharefile est l'outil principal pour fournir des informations confidentielles à des tiers de manière sécurisée. Microsoft Office 365 est largement utilisé pour stocker et partager notamment les documents destinés au travail en équipe (à l'exception des informations très sensibles ou hautement confidentielles). **Connexions à distance.** Les responsables définissent les besoins en matière d'équipements, de logiciels et de connexions à distance pour le travail à distance. VPN client sécurisé ou Citrix/XenApp avec authentification à deux facteurs requise pour le travail à distance. Les appareils mobiles sont protégés par mot de passe/code et, le cas échéant, contrôlés par MDM. Il peut exister des politiques distinctes concernant le travail mobile et le stockage de fichiers et de documents dans le cloud. **Réseaux, serveurs et infrastructure informatique.** Les réseaux de données sont segmentés en sous-réseaux/réseaux virtuels distincts. Des outils et/ou services adaptés sont utilisés pour la surveillance du trafic, la prévention des intrusions et la surveillance, ainsi que pour la surveillance antivirus. Certaines connexions de données et certains composants critiques de périphérie du réseau sont dupliqués. L'objectif est de mettre en place une redondance ou un dispositif de sauvegarde pour tous les composants critiques afin d'atténuer les risques liés aux « points de défaillance uniques » (SPOF) dans les réseaux de données, les serveurs, les systèmes de stockage et autres systèmes critiques. Les pièces de rechange et les composants critiques de l'appareil sont stockés dans leur propre entrepôt. L'alimentation électrique de certains systèmes et appareils critiques est assurée par un système d'alimentation sans interruption (UPS). Il est possible d'utiliser des systèmes de stockage à haute disponibilité (HA), la mise en miroir des données ou d'autres systèmes tolérants aux pannes envisagés pour les systèmes d'information critiques. Des sauvegardes régulières des images et des systèmes sont effectuées sur les serveurs virtuels, les systèmes de production et certains autres ordinateurs utilisés pour des tâches critiques, conformément à la procédure opérationnelle standard en vigueur. Des solutions de secours sont mises en place pour d'autres éléments, en fonction d'une analyse au cas par cas et d'une évaluation des risques. **Politique de sauvegarde.** Le Sous-traitant dispose de divers plans et mesures de sauvegarde à des fins de récupération des données et des systèmes. Les plans et les mesures peuvent varier en fonction de l'importance des données et du système. Le Sous-traitant dispose d'une procédure opérationnelle standard distincte pour les sauvegardes des données et des systèmes d'information. **Logiciel malveillant.** Le Sous-traitant utilise des pare-feu ainsi que des antivirus, des logiciels anti-malware, des filtres anti-spam et d'autres mesures techniques similaires afin de détecter, prévenir et se prémunir contre les cyberattaques externes, les accès non autorisés et l'installation de logiciels malveillants sur ses données, ses systèmes, ses réseaux et ses appareils.

[Fin du DPA.]

Auftragsverarbeitungsvertrag (DE)

1. Einleitung, Zweck und Anwendungsbereich

Dieser Auftragsverarbeitungsvertrag („**AVV**“) gilt als Bestandteil des zwischen den Parteien geschlossenen Vertrags („**Vertrag**“) für die Verarbeitung personenbezogener Daten durch eine in Angebot, Auftragsbestätigung oder Vertrag bezeichnete Rechtseinheit von Beamex, wie beispielsweise Beamex Oy Ab oder eine ihrer Tochtergesellschaften („**Auftragsverarbeiter**“). Die Verarbeitung erfolgt im Zusammenhang mit der Erbringung digitaler oder sonstiger Dienstleistungen („**Dienstleistungen**“) gegenüber dem Kunden, der Vertragspartei des Vertrags und zugleich Verantwortlicher im Sinne der anwendbaren Datenschutzgesetze („**Verantwortlicher**“) ist. Die Dienstleistungen sind im Vertrag näher beschrieben.

Dieser AVV ist integraler und untrennbarer Bestandteil des Vertrags zwischen den Parteien. Soweit in diesem AVV verwendete Begriffe nicht definiert sind, haben sie die gleiche Bedeutung wie im Vertrag. Im Falle von Widersprüchen zwischen dem Vertrag und diesem AVV gehen die Bestimmungen dieses AVV vor.

2. Begriffsbestimmungen

„**Verantwortlicher**“ bezeichnet die in diesem AVV genannte natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

„**Datenschutzgesetze**“ bezeichnet die Datenschutz-Grundverordnung (EU) 2016/679 sowie alle anwendbaren nationalen und sonstigen gesetzlichen Bestimmungen zum Schutz personenbezogener Daten in ihrer jeweils geltenden Fassung sowie verbindliche Vorgaben und Anweisungen der zuständigen Aufsichtsbehörden.

„**Betroffene Person**“ bezeichnet eine identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten verarbeitet werden.

„**Personenbezogene Daten**“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

„**Verletzung des Schutzes personenbezogener Daten**“ bezeichnet eine Verletzung der Datensicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

„**Verarbeitung**“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie insbesondere das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

„**Auftragsverarbeiter**“ bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

„**Standardvertragsklauseln**“ bezeichnet die Standardvertragsklauseln wie definiert im Durchführungsbeschluss (EU) 2021/914 vom 4. Juni 2021. Jede Bezugnahme auf die Standardvertragsklauseln bezieht sich auf diese einschließlich der von den Parteien gewählten Module und optionalen Klauseln sowie der Anhänge I bis II dieses AVV. Darüber hinaus vereinbaren die Parteien, dass der Einsatz von Unterauftragsverarbeitern gemäß Klausel 9 Option 1 der Standardvertragsklauseln erfolgt.

„**Unterauftragsverarbeiter**“ bezeichnet eine natürliche oder juristische Person, die vom Auftragsverarbeiter als Subunternehmer beauftragt wird und personenbezogene Daten im Auftrag des Auftragsverarbeiters im Zusammenhang mit der Erbringung der Dienstleistungen für den Verantwortlichen verarbeitet.

3. Umfang der Verarbeitung und Verarbeitungstätigkeiten

Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten, für die der Verantwortliche als alleiniger Verantwortlicher im Sinne der anwendbaren Datenschutzgesetze handelt.

Der Auftragsverarbeiter verarbeitet personenbezogene Daten (i) in Übereinstimmung mit den anwendbaren Datenschutzgesetzen und den Bestimmungen dieses AVV zur Erfüllung der im Vertrag beschriebenen Verpflichtungen sowie (ii) ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern und soweit nicht anwendbare Datenschutzgesetze eine abweichende Verarbeitung vorschreiben. Der Auftragsverarbeiter ist nicht berechtigt, personenbezogene Daten zu eigenen Zwecken zu verarbeiten oder an Dritte weiterzugeben, es sei denn, dies ist nach diesem AVV ausdrücklich zulässig. Der

Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Auffassung ist oder den begründeten Verdacht hat, dass eine Weisung des Verantwortlichen gegen anwendbare Datenschutzgesetze verstößt. Sofern in diesem AVV oder seinen Anlagen nichts Abweichendes geregelt ist, darf der Auftragsverarbeiter personenbezogene Daten nur für die Dauer des Vertrags verarbeiten.

Der Verantwortliche (i) verpflichtet sich, bei der Verarbeitung personenbezogener Daten die für ihn geltenden Datenschutzgesetze einzuhalten, und (ii) gewährleistet, dass er als alleiniger Verantwortlicher zur Verarbeitung der personenbezogenen Daten berechtigt ist und seine Informationspflichten gegenüber den betroffenen Personen erfüllt hat sowie – soweit erforderlich – alle nach den anwendbaren Datenschutzgesetzen erforderlichen Einwilligungen eingeholt hat oder einholen wird, damit der Auftragsverarbeiter berechtigt ist, die personenbezogenen Daten im Auftrag des Verantwortlichen gemäß diesem AVV zu verarbeiten.

Die Einzelheiten der Verarbeitung, insbesondere Art, Umfang und Zweck der Verarbeitung sowie die Kategorien personenbezogener Daten und betroffener Personen, sind in **Anlage 1** geregelt. Die Anlage kann aktualisiert werden, sofern sich Änderungen in Bezug auf die Verarbeitung ergeben.
Ungeachtet dessen erkennt der Verantwortliche an und stimmt zu, dass der Auftragsverarbeiter im Rahmen der Erbringung der Dienstleistungen berechtigt ist, Informationen im Zusammenhang mit dem Betrieb, der Unterstützung oder der Nutzung der Dienstleistung oder im Zusammenhang damit gewonnene Informationen für eigene rechtmäßige interne Geschäftszwecke zu verwenden, insbesondere (i) zur nutzungs- oder nutzerbasierten Abrechnung der Dienstleistungen, (ii) zur Erbringung und Verwaltung der Dienstleistungen, (iii) zur funktionalen und technischen Weiterentwicklung der Dienstleistungen, (iv) zur Einhaltung gesetzlicher Verpflichtungen (einschließlich der Beantwortung behördlicher Anfragen), (v) zur Gewährleistung der Sicherheit der Dienstleistungen sowie (vi) zur Verhinderung von Betrug und Missbrauch oder zur Risikominimierung. Soweit es sich bei diesen Informationen um personenbezogene Daten handelt, verpflichtet sich der Auftragsverarbeiter, (a) diese personenbezogenen Daten ausschließlich in Übereinstimmung mit den anwendbaren Datenschutzgesetzen und nur für Zwecke zu verarbeiten, die mit den in diesem Abschnitt genannten Zwecken vereinbar sind, und (b) diese personenbezogenen Daten nicht für andere Zwecke zu verwenden oder an Dritte weiterzugeben, es sei denn, die Daten wurden zuvor so anonymisiert, dass weder der Verantwortliche noch eine sonstige natürliche oder juristische Person anhand der Daten identifiziert werden kann.

