Personal Data Processing Agreement for Add-On Products' Cloud Services

1. Background

1.1 Purpose and Application.

This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between Add-On Products and Customer. This DPA applies to Personal Data processed by Add-On Products and its Sub Processors in connection with its provision of the Hosted Cloud Service. This DPA does not apply to non-production environments of the Hosted Cloud Service if such environments are made available by Add-On Products, and Customer shall not store Personal Data in such environments.

1.2 Structure

Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organizational measures.

1.3 GPDR

Add-On Products and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/ Controllers that is processed under the DPA.

In the event that Add-On Products transfers personal data out of the European Area to Customers placed in third countries, applicable Data Protection Laws, including but not limited to the General Data Protection Regulation 2016/679 ("GDPR"), the UK GDPR and Data Protection Act 2018, the Hong Kong Personal Data (Privacy) Ordinance ("PDPO"), and the California Consumer Privacy Act ("CCPA") as amended by the California Privacy Rights Act (CPRA), shall apply.

1.4 Governance

Add-On Products acts a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents, and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use Add-On Products as a Processor. Where authorizations, consent, instructions, or permissions are provided be Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where Add-On Products informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use Cloud Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

2. Security of Processing

2.1 Appropriate Technical and Organizational Measures.

Add-On Products has implemented and will apply the technical and organizational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate considering the state of the art, the costs of implementation, nature, scope, context, and purposes of the processing of Personal Data.

2.2 Changes

Add-On Products applies the technical and organizational measures set forth in Appendix 2 to Add-On Products' entire customer base hosted out of the same Data Center and receiving the same Cloud Service. Add-On Products may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3. Add-On Products Obligations

3.1 Instructions from Customer

Add-On Products will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions, and each use of the Cloud Service then constitutes further instructions. Add-On Products will use reasonable efforts to follow any other Customer instructions, if they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or Add-On Products otherwise cannot comply with an instruction or is if the opinion that an instruction infringes Data Protection Law, Add-On Products will immediately notify Customer (email permitted).

3.2 Processing on Legal Requirement.

Add-On Products may also process Personal Data where required to do so by applicable law. In such a case, Add-On Products shall inform Customer of that legal requirement before processing unless that law prohibits such information on important ground of public interest.

3.3 Personnel

To process Personal Data, Add-On and its Sub processors shall only grant access to authorized personnel who have committed themselves to confidentiality. Add-On Products and Its Sub processors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

3.4 Cooperation

At the request from the Customer, Add-On will reasonably cooperate with the Customer and Controllers in managing requests from Data Subjects or regulatory authorities relating to Add-On Products' processing of Personal Data or a Personal Data breach. Add-On Products will promptly inform the Customer of any request received from a Data Subject regarding Personal Data processing and will not respond to the request without further instructions from the Customer, as applicable. Add-On Products shall provide functionality that supports the Customer's ability to correct or remove Personal Data from the Cloud Service or to restrict its processing in accordance with Data Protection Law. In situations where such functionality is not provided.

3.5 Personal Data Breach Notification

Add-On will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data protection Law. Add-On Products may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by Add-On Products.

3.6 Data Protection Impact Assessment

If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, Add-On Products will provide such documents as are generally available for the Cloud Service (for example, This DPA, the Agreement, an Executive Security summery) Any additional assistance shall be mutually agreed between the Parties.

If Customer (or its Controllers) is required under Data Protection Law to conduct a data protection impact assessment or prior consultation with a regulator, Add-On Products will provide the Customer with generally available documents related to the Cloud Service, such as this DPA, the Agreement and executive security summary, upon request. Any further assistance required by the Customer will be mutually agreed upon by the Parties. This may include providing additional documentation or answering specific questions related to the processing of Personal Data by Add-On Products. Add-On Products shall reasonably cooperate with the Customer to ensure that all necessary information is made available to the Customer to fulfil its obligations under Data Protection Law.

