FRAMEWORK DATA PROCESSING AGREEMENT

CONTENTS

1 Subject and duration of the DPA

(1) This data processing agreement ("DPA") forms an integral part of the Service Contract or other agreement between Customer (Controller) and SoftwareONE (Processor) governing SoftwareONE's provision of services to the Controller, when applicable data protection law requires such a DPA to the use of SoftwareONE's services.

(2) This DPA governs the rights and obligations of the Parties in connection with the processing of personal data. The specific details of the performed data processing operations, including but not limited the subject-matter, the nature and purpose of the processing, the type of personal data, the categories of data subjects are regulated by the Parties in the Data Processing Addendum (hereinafter "Addendum"), which is an integral part of this DPA and shall be concluded on a mandatory basis.

(3) This DPA shall apply as long as SoftwareONE processes personal data on behalf of the Controller under the Service Contract or other agreement between Controller and SoftwareONE.

2 Instructions of the Controller

(1) The Controller is responsible for compliance with data protection provisions, in particular for the lawfulness of the data processing and for data subjects' rights according to the data protection provisions.

(2) The Processor processes the personal data given by the Controller solely in the scope of the agreed regulations and under the written instructions of the Controller. Additional instructions outside the scope of those given or agreed to be given in this DPA require prior written agreement between the Processor and the Controller, including agreement on any additional fees payable by Controller to Processor for carrying out such instructions.

(3) The processing occurs only under the Controller's instructions, expect where the Processor is required to process the personal data according to Union or Member State law. In these cases, the Processor will inform the Controller of such legal requirements prior to the processing, provided that such information is not forbidden on important grounds of public interest.

(4) If the Processor believes that an instruction given by the Controller infringes applicable data protection legal provisions, the Processor shall immediately inform the Controller of this prior to exercising such instruction. If, despite the Processor's notification of such an instruction, the Controller insists in exercising such an instruction, the Processor shall then be entitled to suspend the execution of the relevant instructions until the Controller changes them.

3 Technical and organizational measures

(1) The Processor shall implement adequate technical and organizational security measures for the data processing in accordance with Appendix 2 of this DPA. Controller agrees that these security measures are appropriate to the risks involved with the specific personal data processing operations.

(2) The measures that have been taken can be adapted by the Processor to future technical and organizational developments. The Processor may only carry out these adaptions, if they satisfy at minimum the previous level of security. The Processor shall only be required to inform the Controller of substantial changes.

4 Obligations of the Processor

(1) The Processor warrants and undertakes that all employees involved in the data processing procedures are familiar with the relevant data protection regulations. The Processor assures that those employees are bound to maintain confidentiality, and are subject to an adequate legal obligation of secrecy.

(2) The Processor may only access the Controller's personal data if it is necessary for the purposes of carrying out the data processing.

(3) The Parties agree to provide the contact details of the appointed Data Protection Officer or a contact person for data protection topics within their organization in order to enable all necessary communications between the Parties regarding this DPA. This information is included in Appendix 1 of this Agreement.

(4) The Processor shall support the Controller to ensure that the Controller can fulfill its obligations to respond to requests for exercising the data subject's rights, e.g. the right of access, rectification and erasure of data, restriction of processing, data portability and right to object. Information related to those requests may only be provided to data subjects with the prior instruction of the Controller. If a data subject exercises their data protection rights upon the Processor, the Processor shall forward this request to the Controller.

(5) To the extent required by law, the Processor shall assist the Controller with the latter's obligation to conduct a data protection impact assessment where required and if necessary, with prior consultations with supervisory authorities taking into the nature of processing and information available to the Processor.

(6) Processing of personal data in a third country outside the EU/EEA and/or Switzerland and/or UK requires the execution of the appropriate standard contractual clauses or other legal requirements for such transfer. If a sub-processor of Processor is a data importer (as defined in the standard

contractual clauses), Processor is authorized to and shall enter into the standard contractual clauses with such a sub-processor on behalf of Controller and its affiliates.

5 Sub-processing

(1) The Processor may only assign sub-processors, after informing the Controller of every intended appointment or change whereby the Controller has the opportunity to object to such changes. The Controller may only object to the proposed changes on reasonable grounds. If the Controller objects to the use of a further sub-processor, the Parties will work together in good faith to find a mutually acceptable resolution to address such objection. To the extent, such mutual resolution cannot be reached, the Parties shall have the right to terminate the affected services in whole or in part with immediate effect.

(2) The sub-processing relationship shall be established when the Processor appoints another Processor(s) in part or in whole for the provision of services agreed upon in this DPA. Ancillary services that are provided to and on behalf of the Processor by third-party service providers and which may support the Processor in the exercise of its duties shall not be regarded as sub-processing within the meaning of this DPA. Such services may include, for example, provision of telecommunication services or facility management.

