# Data Processing Agreement (“DPA”) for Unify Cloud Services

Effective as of 15 May 2018 (the “Effective Date”)

By and between Customer (“Customer” or “Controller”) and Unify Software and Solutions GmbH & Co.KG (“Unify” or “Co-Controller”)

Customer and Unify each a “Party” and, collectively, the “Parties”.

Unify Cloud Services allow Customer and its Unify Cloud Services Users to enter information for processing by the software provided as a service. To the extent this information contains Personal Data, the Parties expressly agree that this DPA will apply, where both Parties share the roles and responsibilities of a Controller as follows:

- Customer (i) defines alone or jointly with others, the purposes of the Processing of Personal Data, (ii) is responsible for the accuracy of the Personal Data, (iii) is in charge of informing the data subjects about the processing of Personal Data and the modalities for the exercise of their rights, and (iv) is in charge of making notifications (including data breach notifications) to data protection authorities, if needed.
- Unify (i) defines the means of the Processing and (ii) is in charge of implementing the security measures,

and Unify assumes in addition the role of Processor as per the definitions in section 1. These roles and responsibilities are further detailed in Section 4 (Roles and Responsibilities) below.

This DPA applies to all activities carried out by Unify within the framework of Unify Cloud Services and the Terms of Service Production (TOSP) released by Unify for these Unify Cloud Services http://go.unify.com/Dataprotection, whereby Unify’s employees or third parties sub-contracted by Unify might handle Customer’s Personal Data.

The DPA does not apply to any other online or offline Unify products, sites, or services. With respect to Unify Cloud Services, this DPA prevails over any other existing data processing agreement or similar arrangement between Unify and the Customer that may already be in place for such other products, sites or services.

Customer recognizes that it has received all information it deems necessary to establish the fact that Unify provides sufficient guarantees with regard to the protection of Personal Data.

## 1. Definitions

In addition to the terms defined elsewhere in the TOSP the following definitions apply:

1.1 “Applicable Data Protection Law”: means the laws and regulations relating to the processing and protection of Personal Data applicable in the country where Unify is established. In particular, Applicable Law means (a) EU Regulation 2016/679 (General Data Protection Regulation; ‘GDPR’) (b) Member State laws or regulations relating to the processing and protection of Personal Data implementing or complementing GDPR; and (c) any other applicable laws or regulations relating to the processing and protection of Personal Data for the purpose of this Agreement.

1.2 "Personal Data" designates any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic cultural or social identity.

1.3 “Processing” or “Processes” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

1.4 "Processor" means the person or entity that Processes Personal Data on behalf of Customer as contemplated by the Agreement and this DPA

1.5 "Controller" means the legal person or entity which alone or jointly with others, determines the purposes and means of Processing of Personal Data. In the context of the Unify Cloud Services under this DPA, it is agreed as outlined above that the Parties share the roles and responsibilities of a Controller as follows:

- Customer (i) defines alone or jointly with others, the purposes of the Processing of Personal Data, (ii) is responsible for the accuracy of the Personal Data, (iii) is in charge of informing the data subjects about the processing of Personal Data and the modalities for the exercise of their rights, and (iv) is in charge of making notifications (including data breach notifications) to data protection authorities, if needed.
- Unify (i) defines the means of the Processing and (ii) is in charge of implementing the security measures,

## 2. Categories of Personal Data under this DPA:

The following categories of Personal Data are generally collected, processed by Unify to perform the Services under the TOSP:

- Profile Data: Personal Data of Unify Cloud Services Users (Users) create, in particular their user name, password, email address, access rights;
- Activity Data: Personal Data derived from User's use of Unify Cloud Services, in particular call journal data, content deletion or change records or data relating to service usage (e.g. used end-points) by a user to the extent that such data was not anonymized in order to generate aggregated Usage Data
- Transient and Session Data: Personal Data which are not stored on Unify Cloud Services (such as presence or location information) or which are tied to a log-on session on Unify Cloud Services (e.g. IP addresses)

Excluded from this DPA are the following categories of Personal Data:

- Personal Data of third parties individuals which Users of Unify Cloud Services may enter into Unify Cloud Services via text posts, document upload or voice recordings. Such data cannot be recognized by Unify Cloud Services as Personal Data.
- Personal Data of third parties individuals which Users of Unify Cloud Services may enter into their phone devices, such as into private address books. Such data are not stored in or processed by Unify Cloud Services but reside only on the Users' phone, outside of Unify Cloud Services.
  Customer is advised to govern the usage with regards to such Personal Data of Unify Cloud Services by appropriate data protection policies.