4. Data Export and Deletion

4.1 Export and Retrieval by Customer

During the Subscription Term, Export and retrieval of Personal Data may be subject to technical limitations, which may restrict Customer's ability to access or retrieve such data. In such cases, Add-On Products and the Customer shall work together to identify a reasonable method to enable the Customer to access the Personal Data. This may include identifying alternative methods of access or retrieval, modifying existing processes, or upgrading technical capabilities, as appropriate and agreed upon by the Parties. The availability and feasibility of such methods shall be subject to the terms and conditions of the Agreement between the Parties. Add-On Products shall make reasonable efforts to ensure that any technical limitations are identified and addressed in a timely and efficient manner to minimize any impact on the Customer's ability to access or retrieve Personal Data. Any costs associated with such export will be at the expense of the Customer, unless otherwise agreed upon by the Parties in the Agreement.

4.2 Deletion

At the end of Subscription Term, Add-On Products deletes the Personal Data remaining on servers hosting the Cloud Service within a reasonable time in line with Data Protection Law (not to exceed six months) unless applicable law requires retention.
If the Customer requests it, Add-On Products shall provide written confirmation that such deletion has been completed in accordance with this section.

5. Certifications and Audits

5.1 Customer Audit

Customer, or an independent third-party auditor reasonably acceptable to Add-On Products (provided that such auditor is not a competitor of Add-On Products, and is suitably qualified and independent), may conduct an audit

of Add-On's control environment and security practices relevant to Personal Data processed by Add-On Products if any of the following circumstances occur:

A) Add-On Products has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the data Center where Personal Data is processed by the Cloud Service, as demonstrated by a certification or attestation report issued by an independent third-party auditor reasonably acceptable to Add-On Products. The certification or attestation report should cover the controls and procedures implemented by Add-On Products in accordance with industry best practices and applicable laws and regulations. Upon request, audit reports or certifications are available through the third-party auditor or Add-On Products. The costs for such an audit will be at the expense of the Customer.

B) In the event of a Personal Data Breach, Add-On Products shall inform the Customer via detailed report of the breach. Add-On Products will conduct a thorough investigation of the breach and remit all necessary precautions, hereby avoiding a similar event.

C) An audit is formally requested by Customer's data protection authority; or

D) Mandatory Data Protection Law provides Customer with a direct audit right, in which case Customer may only audit once in any twelve-month period unless mandatory Data Protection Law requires more frequent audits. The costs for such an audit will be at the expense of the Customer.

5.2 Other Controller Audit

Any other Controller may audit Add-On Products control Environment and security practices relevant to Personal Data processed by Add-On Products in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by Add-On Products based on the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

5.3 Scope of Audits

Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audits reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to Add-On Products.

5.4 Cost of Audits

Customer shall bear the costs of any audit unless such audit reveals a material breach by Add-On Products of this DPA, then Add-On Products shall bear its own expenses of an audit. If an audit determines that Add-On Products has breached its obligations under the DPA, Add-On Products will promptly remedy the breach at its own cost.

6. Sub processors

6.1 Permitted use.

Add-On Products is granted a general authorization to subcontract the processing of Personal Data to Sub processors, provided that:

(a) Add-On Products shall engage Subprocesses under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Suppressor's processing of Personal Data. Add-On Products shall be liable for any breaches by the sub processor in accordance with the terms of this DPA; and

(b) Add-On Products will evaluate the security, privacy, and confidentiality practices of a sub processor prior to selection to establish that it can provide the level of protection of Personal Data required by this DPA; and

(c) Add-On Products' list of Sub processors in place on the effective date of the Agreement is published by Add-On Products or Add-On Products will make it available to Customer upon request, including the name, address, and role of each sub processor Add-On Products uses to provide the Cloud Service.

6.2 New Sub processors

(a) Add-On Products will inform Customer in advance (by email or by posting on the designated Add-On Products product page) of any intended additions or replacements to the list of Sub processors including name, address, and role of the new Sub processor.; and

(b) Customer may object to such changes as set out in Section 6.3

6.3 Objections to New Sub processors

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Sub processors processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Sub processor is intended to be used) on written notice to Add-On Products. Such termination shall only take effect at the Agreement Renewal. If Customer does not terminate, then Customer is deemed to have accepted the new Sub processor.

(b) After Add-On Products´ notice to Customer informing Customer of the new Sub processor, Customer may request that the parties come together in good faith to discuss resolution to the objection.