4. Subunternehmer und Unterauftragsverarbeiter

Der Auftragsverarbeiter ist berechtigt, Unterauftragsverarbeiter zur Verarbeitung der Daten einzusetzen. Der Auftragsverarbeiter hat dem Verantwortlichen auf Anfrage Informationen zu den eingesetzten Unterauftragsverarbeitern zur Verfügung zu stellen. Beabsichtigt der Auftragsverarbeiter wesentliche Änderungen hinsichtlich der eingesetzten Unterauftragsverarbeiter, hat er den Verantwortlichen hierüber vorab schriftlich zu informieren. Der Verantwortliche ist berechtigt, den Einsatz eines bestimmten Unterauftragsverarbeiters aus berechtigtem Grund zu untersagen. Untersagt der Verantwortliche den Einsatz eines bestimmten Unterauftragsverarbeiters und ist es dem Auftragsverarbeiter nicht möglich oder nicht zumutbar, die betreffenden Leistungen anderweitig zu oder durch einen anderen Unterauftragsverarbeiter oder selbst zu erbringen, ist der Auftragsverarbeiter berechtigt, diesen AVV zu kündigen und die Verarbeitung zu beenden. Dem Verantwortlichen stehen in diesem Fall keine Ansprüche allein aufgrund der Beendigung der Verarbeitung und der Kündigung dieses AVV zu.

Der Auftragsverarbeiter hat mit jedem Unterauftragsverarbeiter einen schriftlichen Vertrag zu schließen, der die nach den anwendbaren Datenschutzgesetzen erforderlichen Bestimmungen enthält und dem Unterauftragsverarbeiter im Wesentlichen die gleichen Verpflichtungen auferlegt, denen der Auftragsverarbeiter nach diesem AVV unterliegt. Der Auftragsverarbeiter haftet für das Verhalten seiner Unterauftragsverarbeiter wie für eigenes Verhalten.

5. Datensicherheit

Der Auftragsverarbeiter hat geeignete technische, physische und organisatorische Maßnahmen zu treffen und umzusetzen, um ein angemessenes Sicherheitsniveau bei der Verarbeitung personenbezogener Daten zu gewährleisten und personenbezogene Daten vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung, Beschädigung, Veränderung oder unbefugter Offenlegung zu schützen. Bei der Beurteilung des angemessenen Sicherheitsniveaus sind insbesondere die Weisungen des Verantwortlichen, der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schweregrade der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

Geeignete Maßnahmen können insbesondere umfassen: (i) die Pseudonymisierung und Verschlüsselung personenbezogener Daten; (ii) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang auf Dauer sicherzustellen; (iii) die Fähigkeit, die Verfügbarkeit personenbezogener Daten

und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; sowie (iv) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Der Auftragsverarbeiter stellt sicher, dass jede natürliche Person, die seiner Weisungsbefugnis unterliegt und Zugang zu personenbezogenen Daten hat, diese ausschließlich entsprechend den Weisungen des Verantwortlichen verarbeitet, sofern und soweit keine gesetzliche Verpflichtung zur anderweitigen Verarbeitung besteht. Der Auftragsverarbeiter ist nach Maßgabe seiner internen Richtlinien für die Erstellung von Sicherungskopien (Backups) der in seinem Besitz befindlichen Daten und Dateien des Verantwortlichen sowie für deren Funktionsfähigkeit verantwortlich.

Unbeschadet der vorstehenden Anforderungen ist der Auftragsverarbeiter verpflichtet, mindestens solche technischen und organisatorischen Maßnahmen umzusetzen, die im Wesentlichen den in **Anlage 2** beschriebenen Maßnahmen entsprechen.

6. Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass – soweit dies angemessen und möglich ist – nur solche Personen Zugriff auf personenbezogene Daten erhalten, die diesen Zugriff zur Erfüllung des Zwecks dieses AVV benötigen. Der Auftragsverarbeiter stellt ferner sicher, dass alle zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen.

7. Internationale Datenübermittlungen

7.1 Zulässigkeit von Datenübermittlungen

Der Auftragsverarbeiter ist berechtigt, personenbezogene Daten in Staaten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums zu übermitteln. Der Auftragsverarbeiter hat dabei stets die Voraussetzungen und Anforderungen der anwendbaren Datenschutzgesetze einzuhalten, insbesondere durch den Einsatz der von der Europäischen Kommission veröffentlichten Standardvertragsklauseln für Datenübermittlungen.

7.2 Auftragsverarbeiter im EWR und Verantwortlicher außerhalb des EWR

Befindet sich der Auftragsverarbeiter im Europäischen Wirtschaftsraum (EWR) und der Verantwortliche außerhalb des EWR, richtet sich die Übermittlung personenbezogener Daten nach Modul 4 der Standardvertragsklauseln, die durch Bezugnahme in diesen AVV einbezogen werden und einen integralen Bestandteil dieses AVV bilden. Der Verantwortliche schließt die Standardvertragsklauseln als „Datenimporteur“ ab, der Auftragsverarbeiter als „Datenexporteur“.

Für die Zwecke der Standardvertragsklauseln gilt:

a. Modul 4 findet Anwendung;
b. die optionale Docking-Klausel (Klausel 7) findet Anwendung;
c. der optionale Wortlaut in Klausel 11 wird gestrichen;
d. in Klausel 17 gilt das materielle Recht Finnlands;
e. in Klausel 18 werden Streitigkeiten vor den zuständigen Gerichten in Helsinki, Finnland, entschieden; und
f. die Anhänge der Standardvertragsklauseln gelten als mit den in diesem AVV einschließlich seiner Anlagen enthaltenen Informationen ausgefüllt.

Soweit und sofern die Standardvertragsklauseln im Hinblick auf die Übermittlung personenbezogener Daten vom Verantwortlichen an den Auftragsverarbeiter im Widerspruch zu Bestimmungen dieses Vertrags oder dieses AVV stehen, gehen die Standardvertragsklauseln insoweit vor.

Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter außerhalb des EWR, hat der Auftragsverarbeiter mit diesem Unterauftragsverarbeiter die Standardvertragsklauseln (Modul 3) abzuschließen. Jede weitere Übermittlung personenbezogener Daten hat im Einklang mit dem jeweils anwendbaren Modul der Standardvertragsklauseln zu erfolgen.

8. Verletzungen des Schutzes personenbezogener Daten und Meldepflichten

Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich nach Kenntniserlangung über jede tatsächliche oder vermutete Verletzung des Schutzes personenbezogener Daten zu informieren.

Der Auftragsverarbeiter stellt dem Verantwortlichen sämtliche ihm vorliegenden Informationen über die Verletzung des Schutzes personenbezogener Daten zur Verfügung, soweit diese für die Erfüllung der Untersuchungs- und Meldepflichten des Verantwortlichen erforderlich sind. Sofern dem Auftragsverarbeiter zum Zeitpunkt der Meldung noch nicht alle Informationen vorliegen, hat er diese unverzüglich nachzureichen, sobald sie verfügbar sind. Der Auftragsverarbeiter unterstützt den Verantwortlichen im Übrigen angemessen bei der Untersuchung der Verletzung des Schutzes personenbezogener Daten sowie bei damit zusammenhängenden Meldungen an Aufsichtsbehörden und betroffene Personen. Der Auftragsverarbeiter hat zudem angemessene Maßnahmen zu ergreifen, um die nachteiligen Auswirkungen der Verletzung zu begrenzen, die Verletzung zu beheben und künftige Verletzungen zu verhindern. Der Auftragsverarbeiter ist nicht berechtigt,

ohne vorherige ausdrückliche schriftliche Zustimmung und Weisung des Verantwortlichen gegenüber Dritten, insbesondere Medienvertretern, Stellung zu nehmen, es sei denn, eine solche Offenlegung ist nach anwendbaren Datenschutzgesetzen zwingend erforderlich.

Sofern und soweit nicht anwendbare Datenschutzgesetze oder Anordnungen zuständiger Behörden etwas anderes vorschreiben, entscheidet der Verantwortliche nach eigenem Ermessen über die Notwendigkeit sowie die Art und Weise einer Meldung an Aufsichtsbehörden oder sonstige betroffene Stellen. Beabsichtigt der Auftragsverarbeiter, eine Verletzung des Schutzes personenbezogener Daten gegenüber Behörden oder sonstigen Dritten zu melden, bedarf dies der vorherigen Zustimmung des Verantwortlichen.

9. Dokumentation und Auditrechte

Die Parteien sind verpflichtet, einander alle erforderlichen Informationen und Unterlagen zur Verfügung zu stellen, die zur Überprüfung der Einhaltung dieses AVV sowie der anwendbaren Datenschutzgesetze erforderlich sind.

Der Auftragsverarbeiter hat dem Verantwortlichen auf Anfrage zu ermöglichen, die Verarbeitung, die Dienstleistungen, die technischen und organisatorischen Maßnahmen sowie die entsprechenden Systeme und Prozesse des Auftragsverarbeiters zu auditieren sowie an solchen Audits in angemessenen Abständen mitzuwirken, um die Einhaltung dieses AVV und der anwendbaren Datenschutzgesetze sicherzustellen. Solche Audits dürfen höchstens einmal jährlich durchgeführt werden, es sei denn, es bestehen konkrete Anhaltspunkte dafür, dass der Auftragsverarbeiter gegen diesen AVV oder anwendbare Datenschutzgesetze verstößt. Die Audits können auch Vor-Ort-Audits in den Geschäftsräumen oder sonstigen Einrichtungen des Auftragsverarbeiters umfassen. Die Audits sind während der üblichen Geschäftszeiten und so durchzuführen, dass der Geschäftsbetrieb des Auftragsverarbeiters nicht unangemessen beeinträchtigt wird. Jede Partei trägt ihre im Zusammenhang mit dem Audit entstehenden jeweils eigenen Kosten. Geplante Audits sind dem Auftragsverarbeiter mit einer Frist von mindestens fünfzehn (15) Tagen vorab anzukündigen. Die im Rahmen eines Audits erlangten Informationen über die Tätigkeit des Auftragsverarbeiters sind vertraulich zu behandeln.