## 3. Categories of Data Subjects under this DPA:

The following categories of Data Subjects are affected by the processing of their Personal Data within the framework of this DPA:

- Tenancy Users in Customer's Cloud Services Tenancy,
- Cross-Tenancy Users with access into Customer's Cloud Services Tenancy (only Activity Data kept in Customer's Cloud Services Tenancy)
- Session Guests Users with access into Customer's Cloud Services Session

## 4. Roles and Responsibilities of Customer and Unify

### 4.1 Customer Role and Responsibilities:

4.1.1 **Purpose and Legality of Processing**: Customer shall be responsible for defining the purpose of Processing Personal Data, for the legality of the transfer of Personal Data to Unify, and for the legality of the data Processing. Customer shall, and shall cause its Affiliates and contractors, to comply with all its obligations under the Data Protection Laws when processing Personal Data in connection with the Cloud Services. In this respect, Customer shall notably

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

ensure having obtained and maintaining all necessary registrations or authorizations with the competent data protection authorities and valid legal grounds to process Personal Data.

4.1.2 **Data Subjects Exercising Rights**: Customer shall be the primary contact for Data Subjects to exercise their rights as per applicable Data Protection Legislation. See article 4.2.9 for Unify responsibilities in this context.

4.1.3 **Accuracy, Quality, Legality, Reliability of Personal Data**: Customer shall have the sole responsibility for the accuracy, quality, legality and reliability of Personal Data, and of the means by which it acquires Personal Data for processing by Unify Cloud Services

4.1.4 **Risk Assessment**: Customer shall be responsible for the assessment of the risks resulting from the Personal Data Processing

4.1.5 **Records of Processing:** To the extent required by applicable law, Customer shall be responsible for keeping and maintaining Records of Processing for Controllers for all Controller responsibilities assigned to Customer by this DPA. See also article 4.2.1, 4.2.3, and 4.2.14 on Unify responsibilities in this context, as well as article 4.1.12.

4.1.6 **Information of Data Subjects:** Customer shall be responsible for providing the information to Data Subjects on the processing of Personal Data as required by applicable Data Protection Legislation. See also article 4.2.1 and 4.2.3 on Unify responsibilities in this context, as well as article 4.1.12.

4.1.7 **Information on Controller / Co-Controller Split of Responsibilities to Data Subjects**: Customer is responsible to inform Data Subject about the responsibility split between Controller and Co-Controller as per this DPA. See article 4.2.4 for Unify's responsibility in this context.

4.1.8 **Data Breach Notification:** Customer shall comply with any data breach notification duties resulting from applicable Data Protection requirements. Where imposed by the applicable Data Protection Law, Customer is responsible for the notification of data breach to the Data Subjects and the Data Protection Authorities. See also 4.2.5 on Unify responsibilities in this context.

4.1.9 **Changes in Applicable Legislation:** Customer must notify Unify in due time about changes in legal regulations that may affect the contractual duties of Unify under this DPA and which may require amending this DPA and the agreed remuneration. Unify may also submit proposals to Customer if Unify deems a certain change to be necessary to remain compliant with Applicable Law.

4.1.10 **Irregularities or Errors in Processing of Personal Data:** Customer shall inform Unify promptly and comprehensively about any errors or irregularities related to Data Protection Laws on the Processing of Personal Data that it becomes aware of.

4.1.11 **Notification of Recipients of Personal Data about Rectification, Erasure or Personal Data, or Restriction of Processing:** Unify does not disclose Personal Data for any other purpose than for Processing required for the delivery of Unify Cloud Services (see section 8). To the extent that Customer discloses Personal Data to a recipient, e.g by federating Unify Cloud Services with other cloud services of transmitting Personal data via Circuit interfaces outside Circuit, Customer is obligated to notify such recipients about requests of Data Subjects for rectification or erasure of disclosed Personal Data, or a restriction of processing.

4.1.12 **Disclosure of Personal Data:** Unify discloses Personal Data only to recipients to whom it is required to disclose the Personal Data for the purposes of the processing. See "Information on Processing" http://go.unify.com/Dataprotection for details. Certain features of Unify Cloud Services allow customers and users to disclosure Personal Data to third parties. To the extent Customer or users of Customer takes advantage of such features, Customer is responsible for informing Data Subjects (article 4.1.6) and for including such use in the Records of Pro-

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

cessing (article 4.1.5).

### 4.2 Unify Role and Responsibilities

4.2.1 **Means of Processing:** Unify shall be responsible for defining the means of Processing and, in reference to articles 4.1.5 and 4.1.6, to provide information about those means to Customer, specifically to allow Customer to complete Records of Processing and to inform Data Subjects as required by applicable Data Protection Legislation. This “Information on Processing” is presented under http://go.unify.com/Dataprotection

4.2.2 **Scope of Processing by Unify:** Unify may collect and process Personal Data only within the framework of this DPA and the TOSP applicable to Unify Cloud Services provided to Customer, and to improve and upgrade these services. Material changes to the scope of Data Processing must be agreed jointly and must be documented. Unify hereby expressly recognizes that it shall only process Personal Data for the provision of Unify Cloud Services, and the improvement and upgrade of such Services.