(3) A sub-processor may only have access to the personal data of the Controller, once the Processor has ensured, by means of a written contract that a similar level of data protection obligations as included in this DPA, is imposed on the sub-processor and in particular adequate guarantees are provided as to the implementation of appropriate technical and organizational measures.

(4) All currently appointed sub-processors are listed in the relevant Data Processing Addendum at within the service specific Data Processing Addendums. SoftwareONE may from time to time update the applicable list of sub-processors on the relevant Data Processing Addendum and will inform the Controller accordingly via the provided contact details in the Services Contract.

6 Controller's audit rights

To the extent required by law, the Processor agrees that the Controller or another auditor mandated by the Controller shall be entitled upon prior written notice to monitor compliance with applicable data protection laws and this DPA using reasonable and appropriate means, including requests for relevant documents and information or by accessing the business premises of the Processor during the designated office hours. Proof of proper data processing can also be provided by appropriate and valid certificates for IT security (e.g. ISO 27001), provided that the specific subject of certification applies to the data processing activity being carried out in the specific case. Processor agrees that in compliance with its obligations under this DPA, it shall bear the costs of one yearly audit or inspection as mandated by the Controller. Audit or inspections

costs arising from further Controller requests shall be borne by the Controller, except in cases of a data related incident arising from the processing activities of the Processor. In such cases, the Processor shall bear the costs of such audit.

7 Personal data breach

The Processor shall notify the Controller, without undue delay, upon becoming aware of the existence of an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data (hereinafter personal data breach), which is likely to result in a risk to the rights and freedoms of the affected data subjects. The Processor shall provide, at a minimum, the following information:

a) A description of the nature of the personal data breach, the category and approximate number of data subjects and personal data records,

b) Name and contact details of the data protection officer or other contact person for further information,

c) A description of any likely consequences of the breach, and

d) A description of the measures taken or proposed to be taken by the Processor for the remedy or mitigation of the breach.

8 Termination of the Agreement

(1) On termination or expiration of this DPA, the Processor shall return or delete all personal data, at the choice of the Controller, provided there is no duty to preserve records due to statutory retention periods set by law.

(2) The Controller may terminate this DPA without notice in case of the Processor's violation of the terms of this DPA or applicable data protection laws and the Controller can therefore not reasonably be expected to continue the data processing until the expiry of the notice period or the agreed termination of DPA.

9 Final provisions

(1) The Parties agree that the limitations and exclusions of liability set out in the Service Contract shall apply in respect of a Party's liability arising out of, or in connection with, this DPA. The Parties agree that no limitations or exclusions of liability set out in the Service Contract shall apply to any Party's liability to data subjects to the extent that such limitations or exclusions are prohibited by applicable data protection laws.

(2) Should a provision of this DPA become unenforceable, that shall not affect the validity or enforceability of any other provision of this DPA.

10 Appendix 1: Contact details for data protection topics

1. Controller

The contact information of the Controller will be provided in the service contract.

2. Processor

Email: data-protection.global@softwareone.com

For more information, please find here [www.softwareone.com/en/about/privacy-center/data-protection-officer] SoftwareONE's appointed data protection officer.

11 Appendix 2: Technical and Organizational Measures

1. Confidentiality Pursuant

Admittance Control

Unauthorized persons shall be denied access to data processing equipment, which processes or uses personal data by means of the following measures. The assigned authorizations are regularly checked for their necessity.

Technical Measures

- Alarm
- Automatic access control system
- Chip cards / transponder systems
- Manual locking system
- Safety Locks
- Locking system with code lock

Organizational Measures

- Documented handout of keys, chip cards etc.
- Reception
- Visitors accompanied by employees
- Care when selecting cleaning services

System Access Control

Access to information systems is granted exclusively on a need-to-know basis. The following measures are taken to prevent unauthorized data processing systems from being used:

Technical Measures

- Login with username + password
- Use of monitored and up-to-date anti-virus protection

- Firewall
- Intrusion Detection Systems, in addition to SoftwareONE's own Intrusion Detection Systems, the infrastructure is also protected by Microsofts security for Azure. Details can be found here Azure infrastructure security | Microsoft Docs
- Mobile Device Management
- MS Direct Access with IPSec tunnel to SoftwareONE's data center
- To access SoftwareONE's managed cloud environments SoftwareONE are run a VDI-based access solution with MFA but without any VPN connectivity from corporate network
- Encryption of data carriers
- Encryption Smartphones:
  Mobile handheld devices are set up in such a way that they cannot be used without entering an access password. The PINs have a minimum length of four characters. The devices are secured using the basic encryption of the manufacturer's methods
- BIOS protection (separate password)
- Automatic desktop lock
- Encryption:
  All Devices are BitLocker encrypted – 256 Bit AES encryption
- File shredder (min. level 4, cross cut)
- External service provider for document shredding (DIN 66399)
- Physical deletion of data media
- Microsoft Azure securely erase or destroy drives used for storage that suffer hardware failure. When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation. Further details can be found here: https://www.microsoft.com/en-us/trustcenter/privacy/you-own-your-data