10. Unterstützung des Verantwortlichen

Der Auftragsverarbeiter hat den Verantwortlichen auf Anfrage des Verantwortlichen und auf dessen Kosten in angemessenem Umfang bei der Erfüllung seiner Pflichten nach den anwendbaren Datenschutzgesetzen zu unterstützen. Die Verpflichtung zur Unterstützung umfasst insbesondere:

10.1 Zugriff auf personenbezogene Daten

Soweit personenbezogene Daten nicht unmittelbar über die Dienstleistungen verfügbar sind, stellt der Auftragsverarbeiter dem Verantwortlichen diese auf Anfrage zur Verfügung. Sofern die Daten in elektronischer Form vorliegen, sind sie dem Verantwortlichen auch in dieser Form bereitzustellen.

10.2 Wahrnehmung der Rechte betroffener Personen und Anfragen von Aufsichtsbehörden

Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren (i) über sämtliche Anfragen, Beschwerden oder Mitteilungen von Aufsichtsbehörden oder sonstigen zuständigen Behörden; sowie (ii) über Anfragen von betroffenen Personen, die ihm unmittelbar zugehen und die die Wahrnehmung der Rechte betroffener Personen betreffen. Eine unmittelbare Beantwortung solcher Anfragen durch den Auftragsverarbeiter ist nur zulässig, wenn und soweit der Verantwortliche dies zuvor ausdrücklich gestattet und entsprechende Weisungen erteilt hat. Auf Anfrage des Verantwortlichen hat der Auftragsverarbeiter diesen in angemessenem Umfang bei der Beantwortung behördlicher Anfragen sowie bei der Wahrnehmung der Rechte betroffener Personen nach den anwendbaren Datenschutzgesetzen zu unterstützen.

10.3 Datenschutz-Folgenabschätzung

Erlangt der Auftragsverarbeiter Kenntnis davon, dass eine geplante Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, hat er den Verantwortlichen hierüber zu informieren und diesen bei Bedarf bei der Durchführung einer Datenschutz-Folgenabschätzung zu unterstützen.

10.4 Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten

Der Auftragsverarbeiter muss entweder (i) die Möglichkeit bereitstellen, personenbezogene Daten über die Funktionen der Dienstleistungen zu berichtigen, zu löschen oder die Verarbeitung einzuschränken, oder (ii) personenbezogene Daten entsprechend den Weisungen des Verantwortlichen zu berichtigen, zu löschen oder die Verarbeitung einzuschränken.

11. Laufzeit und Beendigung

11.1 Inkrafttreten und Beendigung

Sofern nicht anders vereinbart, tritt dieser AVV gleichzeitig mit dem Vertrag in Kraft und bleibt solange gültig, wie der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen im Zusammenhang mit der Erbringung der Dienstleistungen verarbeitet. Ungeachtet der Beendigung dieses AVV bleiben diejenigen Bestimmungen dieses AVV, die ihrer Natur nach über die Beendigung hinaus fortgelten sollen, auch nach Beendigung dieses AVV wirksam.

11.2 Rückgabe oder Löschung personenbezogener Daten nach Beendigung der Verarbeitung

Nach Beendigung dieses AVV hat der Auftragsverarbeiter nach Wahl des Verantwortlichen entweder sämtliche im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten zu löschen oder diese an den Verantwortlichen zurückzugeben und etwaige vorhandene Kopien zu löschen, sofern nicht anwendbare Datenschutzgesetze oder sonstige Vorschriften (z. B. ISO 17025) eine Aufbewahrung der personenbezogenen Daten verlangen. In diesem Fall ist der Auftragsverarbeiter berechtigt, die personenbezogenen Daten im Einklang mit den gesetzlichen Anforderungen aufzubewahren, ohne sie darüber hinaus weiter zu verarbeiten, und unter fortbestehender Einhaltung der in diesem AVV geregelten Vertraulichkeitsverpflichtungen. Die Rückgabe oder Löschung personenbezogener Daten hat unverzüglich auf entsprechende Weisung des Verantwortlichen zu erfolgen. Erteilt der Verantwortliche keine Weisung zur Rückgabe oder Löschung der personenbezogenen Daten, ist der Auftragsverarbeiter berechtigt, die in seinem Besitz befindlichen personenbezogenen Daten nach Ablauf von zwölf (12) Monaten nach Beendigung dieses AVV zu löschen. Der Auftragsverarbeiter hat die personenbezogenen Daten in einem gängigen und datensicheren elektronischen Format oder in einem zwischen den Parteien vereinbarten Format zurückzugeben.

12. Sonstige Bestimmungen

12.1 Änderungen

Änderungen dieses AVV bedürfen der Schriftform und der ausdrücklichen Vereinbarung zwischen den Parteien. Die vom Verantwortlichen jeweils erteilten schriftlichen Weisungen zur Durchführung der Verarbeitung personenbezogener Daten stellen keine Änderungen dieses AVV dar.

12.2 Verantwortlichkeiten und Haftung

Erleidet eine betroffene Person aufgrund eines Verstoßes gegen die anwendbaren Datenschutzgesetze einen Schaden, richtet sich die Haftung des Verantwortlichen und des Auftragsverarbeiters nach Artikel 82 der Datenschutz-Grundverordnung (DSGVO). Jede Partei trägt die Verantwortung für gegen sie verhängte Verwaltungsbußgelder einer Aufsichtsbehörde aufgrund von Verstößen gegen die anwendbaren Datenschutzgesetze. Die Haftung einer Partei gegenüber der anderen Partei wegen einer Verletzung dieses AVV ist der Höhe nach insgesamt auf einen Betrag begrenzt, der den auf Grundlage des Vertrags gezahlten Netto-Dienstleistungsentgelten für die sechs (6) Monate vor Geltendmachung des ersten Schadensersatzanspruchs entspricht. Im Übrigen gelten die im Vertrag zwischen den Parteien oder dessen Anlagen enthaltenen Haftungsbeschränkungen entsprechend für diesen AVV. Soweit nicht ausdrücklich anders geregelt, haftet eine Partei gegenüber der anderen Partei nicht für mittelbare Schäden, Folgeschäden, zufällige Schäden, besondere Schäden oder Strafschadensersatz (einschließlich Schäden durch Betriebsunterbrechung sowie entgangene Nutzung, Datenverlusten, Umsatz- oder Einkommenseinbußen oder entgangenem Gewinn); solche Schäden sind ausgeschlossen.

12.3 Anwendbares Recht und Streitbeilegung

Hinsichtlich des anwendbaren Rechts und der Streitbeilegung gelten die Bestimmungen des Vertrags zwischen den Parteien, sofern und soweit die anwendbaren Datenschutzgesetze nichts Abweichendes vorsehen. Enthält der Vertrag keine Regelungen zum anwendbaren Recht oder zur Streitbeilegung, unterliegt dieser AVV dem materiellen Recht des Staates, in dem der Auftragsverarbeiter seinen Sitz hat.

13. Anlagen

Dieser AVV besteht aus diesem Dokument sowie den nachfolgend aufgeführten Anlagen:

- Anlage 1: Beschreibung der Verarbeitungstätigkeiten
- Anlage 2: Technische und organisatorische Maßnahmen zur Informationssicherheit

Anlage 1 zum AVV (und gegebenenfalls zu den Standardvertragsklauseln)

A. LISTE DER PARTEIEN

Datenexporteur:

Name: Beamex Oy Ab

Anschrift: Ristisuonraitti 10, 68600 Pietarsaari, FINNLAND

Für die Datenübermittlung relevante Tätigkeiten: Beamex ist ein Technologieunternehmen, das Kalibriergeräte, Software sowie damit verbundene Dienstleistungen und Supportleistungen für industrielle Kunden herstellt und bereitstellt. Der Datenimporteur ist ein Kunde von Beamex und Nutzer der digitalen Dienstleistungen von Beamex, auf die sich dieser AVV bezieht.

Rolle (Verantwortlicher/Auftragsverarbeiter):
Auftragsverarbeiter

Datenimporteur(e):

Name: wie im zwischen dem Datenimporteur und Beamex Oy Ab geschlossenen Vertrag angegeben

Anschrift: wie im Vertrag angegeben

Für die Datenübermittlung relevante Tätigkeiten: Der Datenimporteur ist ein Kunde von Beamex und nutzt die digitalen Dienstleistungen von Beamex.

Rolle (Verantwortlicher/Auftragsverarbeiter):
Verantwortlicher

Wesentliche Unterauftragsverarbeiter des Auftragsverarbeiters zum Zeitpunkt des Abschlusses dieses AVV:

a. **Microsoft Datacenter Netherlands B.V.** Da Beamex Oy Ab Azure-Cloud-Dienste (PaaS) – West Europe – auf Grundlage der Microsoft Product Terms nutzt, richten sich die Bedingungen für Datenverarbeitung und Datensicherheit nach dem Microsoft Online Services Data Protection Addendum (DPA).
b. **Bjorkstrom Oy Ab** mit Sitz in Finnland; Verarbeitungstätigkeiten umfassen insbesondere die Entwicklung und Bereitstellung von LOGiCAL.

B. BESCHREIBUNG DER ÜBERMITTLUNG/VERARBEITUNG

	Digitale Dienstleistungen und Cloud-Software von Beamex (z. B. LOGiCAL)	**Weitere Dienstleistungen von Beamex (z. B. Software-Support, Datenmigration, Systemintegration)**
Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden:	In erster Linie Mitarbeiter oder Subunternehmer des Verantwortlichen, die Kalibrierungen mit Kalibriergeräten von Beamex durchführen und deren Ergebnisse anschließend in der Kalibriersoftware von Beamex gespeichert werden.	In erster Linie Mitarbeiter oder Subunternehmer des Verantwortlichen, die Kalibrierungen mit Kalibriergeräten von Beamex durchführen und deren Ergebnisse anschließend in der Kalibriersoftware von Beamex gespeichert werden.