(c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

6.4 Emergency Replacement

Add-On Products may replace a Sub processor without advance notice where the reason for the change is outside of Add-On Products' reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Add-On Products will inform Customer of the replacement Sub processor as soon as possible following its appointment. Section 6.3 applies accordingly.

7. International Processing

7.1 Conditions for International Processing

Add-On Products shall be entitled to process Personal Data, including by using Sub processors, in accordance with the DPA outside the country in which the Customer is located as permitted under Data Protection Law.

7.2 Standard Contractual Clauses

Where (i) Personal Data of an EEA, UK, Hong Kong, US or Swiss based Controller is processed in a country outside the EEA, Switzerland or any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another

Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering Standard Contractual Clauses, then:

(a) Add-On Products and Customer enter the Standard Contractual Clauses.
(b) Customer enters Standard Contractual Clauses with each relevant Sub processor as follows, either (i) Customer joins the Standard Contractual Clauses entered by Add-On Products or the Sub processor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Sub processor (represented by Add-On Products) enters the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply when Add-On Products has expressly confirmed that a Sub processor is eligible for it through the Sub processor list provided under Section 6.1(c), or a notice to Customer; and/ or
(c) Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter Standard Contractual Clauses with Add-On Products and / or the relevant sub processors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter Standard Contractual Clauses on behalf of the other Controllers.

Relation of the Where (i) Personal Data of an EEA, UK, Hong Kong, US or Swiss based Controller is processed in a country outside the EEA, Switzerland or any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering Standard Contractual Clauses, then:

(a) Add-On Products and Customer enter the Standard Contractual Clauses.
(b) Customer enters Standard Contractual Clauses with each relevant Sub processor as follows, either (i) Customer joins the Standard Contractual Clauses entered by Add-On Products or the Sub processor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Sub processor (represented by Add-On Products) enters the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply when Add-On Products has expressly confirmed that a Sub processor is eligible for it through the Sub processor list provided under Section 6.1(c), or a notice to Customer; and/ or
(c) Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter Standard Contractual Clauses with Add-On Products and / or the relevant sub processors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter Standard Contractual Clauses on behalf of the other Controllers.

7.3 Relation of the Standard Contractual Clauses to the Agreement

Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and sub processor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.

7.4 Governing Law of the Standard Contractual Clauses

The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.
The venue shall be the courts of Denmark when dispute resolution before a court in an EU Member State is required under the GDPR, the Data Protection Legislation, or under this DPA.

Disputes between the Parties, not subject to Clause 11(b), arising out of this DPA or related to the subject matter of privacy as regulated by this DPA, shall be finally settled by arbitration administered by the Danish Institute of Arbitration with its Rules of Arbitration in force at the time when such proceedings are commenced. The arbitral tribunal shall consist of three (3) arbitrators. The arbitration shall take place in Copenhagen, Denmark, and shall in all aspects be treated as confidential. The arbitration shall be conducted in the English language unless the Parties agree otherwise. The award of the arbitrators shall be final and binding on both Parties. The Parties may agree on another venue for resolving an identified current dispute. Such agreement must be made in writing and signed by both Parties and cannot include a general deviation of governing venue a stated in this Clause 11(b) and (c).

8. Documentation; Records of Processing

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), to enable the other party to comply with any obligations relating to maintaining records of processing.

9. EU Access

9.1 Optional Service

EU Access is an optional service that may be offered by Add-On Products. Add-On Products shall provide the Cloud Service eligible for EU Access solely for production instances in accordance with this Section 9.

9.2 EU Access

Add-On Products will use only European sub processors to provide support requiring access to Personal Data in the Cloud Service and Add-On Products shall not export Personal Data outside of the EEA or Switzerland unless expressly authorized by Customer in writing (e-mail permitted) on a case-by-case basis; or as excluded under Section 9.4.