Organizational Measures

- Manage user permissions:
  All accesses and identifiers ("accounts") are assigned exclusively on a person specific basis. The use of accounts by several persons (group accounts) is not permitted. If the use of group accounts is unavoidable, the time exact assignability of the use of a group account by a concrete natural person is ensured. All authorization assignments and releases are documented in the ticket system

- Creating user profiles
- Central password management
- Password Policy

  The choice of passwords is made in sufficient complexity and quality. Sufficient complexity and quality requires at least 12 characters and one the following 3 categories (upper and lower case letters, numbers and special characters), no use of generic terms or proper names as well as the inadmissibility of at least the last 5 passwords used. Passwords changes are forced on a regular basis. The IT system forces the user to comply with the above-mentioned password specifications. The password rules correspond to the currently valid recommendations of the BSI. If an incorrect entry is made ten times in a row, the account is locked
- Data Retention Policy
- General Information Security Policy
- Data Protection and Privacy Policy
- Security policy for Systems accessing SoftwareONE IT resources from Secured Home Network that includes rules for the use of Mobile Devices
- The screen saver is activated after 20 minutes at the latest when the user leaves the system or is inactive. To deactivate the screen saver, the password must be entered. When leaving the workstation, the employee must lock the computer manually
- A policy “Data Protection and Home office” has been published with instruction in case of working from home

Data Access Control

SoftwareONE shall ensure that persons authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, changed or re-moved without authorization during processing.

Technical Measures

- Logging of accesses to applications, specifically during the input, modification and deletion of data
- There are separate productive and test systems in case of need of maintenance of the systems

Organizational Measures

- Use of authorization concepts:
  SoftwareONE shall ensure that only persons who are involved in the fulfilment of the associated

task have access to data. For this purpose, appropriate access authorization measures (profiles, groups, roles, etc.) have been set up. A differentiated authorization concept exists that regulates the access of SoftwareONE employees to the Controller's data. Employee access rights to the Controller's data are assigned on request by the IT department. The request must be approved by the superior. The assigned authorizations are checked by means of reviews within the framework of the annual financial statements and security audits

- A multitier admin permission concept is implemented. For emergency cases a central protected admin access repository is available, which can be accessed by IT management approval
- Administration of user rights by administrator

Separation Control

SoftwareONE take the following measures to ensure that data collected for different purposes can be processed separately. The separation of the data is designed in such a way that it is not possible to mix data for different processing purposes or for other contract partners/customers. This logical separation of the Controller's order data from other data is consistently implemented. The procedures used to process the order data are multi-client capable.

Technical Measures

- Separation of productive and test environment
- Logical separation (systems / databases / data carriers)
- Multi-client capability of relevant applications

Organizational Measures

- Control via authorization concept
- Definition of database rights
- Records are provided with purpose attributes

2. Integrity

Handover Control

SoftwareONE shall ensure that personal data cannot be read, copied, modified, removed without authorization during electronic transmission or during its transport or storage on data carriers, and that it is possible to check and determine to which destinations personal data is to be transmitted by data transmission equipment.

Technical Measures

- Encryption
  The employees are instructed to use the system side encryption option for storing, sending and transporting personal data on mobile data carriers (CD, USB stick, memory cards, etc.). Access to SoftwareONE data processing systems and wireless transmission (WLAN, Bluetooth, etc.) of personal data within the corporate network for remote maintenance or services is only possible via secure encrypted connections (at least WPA2 for WLAN, 128-bit AES encryption for Bluetooth)

- Use of VPN
- Logging of accesses and retrievals
- There is both an encryption concept, as well as a key management system:
  - HTTPS/SSL 256-bit transport encryption
  - SSL certificates
  - SHA256-RSA signature algorithm
  - Authentication claim token public key RSA 2048-bit
- Use of signature procedures

Organizational Measures

- Documentation of the data recipients as well as the duration of the planned transfer or the deletion periods
- Overview of regular call-off and transmission processes
- Personal delivery with protocol

Input Control

SoftwareONE warrant that it will be possible to subsequently verify and determine whether and by whom personal data has been entered, modified in or removed from data processing systems. Information systems shall be configured in such a way that process logging is available which adequately supports operational, security and data protection management. Logins, access and data changes for important objects are logged. This function is activated for central software applications that offer options for logging and change history. If necessary, protocols are evaluated for a specific purpose.