Kategorien der übermittelten personenbezogenen Daten:	Insbesondere Name, Berufsbezeichnung, Name des Arbeitgebers sowie Daten im Zusammenhang mit den Tätigkeiten, die die betroffene Person unter Verwendung von Kalibriergeräten von Beamex durchgeführt hat.	Insbesondere Name, Berufsbezeichnung, Name des Arbeitgebers sowie Daten im Zusammenhang mit den Tätigkeiten, die die betroffene Person unter Verwendung von Kalibriergeräten von Beamex durchgeführt hat.
Häufigkeit der Übermittlung:	Die Datenübermittlung erfolgt fortlaufend sowie anlassbezogen, soweit dies zur Erbringung der Dienstleistungen erforderlich ist	Die Datenübermittlung erfolgt anlassbezogen.
Art der Verarbeitung:	Einräumung von Nutzungsrechten an der Kalibriersoftware von Beamex zugunsten des Verantwortlichen sowie Speicherung von Kalibrierdaten in der Software über die von Mitarbeitern und Subunternehmern des Verantwortlichen durchgeführten Kalibrierungen.	Erbringung von Helpdesk-, Support- und Wartungsleistungen gegenüber den Kunden von Beamex sowie Durchführung von Migrations- und Integrationsleistungen im Zusammenhang mit Softwareprodukten, in deren Rahmen eine Verarbeitung personenbezogener Daten erfolgen kann.
Zweck(e) der Datenübermittlung und der weiteren Verarbeitung:	Nutzung der Kalibriersoftware von Beamex zur Speicherung von Kalibrierergebnissen.	Ermöglichung der Nutzung der Produkte von Beamex, deren Implementierung sowie deren Betrieb, auch in Verbindung mit anderen Systemen.
Dauer der Speicherung der personenbezogenen Daten bzw. Kriterien für die Festlegung dieser Dauer:	Für die Dauer des zugrunde liegenden Vertrags sowie solange der Verantwortliche die digitalen Dienstleistungen von Beamex nutzt.	Für die Dauer des Vertrags sowie solange Beamex personenbezogene Daten als Auftragsverarbeiter zu den genannten Zwecken verarbeitet.
ZUSTÄNDIGE AUFSICHTSBEHÖRDE:	Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) Adresse: Lintulahdenkuja 4, 00530 Helsinki, FINNLAND Allgemeine Rufnummer: +358 29 566 6700, Geschäftsstelle: +358 29 566 6768 www.tietosuoja.fi	

Anlage 2 zum AVV (und gegebenenfalls zu den Standardvertragsklauseln)

Beschreibung der technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter zusätzlich zu den im AVV genannten allgemeinen Verpflichtungen umzusetzen hat, um ein angemessenes Niveau der Datensicherheit zu gewährleisten.

Bereich	Maßnahmen und Verfahren
Microsoft Azure (PaaS)	**Die Dienste Beamex LOGiCAL und Beamex Sync basieren auf Microsoft Azure (PaaS). Das Microsoft Service Trust Portal enthält alle relevanten Zertifizierungen, Berichte und Dokumentationen zur Geschäftskontinuität (ISO 22301) sowie zu Informationssicherheits-Managementsystemen (ISO 27001 und weitere Normen der ISO-27000-Reihe) unter https://servicetrust.microsoft.com/viewpage/ISOIEC**
Räumlichkeiten und physische Sicherheit	**Zutritt zu Räumlichkeiten** Der Auftragsverarbeiter beschränkt den Zutritt zu seinen Räumlichkeiten durch den Einsatz persönlicher Identifikationskarten (RFID). Zugriffsrechte auf verschiedene Bereiche der Räumlichkeiten werden auf Grundlage von durch die Geschäftsleitung und Vorgesetzte festgelegten Berechtigungen vergeben. Bestimmte besonders schutzbedürftige Bereiche können zusätzlichen Schutz- und Zutrittskontrollmaßnahmen unterliegen. Besucher erhalten ausschließlich Zutritt zu öffentlich zugänglichen Bereichen (z. B. Empfangsbereich, Kantine, Sanitäranlagen) und dürfen sich in den Räumlichkeiten des Auftragsverarbeiters nur in Begleitung eines Mitarbeiters bewegen. **Alarmsysteme und Sicherung der Einrichtungen** Die Sicherung der Räumlichkeiten wird an ein professionelles Sicherheitsunternehmen ausgelagert. Die Räumlichkeiten sind mit branchenüblichen Alarmsystemen ausgestattet, einschließlich Systemen zur Erkennung unbefugten Zutritts, zur Überwachung von Laborbedingungen, zur Kontrolle von Kühlung und Temperatur in IT-Rechenzentren, Alarmen der Klimaanlagen sowie Brandmeldesystemen. Der Leiter Technischer Dienste ist für die technische Wartung der Zutrittskontroll- und Alarmsysteme verantwortlich. Die Mitarbeiter sind geschult oder verfügen über entsprechende Anweisungen zum Verhalten in Alarm- oder Krisensituationen; bestimmte Szenarien werden regelmäßig geübt.
Personal, Organisation und Informationssicherheitsmanagement	**Personalsicherheit** Die mit den Mitarbeitern abgeschlossenen Arbeitsverträge enthalten branchenübliche Vertraulichkeitsklauseln. In bestimmten Fällen können zusätzliche Vertraulichkeitsvereinbarungen abgeschlossen werden (z. B. im Rahmen spezifischer Projekte und/oder in Bezug auf bestimmte Informationen). Die Mitarbeiter sind ferner verpflichtet, sämtliche vom Auftragsverarbeiter vorgegebenen Richtlinien und Vorgaben einzuhalten, insbesondere solche zu Geschäftsethik, Datenschutz und Informationssicherheit. **Schulungen und Richtlinien** Eine verpflichtende Schulung zur Informationssicherheit ist Bestandteil des Einarbeitungsprogramms für neue Mitarbeiter. Zusätzliche allgemeine oder spezifische Schulungen zur Informationssicherheit werden für die Mitarbeiter regelmäßig durchgeführt. Geschäftsleitung, Vorgesetzte, Systemverantwortliche, für die Zugriffskontrolle zuständige Personen sowie sonstige Verantwortliche werden in Bezug auf die Inhalte der Informationssicherheitsrichtlinie des Auftragsverarbeiters sowie deren zukünftige Aktualisierungen geschult. Viele dieser Personen nehmen zudem an Risikoanalysen sowie an Überprüfungen, Schulungen und/oder Übungen im Bereich Business Continuity Management teil. Für Mitarbeiter bestehen gegebenenfalls spezifische Richtlinien in verschiedenen Bereichen, etwa zur Nutzung von E-Mail, zum Fernzugriff und mobilen Arbeiten, zu eingesetzten Tools und Software sowie zur Verwaltung von Dateien, Dokumenten und Aufzeichnungen. **Management, Überwachung, Überprüfungen und Audits** Die Bewertung von Risiken im Bereich Informationssicherheit und Business Continuity ist Bestandteil der Audits des Qualitätsmanagementsystems des Unternehmens. Auf Grundlage von Feststellungen und identifizierten Risiken sowie im Zusammenhang mit neuen Entwicklungsprojekten oder Änderungen an Systemen, Einrichtungen oder Prozessen werden gesonderte Risikoanalysen, Prüfungen und Maßnahmenpläne erstellt. Zur Bewertung des technischen Niveaus der Informationssicherheit werden – soweit möglich oder erforderlich – externe Experten, Peer Reviews oder Audits herangezogen. Die IT-Abteilung des Unternehmens ist für die Ausgestaltung und Umsetzung der Informationssicherheit verantwortlich und übernimmt wesentliche operative und technische Maßnahmen in diesem Bereich. Die IT-Abteilung ist in der Geschäftsleitung des Unternehmens vertreten.
Business Continuity	Der Auftragsverarbeiter unterhält Pläne und Maßnahmen zur Sicherstellung der Geschäftskontinuität sowie zur Wiederherstellung nach Störungen (Disaster Recovery).