9.3 Data Center Location

The Data Centers used to host Personal Data in the Cloud Service are located in North America, and the European Economic Area (EEA). Add-On Products will not migrate the Customer instance to a Data Center outside of these regions without prior written consent from the Customer (e-mail permitted). If Add-On Products plans to migrate the Customer instance to a Data Center within these regions, Add-On Products will notify the Customer in writing (e-mail permitted) no later than thirty days before the planned migration. Consent for migration will be obtained through a formal request process, which will consider factors such as the potential impact on service performance and data security.

9.4 Exclusions

The following Personal Data is not subject to 9.2 and 9.3:

(a) Contact details of the sender of a support ticket; and

(b) Any other Personal Data submitted by Customer when filling a support ticket. Customer may choose not to transmit Personal Data when filling a support ticket. If this data is necessary for the incident management process, Customer may choose to anonymize that Personal Data before any transmission of the incident message to Add-On Products.

10. Definitions

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

10.1 “Controller”

The data controller determines the purposes for which and the means by which personal data is processed.

10.2 “Data Center”

Data Center means the location where the production instance of the Cloud Service is hosted for the customer in its region, as listed in 9.3 or as otherwise agreed.

10.3 “Data protection Law”

Data Protection Law means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by Add-On Products on behalf of Customer, the GDPR as minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

10.4 “Data Subject”

Data Subject means an identified or identifiable natural person as defined by Data Protection Law.

10.5 “EEA”

EEA means the European Economic Area, namely the European Union Member States along with Island, Liechtenstein, Switzerland, Norway.

10.6 “European Sub processor”

European Sub processor means a Sub processor that is physically processing Personal Data in the EEA.

10.7 “Personal Data”

Personal Data means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by Add-On Products or its sub processors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

10.8 “Personal Data Breach”

Personal Data Breach means a confirmed (1) accidental or unlawful destruction, loss alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

10.9 “Processor”

Processor means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller, be it directly as processor of a controller or indirectly as sub processor of a processor which processes personal data on behalf of the controller.

10.10 “Standard Contractual Clauses”

Standard Contractual Clauses or sometimes also referred to the “EU Model Clauses” means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply).

10.11 “Sub processor”

Sub processor means Microsoft Azure and third parties engaged by Add-On products in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses

Data Exporter

The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.

Data Importer

Add-On Products and its Sub processor Microsoft Azure provide the Cloud Service that includes the following support:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud service
- Monitoring, troubleshooting, and administering the underlying Cloud Service infrastructure and database.
- Security monitoring, network-based intrusion detection Support, penetration testing

Add-On Products provide support when a customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorized Users. Add-On Products answers phones and performs basic troubleshooting and handles support tickets in a tracking system that is separate from the productions instance of the Cloud Service.

Data Subjects

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having personal Data stored in the Cloud Service.

Data Categories

The transferred Personal Data concerns the following categories of data:

Customer determines the categories of data per Cloud Service subscribed. Customer can configure data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data:

- Employee names, email addresses, telephone numbers, meeting data
- Visitor names, email addresses, telephone numbers, meeting data
- Supplier names, email addresses, telephone numbers, meeting data
- Customer names, email addresses, telephone numbers, meeting data

Special Data Categories (if appropriate)

The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including Order Form) if any.

Processing Operations / Purposes

The transferred Personal Data is subject to the following basic processing activities:

- Use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
- Provision of Consulting Services.
- Communication to Authorized Users
- Storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- Upload any fixes or upgrades to the Cloud Service
- Back up of Personal Data
- Computer processing of Personal Data, including data transmission, data retrieval, data access
- Network access to allow Personal Data transfer
- Execution of instructions of Customer in accordance with the Agreement.

Appendix 2
Technical and Organizational Measures

1 Technical and Organizational Measures

The following sections outline the present technical and organizational measures in place at Add-On Products. Please note that Add-On Products reserves the right to modify these measures without prior notice, as long as they maintain an equivalent or higher level of security. Some individual measures may be substituted with new ones that serve the same purpose, while maintaining the same level of security for Personal Data.