Technical Measures

- Technical logging of the input, modification and deletion of data
- Manual or automated control of protocols

Organizational Measures

- Overview, with which programs, which data can be entered, changed or deleted
- Traceability of input, modification and deletion of data by individual user names (not user groups)
- Allocation of rights to enter, change and delete data based on an authorization concept
- Storage of forms from which data has been transferred to automated processing operations
- Clear responsibilities for deletions

3. Availability and Resilience

Availability Control

SoftwareONE shall ensure that personal data is protected against destruction or loss.

Technical Measures

- Fire and smoke detection systems
- Fire extinguisher server room
- Server room monitoring temperature and humidity, server room airconditioned
- Uninterrupted power supply (UPS)
- Centralized managed malware protection solutions are in place within our environments. Related information systems are protected by traffic control. This implies the usage of firewall technologies and network segmentation. A Client Management Suite is installed on all devices and can only be disabled/modified by administrators

Organizational Measures

- Backup & Recovery Concept:
  SoftwareONE has a documented backup concept. The backup recovery functionality is tested regularly.
  At the request of the Controller, SoftwareONE can provide the backup concept.
- Checking the backup process
- Regular data recovery tests and logging of the result

- Regular data backup, checked for recoverability
- Existence of a contingency plan:
  SoftwareONE has multiple business contingency and risk management scenarios in place
- When updates for systems or applications are announced, they are evaluated as quickly as possible and installed after release. The installation of security updates is prioritized. Security related updates are installed promptly and must be implemented within six weeks of release. This maximum period is intended to ensure that there is enough testing time even for critical systems
- The storage systems meet the traditional demands of resilience and reliability

4. Procedures for regular review, assessment and evaluation

Data Protection Management

Procedure for the regular review, evaluation and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing shall be established.

Furthermore, it must be ensured that personal data processed on behalf of the Controller can only be processed in accordance with the instructions of the Controller.

Technical Measures

- Software solutions for data protection management in use
- Approvals or pre-approved requests for granting, re enabling or changing accounts are documented. It is assured that users cannot authorize their own access privileges and that the administrator of the user accounts is not involved in the authorization process. Access to secure data needs manager approvals
- Formal on and off boarding procedures are in place that covers among others access control and asset handling
- Security certification according to ISO 27001
- Other documented safety concept
- A review of the effectiveness of the technical protective measures is carried out at least once a year.

Organizational Measures

- Employees trained and committed to confidentiality/data secrecy

- Central documentation of all procedures and regulations for data protection with access for employees as required / authorized
- Regular sensitization of employees at least once a year
- The Data Protection Impact Assessment (DPIA) will be carried out as necessary
- The organization complies with the information obligations
- Formalized process for processing requests for information from data subjects is in place

Incident Response Management

Support in responding to security breaches

Technical Measures

- Firewall deployment, regular updates, and regular check of the rule set
- Use of spam filters, regular updates, and regular check of the rule set
- Use of virus scanners, regular updates, and regular check of the rule set
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- In addition to our own Intrusion Detection Systems and Intrusion Prevention Systems, the infrastructure is also protected by Microsoft's security for Azure. Details can be found here Azure infrastructure security | Microsoft Docs

Organizational Measures

- Documented process for recognition and reporting of security incidents / data breakdowns (also regarding reporting obligations to supervisory authorities)
- Documented procedure for dealing with security incidents
- Documentation of security incidents and data breakdowns with central ticket system
- Formal process and responsibilities for post processing security incidents and data breaches

Data Protection-friendly default settings

Privacy by design / Privacy by default

Technical Measures

- No more personal data is collected than is necessary for the purpose in question

- Simple exercise of the right of withdrawal by the data subject through technical measures

Order Control (outsourcing to third Parties)

Measures to ensure that personal data processed on behalf of the Controller can only be processed in accordance with the Controller's instructions. In addition to data processing on behalf of the Controller, this point also includes the performance of maintenance and system support work both on site and by remote maintenance. If the Processor uses sub processors in the sense of order processing, the following points shall always be settled with them.

Organizational Measures

- Prior examination of the safety measures taken by the sub processor and their documentation
- Selection of the sub processor from the point of view of due diligence (especially with regard to data protection and data security)
- Conclusion of the necessary agreement for order processing or EU standard contract clauses
- Written instructions to the sub processor
- Obligation of the sub processor's employees to maintain data secrecy
- Obligation to appoint a data protection officer by the sub processor if the obligation to order exists
- Agreement on effective control rights vis-à-vis the contractor
- Regulation on the use of further sub-contractors
- Ensuring the destruction of data after completion of the order
- In the case of prolonged cooperation: ongoing review of the contractor and its level of protection