Dritte, Subunternehmer, Auftragsverarbeiter und Unterauftragsverarbeiter	**Hintergrundprüfung und Verträge** Vor Aufnahme einer Geschäftsbeziehung werden Dritte, Subunternehmer und Unterauftragsverarbeiter in angemessenem Umfang einer Überprüfung unterzogen. Drittanbieter werden vertraglich zur Vertraulichkeit verpflichtet. Mit Partnern, die als Auftragsverarbeiter oder Unterauftragsverarbeiter tätig werden, werden schriftliche Vereinbarungen zur Auftragsverarbeitung (oder entsprechende Vertragsanlagen) geschlossen. Soweit erforderlich werden von dem Auftragsverarbeiter eingesetzte Dritte auch im Hinblick auf die Informationssicherheit geschult oder entsprechend angewiesen. **IT-Beschaffung** Computer, mobile Endgeräte, Systeme und Software werden vorrangig durch die IT-Abteilung beschafft. Lizenzinformationen werden ebenfalls durch die IT-Abteilung erfasst und verwaltet.
Interne Daten, Server und Netzwerke von Beamex	**Zugriffskontrolle und Authentifizierung** Der Auftragsverarbeiter setzt branchenübliche Maßnahmen ein, um Personen und Nutzer zu authentifizieren sowie den Zugriff auf Systeme, Software, Dateien und Daten zu beschränken und unbefugte Zugriffe zu verhindern. Beim Zugriff auf das Netzwerk über Fernverbindungen wird grundsätzlich eine Zwei-Faktor-Authentifizierung verlangt. Ziel ist es, in Anwendungen vorrangig ein domänenbasiertes Single Sign-on zu verwenden. Passwörter müssen mindestens acht (8) Zeichen lang sein; bevorzugt werden jedoch starke Passwörter mit mindestens vierzehn (14) Zeichen, die Sonderzeichen, Zahlen und Großbuchstaben enthalten. Der Zugriff auf bestimmte Dateien kann zusätzlich durch system-, ordner- oder dokumentenspezifische Berechtigungen eingeschränkt werden. **E-Mail-Kommunikation** Es bestehen Richtlinien für die Nutzung und den Umgang mit E-Mail-Kommunikation. Beim Versand und Empfang vertraulicher Informationen werden besondere Sicherheitsanforderungen berücksichtigt. Die Verbindung zwischen E-Mail-Server und Endgerät (z. B. Computer, Telefon, Tablet) erfolgt verschlüsselt. **Dateien und Datenbanken** Für die Speicherung von Daten in Cloud-Umgebungen bestehen geeignete Verfahren und Regelungen. Die Speicherung wesentlicher Daten auf lokalen Festplatten wird nicht empfohlen. Für besonders sensible oder vertrauliche Informationen werden Server und Systeme in den eigenen Rechenzentren des Auftragsverarbeiters genutzt. Für die Ablage sowie Archivierung und Versions- bzw. Lebenszyklusverwaltung von Dokumenten bestehen gesonderte Richtlinien und Verfahren. Für die sichere Übermittlung vertraulicher Informationen an Dritte wird vorrangig „ShareFile“ eingesetzt. Microsoft Office 365 wird insbesondere für die Speicherung und gemeinsame Bearbeitung von Dokumenten im Rahmen der Teamarbeit genutzt (ausgenommen besonders sensible oder hochvertrauliche Informationen). **Fernzugriff** Der Bedarf an Endgeräten, Software und Fernzugriffsmöglichkeiten für mobiles Arbeiten wird durch die zuständigen Vorgesetzten festgelegt. Für den Fernzugriff werden gesicherte Verbindungen (z. B. Client-VPN oder Citrix/XenApp) unter Verwendung von Zwei-Faktor-Authentifizierung eingesetzt. Mobile Endgeräte sind durch Passwort oder Zugriffscode geschützt und werden, soweit erforderlich, durch Mobile-Device-Management (MDM) verwaltet. Für mobiles Arbeiten sowie die Speicherung von Dateien und Daten in Cloud-Systemen können ergänzende Richtlinien bestehen. **Netzwerke, Server und IT-Infrastruktur** Datennetze sind in getrennte Sub- bzw. virtuelle Netzwerke segmentiert. Zur Überwachung des Datenverkehrs sowie zur Erkennung und Verhinderung von Angriffen werden geeignete technische Maßnahmen und Systeme (z. B. Monitoring-, Intrusion-Prevention- und Antiviren-Systeme) eingesetzt. Bestimmte Datenverbindungen sowie kritische Netzkomponenten sind redundant ausgelegt. Ziel ist es, für sämtliche kritischen Komponenten entweder eine Redundanz oder ein Backup-System vorzusehen, um sogenannte Single-Point-of-Failure-(SPOF)-Risiken in Datennetzen, Servern, Speichersystemen und sonstigen kritischen Systemen zu minimieren. Für kritische Geräte und Komponenten werden entsprechende Ersatzteile vorgehalten. Die Stromversorgung kritischer Systeme und Geräte wird durch unterbrechungsfreie Stromversorgungen (USV) abgesichert. Hochverfügbare (HA-)Speichersysteme, Speicher-Spiegelungen sowie andere fehlertolerante Systeme werden für kritische Informationssysteme eingesetzt, soweit dies erforderlich ist. Regelmäßige Image- und System-Backups werden auf virtuellen Servern, Produktionssystemen sowie weiteren kritisch genutzten IT-Systemen gemäß den jeweils geltenden Standardarbeitsanweisungen erstellt. Backups für weitere Systeme werden auf Grundlage einer einzelfallbezogenen Bewertung sowie unter Berücksichtigung einer Risikoeinschätzung durchgeführt. **Backup-Richtlinie** Der Auftragsverarbeiter verfügt über dokumentierte Backup- und Wiederherstellungskonzepte zur Sicherstellung der Verfügbarkeit und Wiederherstellbarkeit von Daten und Systemen. Diese Konzepte werden entsprechend der Kritikalität der jeweiligen Daten und Systeme differenziert angewendet. Für Backups von Daten und Informationssystemen besteht eine gesonderte Standardarbeitsanweisung. **Schadsoftware (Malware)** Der Auftragsverarbeiter implementiert technische und organisatorische Maßnahmen wie Firewalls, Antivirus-, Anti-Malware- und Spamfilter-Systeme sowie vergleichbare Schutzmechanismen, um Cyberangriffe, unbefugte Zugriffe sowie die Installation von Schadsoftware in Daten, Systemen, Netzwerken und Endgeräten zu erkennen, zu verhindern und abzuwehren.

[Ende des AVV.]

Personuppgiftsbiträdesavtal (SV)

1. Inledning, syfte och tillämpning

Detta Personuppgiftsbiträdesavtal (”**DPA**”) tillämpas som en del av det kommersiella avtalet (”**Avtal**”) för behandling av personuppgifter som utförs av en Beamex juridisk enhet som specificeras i erbjudandet, orderbekräftelsen eller Avtalet, såsom Beamex Oy Ab eller något av dess dotterbolag (**”Personuppgiftsbiträde”**) i samband med tillhandahållandet av digitala eller andra tjänster (”**Tjänster**”) till kunden som är en avtalsparter i Avtalet samt datakontrollant för sådan personlig data (”**Personuppgiftsansvarig**”) vars Tjänster beskrivs mer detaljerat i Avtalet som ingåtts mellan Personuppgiftsbiträdet och Personuppgiftsansvarig.

Detta DPA är en integrerad och oskiljaktig del av Avtalet mellan parterna. Alla termer som används i detta DPA, men som inte definieras, har samma betydelse som de har i Avtalet. Om det finns en konflikt mellan Avtalet och detta DPA har villkoren i DPA företräde.

2. Definitioner

”**Personuppgiftsansvarig**” avser den fysiska person eller juridiska enhet, myndighet, agentur eller annan instans som nämns i detta DPA, som ensam eller tillsammans med andra definierar syftena och medlen för behandling av personuppgifter.

”**Dataskyddslag(ar)**” avser dataskyddslagen (1050/2018) och EU:s allmänna dataskyddsförordning (2016/679) med ändringar och ersättningsförordningar samt annan giltig och tillämplig dataskyddslagstiftning och instruktioner samt bindande regler från dataskyddsmyndigheter.

”**Registrerad**” avser en identifierad eller identifierbar fysisk person vars Personuppgifter behandlas på grundval av detta DPA.

”**Personuppgifter**” avser all information som rör en identifierad eller identifierbar fysisk person; en identifierbar fysisk person anses vara en fysisk person som direkt eller indirekt kan identifieras, särskilt utifrån identifieringsinformation såsom namn, personnummer, platsinformation, onlineidentifieringsinformation eller en eller flera fysiska, fysiologiska, genetiska, psykologiska, ekonomiska, kulturella eller sociala faktorer som kännetecknar honom eller henne.

”**Personuppgiftsbrott**” innebär en händelse av dataskyddsbrott som resulterar i oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörig avslöjande eller åtkomst till personuppgifter som överförts, lagrats eller på annat sätt behandlats.

”**Behandling**” betyder den funktion eller de funktioner som tillämpas på Personuppgifter eller datamängder som innehåller Personuppgifter i samband med tillhandahållandet av Tjänster, antingen med hjälp av automatisk databehandling eller manuellt, såsom insamling, lagring, organisering, strukturering, lagring, modifiering eller ändring, söka, fråga, använda, överföra data, distribuera eller på annat sätt göra dem tillgängliga, matcha eller kombinera, begränsa, radera eller förstöra informationen.

”**Personuppgiftsbiträde**” avser den fysiska personen eller juridiska enheten, myndigheten, agenturen eller annan instans som nämns i detta DPA och som behandlar Personuppgifter på uppdrag av den Personuppgiftsansvarige.

”**Standardavtalsklausuler**” avser Standardavtalsklausuler (EU) 2021/914 från och med den 4 juni 2021. Alla hänvisningar till standardavtalsklausulerna ska avse standardavtalsklausulerna, som inkluderar parternas val av vissa moduler och valfria klausuler samt bilaga I till II i detta DPA. Dessutom är parterna överens om att användningen av underbiträden ska regleras av klausul 9, alternativ 1 i standardavtalsklausulerna.

”**Underbiträde**” betyder en fysisk person eller juridisk enhet i ett avtalsförhållande med Personuppgiftsbiträdet, som behandlar Personuppgifter som en underleverantör till Personuppgiftsansvarige som en del av utförandet av Tjänster för den Registrerade.

3. Omfattning av behandling och behandlingsaktiviteter

Enligt detta DPA behandlas sådana personuppgifter, för vilka den Personuppgiftsansvarige agerar som enda Personuppgiftsansvarig.

Personuppgiftsbiträdet behandlar personuppgifter (i) i enlighet med dataskyddslagstiftningen och villkoren i detta DPA för att uppfylla de skyldigheter som beskrivs i Avtalet; och (ii) i enlighet med de skriftliga instruktioner som ges av den Personuppgiftsansvarige från tid till annan, såvida inte annat krävs enligt Dataskyddslags-tiftningen som gäller för Personuppgiftsbiträdet. Personuppgiftsbiträdet får inte behandla personuppgifter för egna ändamål eller överlåta dem till tredje part, såvida inte detta DPA tillåter det. Personuppgiftsbiträdet ska meddela den Personuppgiftsansvarige om det anser eller misstänker att den Personuppgiftsansvariges skriftliga instruktioner bryter mot Dataskyddslagstiftningen. Om inte annat anges i detta DPA eller dess bilagor får Personuppgiftsbiträdet endast behandla Personuppgifter under Avtalets löptid.

Personuppgiftsansvarig (i) åtar sig att följa skyldigheterna i enlighet med Dataskyddslagstiftningen som gäller för den vid Behandling av Personuppgifter; och (ii) ansvarar för att den, som enda Personuppgiftsansvarig, har rätt att behandla personuppgifter och att den har uppfyllt sin skyldighet att informera de registrerade och/eller har fått (eller kommer att få) alla samtycken som krävs enligt tillämplig dataskyddslagstiftning från de registrerade för att Personuppgiftsbiträdet ska behandla personuppgifter för den personuppgiftsansvariges räkning i enlighet med detta DPA.

Mer detaljerad information om behandlingen, såsom arten av behandlingen, typer av personuppgifter och grupper av registrerade, beskrivs i **Bilaga 1**. Bilagan kan uppdateras om ändringar sker i Behandlingen.