1.1 Physical Access Control

Add-On Products do not store any data from the Customer, these are stored by third party PaaS supplier Microsoft Azure. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/ or use Personal Data are located as published at "Azure facilities, premises, and physical security" (Physical security of Azure datacenters - Microsoft Azure | Microsoft Docs)

1.2 System Access Control

To prevent unauthorized use, access to data processing systems used to provide the Cloud Service is restricted to authorized personnel only. Microsoft Azure, the third-party PaaS supplier used by Add-On Products, has implemented a range of system access controls to ensure that data processing systems are only used with proper authorization. These controls are published in detail at "Azure Customer data protection" (Protection of customer data in Azure | Microsoft Docs)

1.3 Data Access Control

Microsoft Azure, the third-party PaaS supplier used by Add-On Products, has implemented multiple measures to ensure Data Access Control is maintained. These measures are published in detail at "Azure customer data protection" (Protection of customer data in Azure | Microsoft Docs)

1.4 Data Transmission Control

Personal Data must not be read, copied, modified, or removed without authorization during transfer, except as necessary for the provision of the Cloud Services in accordance with the Agreement. To ensure the secure transfer of Personal Data, Add-On Products has implemented adequate measures for data transmission control.

Where data carriers are physically transported, such as in the case of backups or disaster recovery procedures, Add-On Products has implemented adequate measures to protect the Personal Data during transport, such as the use of encryption. These measures ensure that the agreed-upon service levels are maintained.

When Personal Data is transferred over Add-On Products internal network, it is protected according to Add-On Products Security Policy (as published at "Add-On Products & Policy about SaaS" (Add-On Products & Policy about SaaS - Add-On Products). This policy outlines the measures taken by Add-On Products to protect the confidentiality, integrity, and availability of Personal Data during transmission over its internal network.

1.5 Data Input Control

It will be possible to retrospectively examine and establish whether and by whom Personal Data haven been entered, modified or removed from the Cloud Service as published at "Azure database security checklist" (Azure database security checklist | Microsoft Docs)

1.6 Job Control

Personal Data processed on behalf of the customer is only processed in accordance with the Agreement and the customer's instructions. To ensure compliance with contractual obligations

Measures:

- Add-On Products implements controls and processes that monitor the compliance of Add-On Products, its sub-processors, and other service providers as published at "Add-On Products & Policy about SaaS" (Add-On Products & Policy about SaaS - Add-On Products).
- Additionally, to ensure the protection of Personal Data, Add-On Products employs measures such as the Add-On Products Security Policy and the Add-On Products Information Classification Standard, which requires Personal Data to have at least the same level of protection as confidential information.
- Add-On Products also ensures that all employees, contractual processors, and service providers are contractually bound to respect the confidentiality of sensitive information, including trade secrets of Add-On Products customers and partners.

1.7 Availability Control

Add-On Products ensures a high level of availability for the Cloud Service, including the Personal Data stored within it, in accordance with the Service Level Agreement ("SLA") (Add-On Products subscription agreement - Add-On Products) outlined in the Subscription Agreement. The SLA specifies the uptime and availability requirements of Cloud Service and the remedies available to the Customer if those requirements are not met.

In the event of a significant service interruption or outage, Add-On Products will take appropriate measures to restore the Cloud Service and ensure the integrity of the Personal Data stored within it. This may include restoring data from backups, implementing disaster recovery procedures, or other appropriate measures to ensure the availability and integrity of Personal Data.

1.8 Data Separation Control

Personal data collected for different purposes is processed separately. This ensures it is not commonly used or mixed up, maintaining the individual integrity and privacy of each data set.

Measures:

- Add-On Products operates dedicated virtual machines (VMs) and databases for each customer or service. This structure ensures separate system landscapes, preventing the potential mixing or misuse of data.
- Databases located on shared Managed SQL servers have rigorous access controls to ensure that each customer or controller can only access their own data.
- Personal data required to handle a support incident is used solely for the processing of that specific incident and is stored in dedicated support systems. This measure ensures the data is not accessed for processing any other support messages.
- Regular audits are conducted to ensure the proper implementation and effectiveness of data separation controls. These audits help in identifying any potential areas of improvement and ensuring compliance with data protection regulations.

This approach underlines our commitment to maintaining the privacy and security of personal data, as per the data protection laws and regulations.

1.9 Data Integrity Control

Personal Data will remain intact, complete and current during processing activities