Den Personuppgiftsansvarige erkänner och accepterar dock att Personuppgiftsbiträdet som en del av tillhandahållandet av Tjänsterna till den Personuppgifts-ansvarige har rätt att använda information som är relaterad till driften, stödet eller användningen av Tjänsten eller som erhållits i samband med den för sina lagliga och legitima interna affärssyften, såsom (i) fakturering av Tjänsten baserat på användning eller antal användare, (ii) leverans av Tjänsten och för att hantera tillhandahållandet av den, (iii) för funktionell och teknisk utveckling av Tjänsten, (iv) för efterlevnad av tillämpliga lagar (inklusive svar på officiella förfrågningar), (v) för att säkerställa Tjänstens säkerhet, och (vi) för att förhindra bedrägerier och missbruk eller minska risker. I den mån sådan information är Personuppgifter förbinder sig att: (a) behandla sådana Personuppgifter i enlighet med tillämplig Dataskyddslagstiftning och endast för ändamål som är förenliga med de syften som beskrivs i detta avsnitt; och (b) inte använda sådana Personuppgifter för något annat ändamål eller lämna ut dem till tredje part, såvida de inte först har anonymiserat uppgifterna så att den Personuppgiftsansvarige eller någon annan person eller enhet inte kan identifieras utifrån uppgifterna.

4. Underentreprenörer och underbiträden

Personuppgiftsbiträdet har rätt att anlita Underbiträden vid Behandlingen. På begäran ska Personuppgiftsbiträdet tillhandahålla den Personuppgiftsansvarige mer information om de Underbiträden som används. Om Personuppgiftsbiträdet gör väsentliga ändringar av sina Underbiträden ska den meddela den Personuppgifts-ansvarige skriftligen. Den Personuppgiftsansvarige har rätt att förbjuda användning av ett visst Underbiträde av motiverade skäl. Om den Personuppgiftsansvarige förbjuder användning av ett visst Underbiträde och det inte rimligen är möjligt att överföra Underbiträdets uppgifter till någon annan, inklusive Personuppgifts-biträdet, har Personuppgiftsbiträdet rätt att avsluta DPA och avsluta behandlingen. Den Personuppgiftsansvarige har inte rätt till någon ersättning enbart på grund av att Behandlingen upphör och DPA har avslutats på grund av att den Personuppgiftsansvarige förbjuder användning av ett specifikt Underbiträde.

Personuppgiftsbiträdet måste ingå ett skriftligt avtal med varje Underbiträde som innehåller de villkor som krävs enligt dataskyddslagstiftningen och i huvudsak liknande typer av skyldigheter som Personuppgiftsbiträdet har enligt detta DPA. Personuppgiftsbiträdet ansvarar för de Underbiträden som man använder, precis som för sina egna handlingar.

5. Datasäkerhet

Personuppgiftsbiträdet ska vidta lämpliga tekniska, fysiska och organisatoriska åtgärder för att säkerställa en hög säkerhetsnivå i Personuppgiftsbiträdets Behandling av Personuppgifter och för att skydda Personuppgifter från obehörig eller olaglig behandling och från oavsiktlig förlust, förstörelse, skada, ändring eller överföring. Vid utvärdering av nödvändiga åtgärder för att garantera säkerhetsnivån, den Personuppgiftsansvariges instruktioner, den senaste tekniken och implementeringskostnaderna, Behandlingens art, omfattning, sammanhang och syften samt riskerna för fysiska personers rättigheter och friheter, vilka varierar i sannolikhet och allvarlighetsgrad, måste beaktas.

Tillämpliga åtgärder kan till exempel vara: (i) pseudonymisering och kryptering av Personuppgifter; (ii) förmågan att garantera systemens och Tjänsternas kontinuerliga sekretess, integritet, tillgänglighet och feltolerans; (iii) möjligheten att snabbt återställa tillgången till Personuppgifter och åtkomst till Personuppgifter i händelse av ett fysiskt eller tekniskt fel; och (iv) förfarandet för regelbunden testning, granskning och utvärdering av effektiviteten hos tekniska och organisatoriska åtgärder för att säkerställa säkerheten för behandlingen. Personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som arbetar under Personuppgiftsbiträdet och som har tillgång till Personuppgifter endast behandlar dem i enlighet med den Personuppgiftsansvariges instruktioner, om inte annat krävs enligt tillämplig dataskyddslagstiftning. Personuppgiftsbiträdet ansvarar, i enlighet med sina egna policyer, för att ta säkerhetskopior av den Personuppgiftsansvariges data och filer i sin besittning och för att kontrollera deras funktionalitet.

Utan att begränsa de krav och skyldigheter som beskrivs ovan, måste Personuppgiftsbiträdet alltid genomföra minst de tekniska och organisatoriska informations-säkerhetsåtgärder som i huvudsak motsvarar de åtgärder som beskrivs i **Bilaga 2**.

6. Konfidentialitet

Personuppgiftsbiträdet ska, i den mån det är rimligen möjligt, säkerställa att endast de personer som agerar för dess räkning och som har behov av att få tillgång till informationen för att uppfylla syftet med detta DPA har tillgång till Personuppgifterna och att de personer som har rätt att behandla Personuppgifterna är skyldiga att följa sekretessförpliktelsen eller omfattas av lämplig lagstadgad sekretessförpliktelse.

7. Internationella dataöverföringar

7.1 Tillåtna överföringar

Personuppgiftsbiträdet kan överföra till ett land utanför Europeiska unionen eller Europeiska ekonomiska samarbetsområdet. Personuppgiftsbiträdet måste alltid följa villkoren och kraven i Dataskyddslagstiftningen vid överföring av uppgifter till länder utanför Europeiska unionen eller Europeiska ekonomiska samarbetsområdet, till exempel genom att använda standardavtalsklausuler som publicerats av EU-kommissionen och som gäller för dataöverföring.

7.2 Personuppgiftsbiträden inom EES och den personuppgiftsansvarige utanför EES

Om Personuppgiftsbiträdet är beläget inom EES och den Personuppgiftsansvarige utanför EES ska överföringen av Personuppgifter regleras av Modul 4 i Standardavtalsklausulerna, som införlivas häri genom hänvisning och utgör en integrerad del av DPA. Den Personuppgiftsansvarige ingår standardavtalsklausulerna som ”uppgiftsimportör” och Personuppgiftsbiträdet som ”uppgiftsexportör”.

För ändamålen med standardavtalsklausulerna:

a) modul fyra ska tillämpas,
b) den valfria dockningsklausulen, klausul 7, ska gälla,
c) I klausul 11 ska det valfria språket strykas,
d) i klausul 17 ska Finlands materiella lagstiftning gälla,
e) i klausul 18 ska tvister avgöras i Helsingfors tingsrätt och
f) bilagorna till standardavtalsklausulerna ska fyllas i med den information som anges i DPA, inklusive dess bilagor.

Om och i den utsträckning som standardavtalsklausulerna strider mot någon bestämmelse i avtalet eller DPA avseende överföring av Personuppgifter från Personuppgiftsansvarig till Personuppgiftsbiträde ska standardavtalsklausulerna ha företräde i den utsträckning som en sådan konflikt föreligger.

Om Personuppgiftsbiträdet är beläget inom EES och anlitar ett Underbiträde som är beläget utanför EES ska Personuppgiftsbiträdet ingå standardavtalsklausuler (Modul 3) med sådant Underbiträde. All vidare överföring av Personuppgifter måste följa tillämplig modul i standardavtalsklausulerna.

8. Personuppgiftsincidenter och rapporteringsskyldigheter

Personuppgiftsbiträdet ska meddela den Personuppgiftsansvarige om alla faktiska eller misstänkta personuppgiftsincidenter utan onödigt dröjsmål efter att ha fått kännedom om incidenten.

Personuppgiftsbiträdet ska förse den Personuppgiftsansvarige med all tillgänglig information om personuppgiftsincidenten som den Personuppgiftsansvarige kan behöva för att uppfylla sina egna utrednings- och rapporteringsskyldigheter. Personuppgiftsbiträdet kan senare komplettera informationen om det inte har omfattande information om överträdelsen omedelbart tillgänglig. Personuppgiftsbiträdet ska i övrigt bistå och samarbeta med den Personuppgiftsansvarige i utredningen av personuppgiftsincidenten och i eventuella frågor som rör anmälningar till myndigheter och intressenter. Personuppgiftsbiträdet ska också vidta nödvändiga rimliga uppföljningsåtgärder för att mildra de negativa effekterna av personuppgiftsincidenten, åtgärda den inträffade överträdelsen eller förhindra framtida överträdelser.

Personuppgiftsbiträdet får inte kommentera personuppgiftsincidenten till tredje part, särskilt mediarepresentanter, utan uttryckligt skriftligt samtycke och instruktioner från den Personuppgiftsansvarige, om inte annat krävs enligt dataskyddslagstiftningen.

Såvida inte annat krävs enligt dataskyddslagstiftningen eller behörig myndighets föreskrift fattar den Personuppgiftsansvarige det slutliga beslutet efter eget gottfinnande om huruvida personuppgiftsincidenten ska anmälas till myndigheterna eller andra berörda parter, och på vilket sätt sådana anmälningar kan göras. Om Personuppgiftsbiträdet rapporterar en personuppgiftsincident till myndigheter eller andra intressenter måste det godkännas i förväg av den Personuppgiftsansvarige.

9. Dokumentations- och revisionsrättigheter

En part är skyldig att tillhandahålla den andra parten all information och alla dokument som krävs för att visa efterlevnad av detta DPA och dataskyddslagstiftningen.

På den Personuppgiftsansvariges begäran måste Personuppgiftsbiträdet också tillåta revisioner av Behandlingen, Tjänsterna, informationssäkerhetsåtgärderna och Personuppgiftsbiträdets informationssystem och processer och delta i sådana revisioner med rimliga intervall i syfte att säkerställa efterlevnad av detta DPA och dataskyddslagstiftningen. Sådana revisioner får utföras högst en gång per år, såvida det inte finns skälig anledning att anta att Personuppgiftsbiträdet inte följer DPA eller dataskyddslagstiftningen. Revisioner kan även omfatta besök på Personuppgiftsbiträdets kontor eller andra fysiska lokaler. Revisionen genomförs under normal arbetstid och på ett sådant sätt att den inte i onödan stör Personuppgiftsbiträdets verksamhet. I samband med revisionen ansvarar vardera parten för sina egna kostnader. Personuppgiftsbiträdet ska underrättas om planerade revisioner minst femton (15) dagar före den avsedda revisionen. Information om Personuppgiftsbiträdets verksamhet som den Personuppgiftsansvarige erhåller under revisionen är konfidentiell.

10. Bistå personuppgiftsansvarige

Personuppgiftsbiträdet ska, på begäran och bekostnad av den Personuppgiftsansvarige, rimligen bistå den Personuppgiftsansvarige med att uppfylla de skyldigheter som Personuppgiftsansvarige har i enlighet med dataskyddslagstiftningen. Skyldigheten att bistå gäller särskilt i följande frågor:

10.1 Tillgång till personuppgifter

I den mån Personuppgifterna inte är tillgängliga direkt genom Tjänsterna ska Personuppgiftsbiträdet på begäran tillhandahålla de aktuella uppgifterna till den Personuppgiftsansvarige. Om informationen är tillgänglig i elektronisk form ska den också levereras till den Personuppgiftsansvarige i den formen.

10.2 Uppfyllande av den registrerades rättigheter och begäran från tillsynsmyndigheten

Personuppgiftsbiträdet ska utan dröjsmål meddela den Personuppgiftsansvarige: (i) alla förfrågningar, klagomål eller meddelanden från tillsynsmyndigheten eller annan behörig myndighet och (ii) från alla förfrågningar som mottagits direkt från den registrerade, i samband med uppfyllandet av den registrerades rättigheter. Personuppgiftsbiträdet får endast svara direkt på begäran om den Personuppgiftsansvarige i förväg har gett tillstånd och instruktioner att göra det. Om den Personuppgiftsansvarige begär det ska Personuppgiftsbiträdet rimligen bistå den Personuppgiftsansvarige med att besvara officiella förfrågningar och uppfylla den registrerades rättigheter enligt dataskyddslagstiftningen.

10.3 Konsekvensbedömning av dataskydd

Om Personuppgiftsbiträdet blir medvetet om att den planerade Behandlingen skulle medföra en hög risk med avseende på en fysisk persons rättigheter och friheter ska den Personuppgiftsansvarige informeras om detta och vid behov bistå den Personuppgiftsansvarige med att genomföra en konsekvensbedömning avseende dataskydd.

10.4 Korrigering, radering och begränsning av personuppgifter

Personuppgiftsbiträdet ska antingen (i) erbjuda möjligheten att korrigera, radera eller begränsa behandlingen av Personuppgifter genom Tjänstens funktioner eller (ii) korrigera, radera eller begränsa behandlingen av Personuppgifter i enlighet med den Personuppgiftsansvariges instruktioner.

11. Avtalsperiod och upphörande

11.1 Ikraftträdande och uppsägning

Om inget annat överenskommits träder detta DPA i kraft samtidigt som Avtalet och förblir giltigt så länge Personuppgiftsbiträdet behandlar Personuppgiftsansvarigs Personuppgifter i samband med tillhandahållandet av dess Tjänster. Oavsett uppsägning av DPA förblir bestämmelserna i DPA, som är av sådan karaktär att de är avsedda att fortsätta gälla oavsett uppsägning av Avtalet, i kraft oavsett uppsägning av DPA.

11.2 Återlämnande eller radering av Personuppgifter vid behandlingens slut

Vid uppsägning av DPA måste Personuppgiftsbiträdet, efter den Personuppgiftsansvariges val, antingen radera alla Personuppgifter som behandlas för den Personuppgiftsansvariges räkning eller, alternativt, återlämna alla Personuppgifter till den Personuppgifts-ansvarige och radera befintliga kopior, såvida inte dataskyddslagstiftningen eller annan förordning (t.ex. ISO 17025) kräver lagring av Personuppgifter.

I sådant fall har Personuppgiftsbiträdet rätt att behålla Personuppgifterna i enlighet med kraven i lagen, utan att i övrigt fortsätta Behandlingen av Personuppgifterna och ändå följa de sekretessförpliktelser som beskrivs i detta DPA. Återlämning eller radering av Personuppgifter ska ske utan onödigt dröjsmål efter den Personuppgifts-ansvariges begäran. Om den Personuppgiftsansvarige inte har gett några instruktioner om radering eller återlämning av Personuppgifter kan Personuppgiftsbiträdet på eget initiativ radera de Personuppgifter som finns i dess besittning när tolv (12) månader har gått från avslutet av DPA. Personuppgiftsbiträdet ska återlämna Personuppgifterna i ett allmänt använt, datasäkert elektroniskt format eller i ett annat format som parterna kommer överens om.

12. Övriga villkor

12.1 Ändringar

Alla ändringar av detta DPA måste avtalas skriftligen mellan parterna. För tydlighetens skull anges att de skriftliga instruktioner som ges av den Personuppgifts-ansvarige från tid till annan för att utföra Behandlingen av Personuppgifter inte anses vara ändringar av detta DPA.

12.2 Ansvar och ansvarsskyldighet

Om den Registrerade lider skada på grund av ett brott mot dataskyddslagstiftningen fastställs den Personuppgiftsansvariges och Personuppgiftsbiträdets ansvar för skadan i enlighet med artikel 82 i EU:s allmänna dataskyddsförordning (2016/679). Varje part ansvarar för eventuella administrativa böter som åläggs av tillsynsmyndigheten på grund av ett brott mot dataskyddslagstiftningen. En parts skadeståndsansvar gentemot den andra parten på grund av avtalsbrott mot detta DPA är ett totalt maximibelopp som motsvarar de momsfria avgifter för Tjänster som betalats på grundval av Avtalet under de sex (6) månader som föregår inlämnandet av det första skadeståndsanspråket. I övrigt gäller de villkor för Ansvarsbegränsning som kan finnas i Avtalet mellan parterna eller dess bilagor även för detta DPA. Såvida inte annat uttryckligen anges häri är en part inte ansvarig gentemot den andra för indirekta, följdmässiga, tillfälliga, special- eller straffskador (inklusive eventuella skador för verksamhetsavbrott och förlorad användning, data, försäljning, intäkter eller vinst), som uttryckligen utesluts.

12.3 Tillämplig lag och tvistlösning

Vad gäller Tillämplig lag och Tvistlösning ska villkoren i Avtalet mellan parterna följas, om inte dataskyddslags-tiftningen anger annat. Om Avtalet inte anger Tillämplig lag eller innehåller villkor för Tvistlösning ska DPA regleras av den materiella lagstiftningen i Personuppgiftsbiträdets hemvist.

13. Bilagor

Detta DPA består av detta dokument och de bilagor som anges nedan:

- Bilaga 1: Beskrivning av behandlingsaktiviteter
- Bilaga 2: Tekniska och organisatoriska informationssäkerhetsåtgärder

Bilaga 1 till DPA (och i förekommande fall till standardavtalsklausuler)

A. FÖRTECKNING ÖVER PARTER

Dataexportör:

Namn: Beamex Oy Ab

Adress: Ristisuonraitti 10, 68600 Pietarsaari, FINLAND

Aktiviteter som är relevanta för de uppgifter som överförs enligt dessa klausuler: Beamex är ett teknikföretag som tillverkar och tillhandahåller kalibreringsutrustning, programvara och relaterade Tjänster och support till sina industrikunder. Uppgiftsimportören är kund hos Beamex och användare av Beamex digitala tjänster som detta DPA avser.

Roll (personuppgiftsansvarig/personuppgiftsbiträde): Personuppgiftsbiträde.

Dataimportör(er):

Namn: det namn som anges i det handelsavtal som ingåtts med Beamex Oy Ab.

Adress: enligt handelsavtalet.

Aktiviteter som är relevanta för de uppgifter som överförs enligt dessa klausuler: Uppgiftsimportören är kund hos Beamex och använder Beamex digitala tjänster.

Roll (personuppgiftsansvarig/personuppgiftsbiträde): Personuppgiftsansvarig.

Personuppgiftsbiträdets väsentliga Underbiträden vid tidpunkten för ingåendet av DPA:

a) **Microsoft Datacenter Netherlands B.V.** Eftersom Beamex Oy Ab prenumererar på Azure molntjänster (PaaS) - Västeuropa enligt villkoren på sidan Microsoft Product Terms, där definieras villkoren för databehandling och säkerhet i Microsoft Online Services Data Protection Addendum (DPA).
b) **Bjorkstrom Oy Ab** – hemmahörande i Finland, bearbetningsaktiviteter inkluderar utveckling och implementering av LOGiCAL.

B. BESKRIVNING AV ÖVERFÖRING/BEHANDLING

	Beamex digitala tjänster och molnprogramvara (t.ex. LOGiCAL)	**Andra Beamex-tjänster (t.ex. programvarusupport, datamigrering, systemintegration)**
Kategorier av Registrerade vars Personuppgifter överförs:	Främst sådana anställda eller underleverantörer till Personuppgiftsansvarige som använder och utför kalibreringar med Beamex kalibreringsutrustning, vars resultat sedan lagras i Beamex kalibreringsprogramvara.	Främst sådana anställda eller underleverantörer till Personuppgiftsansvarige som använder och utför kalibreringar med Beamex kalibreringsutrustning, vars resultat sedan lagras i Beamex kalibreringsprogramvara.
Kategorier av överförda personuppgifter:	Särskilt namn, befattning, arbetsgivarens namn samt uppgifter om de aktiviteter personen utfört med Beamex kalibreringsutrustning.	Särskilt namn, befattning, arbetsgivarens namn samt uppgifter om de aktiviteter personen utfört med Beamex kalibreringsutrustning.
Överföringsfrekvensen:	Data överförs både kontinuerligt och vid behov för att tillhandahålla tjänsten/tjänsterna.	Efter behov.
Typ av behandling:	Tillhandahålla användarrättigheter till Beamex kalibreringsprogramvara till Personuppgiftsansvarige och lagra kalibreringsdata i programvaran för de kalibreringar som styrenhetens anställda och underleverantörer har utfört.	Tillhandahållande av helpdesk-, support- och underhållstjänster till Beamex kunder samt tillhandahållande av migrerings- och integrationstjänster relaterade till programvaruprodukter, under vilka behandling av Personuppgifter kan förekomma.
Syftet/syftena med dataöverföringen och vidare behandling:	Användning av Beamex kalibreringsprogramvara för lagring av kalibreringsresultat.	För att möjliggöra användning av Beamex produkter, deras implementering och/eller deras drift tillsammans med andra system.
Den period under vilken Personuppgifter kommer att lagras, eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period:	Det kommersiella avtalets löptid och så länge som den Personuppgiftsansvarige använder Beamex digitala tjänster.	Varaktigheten för det kommersiella avtalet och så länge Beamex behandlar uppgifterna som Personuppgiftsbiträde för ändamålen.
BEHÖRIG TILLSYNSMYNDIGHET:	Dataombudsmannens byrå (Tietosuojavaltuutetun toimisto) Gatuadress: Lintulahdenkuja 4, 00530 Helsingfors, FINLAND Växel: +358 29 566 6700, Register: +358 29 566 6768 www.tietosuoja.fi	

Bilaga 2 till DPA (och i förekommande fall till standardavtalsklausuler)

En beskrivning av de tekniska och organisatoriska åtgärder som Personuppgiftsbiträdet måste vidta utöver de allmänna skyldigheter som nämns i DPA för att säkerställa en lämplig nivå av datasäkerhet.

Område	Planer och rutiner
Microsoft Azure (PaaS)	**Beamex LOGiCALoch Beamex Sync-tjänster bygger på Azure (PaaS). Microsoft Service trust portal listar alla relevanta affärskontinuitets (ISO22301) och ISMS (ISO27001 och andra 27000-serien) certifieringar, rapporter, dokument etc., på adress https://servicetrust.microsoft.com/viewpage/ISOIEC**
Lokaler och fysisk säkerhet	**Tillgång till lokaler.** Personuppgiftsbiträdet begränsar tillträdet till sina lokaler med personliga ID-kort (RFID). Tillträdesrättigheter till olika områden inom lokalerna beviljas utifrån behörigheter som definieras av ledningen och arbetsledare. Vissa särskilda områden kan ha utökade skyddsåtgärder och tillträdeskontroll. Gäster har endast tillträde till offentliga lokaler (lobby, kafeteria, toaletter) och rör sig endast i Personuppgiftsbiträdets lokaler tillsammans med en värd. **Larmsystem och bevakning av anläggningar.** Bevakning av lokaler utkontrakteras till ett professionellt bevakningsföretag. Lokalerna har branschstandardiserade larmsystem, inklusive larm för obehörigt tillträde, övervakning av laboratorieförhållanden, kylning/temperatur i IKT-datacenter, luftkonditioneringslarm och brandlarmsystem. Företagets chef för tekniska tjänster ansvarar för det tekniska underhållet av tillträdesövervaknings- och larmsystemen. Medarbetarna har utbildats eller fått instruktioner om hur de ska agera i olika larm- eller krissituationer. Vissa situationer kan övas regelbundet.
Personal-, organisations- och informationssäkerhetshantering	**Personsäkerhet.** Anställningsavtal som tecknas med anställda innehåller en branschstandardiserad sekretessklausul. I vissa särskilda situationer kan ytterligare sekretessavtal tecknas (t.ex. specifika projekt och/eller information). Medarbetarna är också skyldiga att följa alla riktlinjer eller policyer som Personuppgiftsbiträdet kan ha, inklusive men inte begränsat till de som rör affärsetik, integritet och informationssäkerhet. **Utbildning och riktlinjer.** En obligatorisk utbildning inom informationssäkerhet är en del av introduktionsprogrammet för alla nya medarbetare. Ytterligare allmän eller specifik utbildning inom informationssäkerhet anordnas för medarbetarna från tid till annan. Ledning, arbetsledare, systemägare, åtkomstkontroll och andra ansvariga personer utbildas i innehållet i Personuppgiftsbiträdets informationssäkerhetspolicy och dess framtida revideringar. Många av dessa personer deltar också i granskningar, utbildningar och/eller övningar av riskhantering och affärskontinuitetsplanering. Det kan finnas särskilda riktlinjer för medarbetare inom olika områden, såsom arbets e-post, fjärråtkomst och distansarbete, verktyg och programvara samt hantering av filer, dokument och register. **Ledning, övervakning, granskningar och revisioner.** Bedömningen av informations-säkerhets- och affärskontinuitetsrisker ingår i företagets kvalitetssystemrevisioner. Separata riskbedömningar, inspektioner och utvecklingsplaner görs utifrån fynd, identifierade risker och alltid i samband med nya utvecklingsprojekt eller planerings-system/anläggningar/processförändringar. Externa experter, kollegiala granskningar eller revisioner används när så är möjligt eller nödvändigt för bedömning av den tekniska informationssäkerhetsnivån. Företagets IKT-funktion hanterar ramverket för informationssäkerhet och ansvarar för många praktiska och tekniska informationssäkerhetsåtgärder. IKT är representerat i bolagets ledningsgrupp.
Kontinuitet i verksamheten	Personuppgiftsbiträdet upprätthåller planer och åtgärder för affärskontinuitet och katastrofåterställning.
Tredje parter, underleverantörer, Personuppgiftsbiträden och Underbiträden	**Bakgrund och avtal.** Bakgrundskontroll av tredje part, underleverantörer och Underbiträden görs som bedöms lämpligt och nödvändigt innan affärsrelationen inleds. Tredjeparts samarbetspartners är avtalsenligt bundna till sekretess. Skriftliga personuppgiftsbiträdesavtal (eller bilagor) ingås med sådana partners som betraktas som personuppgiftsbiträden eller underbiträden till Personuppgiftsbiträdet. Om och när det är relevant kan utbildning eller instruktioner tillhandahållas till tredje parter som anlitas av Personuppgiftsbiträdet i frågor som även rör informationssäkerhet. **IT-upphandling.** Datorer, mobila apparater, system och mjukvara anskaffas främst av IT-funktionen. Licensinformation registreras och lagras även av IT.

Beamex interna data, servrar och nätverk	**Åtkomstkontroll och autentisering.** Personuppgiftsbiträdet använder branschstandard-åtgärder för att autentisera personer och användare, begränsa åtkomst (samt förhindra obehörig åtkomst) till system, programvara, filer och data. Tvåfaktorsautentisering krävs i första hand när du loggar in på nätverket från en fjärranslutning. Målet är att i första hand använda domänens single sign-on i applikationerna. Lösenord måste vara minst 8 tecken långa, men starka lösenord på 14 tecken som innehåller specialtecken, siffror och stora bokstäver rekommenderas. Åtkomsten till vissa filer kan också begränsas till system-, mapp- och dokumentspecifika åtkomsträttigheter. **E-post.** Det finns riktlinjer för e-postkommunikation. Särskilda e-postsäkerhetsfrågor måste beaktas när konfidentiell information skickas eller tas emot. Anslutningen mellan e-postservern och den slutliga apparaten (dator, telefon, surfplatta osv.) är krypterad. **Filer och databaser.** Det finns olika metoder för att lagra data i molnet. Vi rekommenderar inte att viktiga data sparas på en lokal dators hårddisk. Servrar och system i Person-uppgiftsbiträdets egna lokaler används för att spara känslig eller mycket konfidentiell information. Det finns separata riktlinjer och rutiner för lagring och hantering av dokument som kräver arkivering eller versions- och livscykelhantering. Sharefile är det primära verktyget för att leverera konfidentiell information till tredje part på ett säkert sätt. Microsoft Office365 används i stor utsträckning för att lagra och dela dokument som används i teamarbete (med undantag för mycket känslig eller mycket konfidentiell information). **Fjärranslutningar.** Arbetsledare definierar behovet av apparater, programvara och fjärranslutningar för mobilt arbete. Säker klient-VPN eller Citrix/XenApp med tvåfaktorsautentisering krävs för distansarbete. Mobila apparater är lösenords-/kodskyddade och i förekommande fall MDM-styrda. Det kan finnas separata policyer för mobilt arbete och lagring av filer och dokument i molnet. **Nätverk, servrar och IT-infrastruktur.** Datanätverken är uppdelade i separata sub/virtuella nätverk. Lämpliga verktyg och/eller tjänster används för trafikövervakningen, intrångsförebyggande och observation samt AV-övervakning. Vissa dataanslutningar och kritiska Edge nätverkskomponenter dupliceras. Syftet är att arrangera antingen duplicering eller en backup-apparat för alla kritiska komponenter för att minska s.k. SPOF-risker (single point of failure) i datanätverk, servrar, lagringar och andra kritiska system. Ett eget lager upprätthålls för reservdelar och komponenter till kritiska apparater. Strömförsörjningen till vissa kritiska system och apparater backas upp av en avbrottsfri strömförsörjning (UPS). Lagringssystem med hög tillgänglighet (HA), lagringsspegling eller andra feltoleranta system som övervägs för kritiska informationssystem kan användas. Regelbundna bild-/systembackuper utförs på virtuella servrar, produktionssystem och vissa andra datorer i kritisk användning, i enlighet med gällande standardrutin. Systembackuper implementeras i övriga objekt enligt fallspecifik övervägande och riskbedömning. **Backup-policy.** Personuppgiftsbiträdet har olika backupplaner och åtgärder i syfte att återställa data och system. Planerna och åtgärderna kan variera beroende på datans och systemets betydelse. Personuppgiftsbiträdet har en separat standardrutin för säkerhetskopiering av data och informationssystem. **Skadlig programvara.** Personuppgiftsbiträdet upprätthåller brandväggar samt antivirus, antimalware, spamfiltrering och andra liknande tekniska åtgärder för att upptäcka, förhindra och skydda mot externa cyberattacker, obehörig åtkomst och installation av skadlig programvara i sina data, system, nätverk och apparater.

[Slut på DPA.]