4.2.3 **Implementation of Security Measures**: Unify shall be responsible for the implementation of security measures for the Processing of Personal Data within the framework of Unify Cloud Services. Unify shall take the appropriate Technical and Organizational Measures (TOMs), as laid out in Annex 1 to this DPA, designed to protect Customer's Personal Data against misuse and loss, or against any other data breach in accordance with the applicable Data Protection Laws. Customer understands that TOMs are subject to technical progress and further development. In this respect Unify shall be permitted to use alternative, suitable measures, informing customers by making available a description of those measures upon request. In reference to articles 4.1.5 and 4.1.6, to provide information about those TOMs to Customer, specifically to allow Customer to complete records of processing and to inform Data Subjects as required by Applicable Data Protection Law.

4.2.4 **Information on the Parties Split of Responsibilities to Data Subjects:** Unify is responsible to make the standard DPA document without any changes accessible to all Unify Cloud Services Users. In case this DPA contains changes to the standard DPA document requested by Customer, Unify has no responsibility to make these changes accessible to Data Subjects.

4.2.5 **Data Breach Notification:** In context of article 4.1.8, in the event of a breach of Personal Data, Unify shall assist Customer and provide all necessary information it has access to in order to permit Customer to comply with its obligations. Unify shall notify Customer without undue delay of any breach of Customer’s Personal Data discovered by Unify.

4.2.6 **Retention of Personal Data/Limitation to deletion:** Personal Data processed by Unify Cloud Services are generally retained until a) deleted by Customer or Unify Cloud Services Users, or b) a Customer-instructed retention period has expired, or c) the Cloud services agreement of Customer on Unify Cloud Services is terminated (see article 4.2.7 on effect of termination). Customer cannot demand the deletion of Personal Data insofar as Unify is required by statutory law to retain material that contains that Personal Data, e.g. any applicable data retention rules. Where Unify needs to retain Personal Data for such reasons, its processing shall be restricted by Unify until the applicable retention period has expired. In addition, Personal Data processing shall be restricted rather than Personal Data being deleted, to the extent legally permitted under applicable Data Protection Requirements, in particular, if the deletion is not reasonably feasible or only possible with disproportional cost due to the particular type of storage. Customer acknowledges and accepts that some requests may result in additional remuneration claims for Unify. Unify will inform Customer accordingly prior to executing the request.

4.2.7 **Personal Data Deletion and Export upon Termination of Cloud Services Agreement**: Unify shall be responsible to delete all data entered by Customer and Unify Cloud Services Users into the Software applications provided by Unify Cloud Services (“Tenancy Data”) including Personal Data at the end of the calendar month following the expiration or termination

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

of Customer's use of the Unify Cloud Services, or at any time upon request by Customer. Upon request by Customer, Unify shall provide an export of Tenancy Data in a data format which can be processed by Customer for portation to other Cloud services. For exceptions and limitation: see article 4.2.6.

4.2.8 **Customer Requests on Personal Data:** Unify shall be responsible to fulfil Customer requests for correction, deletion, restriction and making available of Personal Data both during the term of, and at the termination of the Agreement. For exceptions and limitation see article 4.2.6

4.2.9 **Data Subjects Exercising Rights:** In the event Unify receives a request from a Data Subject to exercise rights as per applicable Data Protection Legislation, Unify shall forward such request to Customer which shall then instruct Unify without undue delay as to how to proceed. Customer acknowledges that in case of a conflict between Data Subject and Customer, applicable legislation might force Unify to fulfil the Data Subject's request against Customer's objection. Unify would however not take such step without due consideration of the legal situation with Customer.

4.2.10 **Effects of Deletion of Personal Data:** Customer hereby confirms and acknowledges that in the event Customer requests Unify to delete Personal Data or restrict its Processing, this may render the provision of the provided or subscribed-to products or services impossible. Unify shall notify Customer of such consequence before the execution of such request.

4.2.11 **Back-up Copies of Personal Data:** Unify shall make back-up copies of the Personal Data insofar as they are required to ensure correct Personal Data processing, and may copy and retain Personal Data that is needed for Customer's or Unify's compliance with its statutory document retention obligations.

4.2.12 **Handling of Media and Test Material:** Unify shall store and handle media provided to Unify, and all copies or reproductions thereof, with care so that they are not accessible by third parties. Unify shall be obliged to provide for a destruction of test material and other material containing Personal Data that is to be discarded on in a manner compliant with the law only on the basis of an individual request by Customer and at the latter's expense.

4.2.13 **Data Protection Officer:** Unify shall provide the contact details of Unify's data protection officer (DPO) on the internet. As of the Effective Date of this DPA, the DPO's current contact details are dp.it-solutions@atos.net.

4.2.14 **Records of Processing:** Unify shall be responsible for keeping and maintaining Records of Processing for Processors and for Controllers for all Controller responsibilities assigned to Unify by this DPA. See also article 4.1.5 for Customer's responsibilities in this context. Unify will make the respective information available in the "Information on Processing: http://go.unify.com/Dataprotection

## 5. Mutual Agreements and Responsibilities

5.1 The Parties agree that any requests regarding Personal Data issued by Customer shall be made in a written and in explicit manner. In the event that such requests require a change of services, such change shall be renegotiated in good faith by both Parties, as well as the associated price.

5.2 Each of the Parties shall ensure that their respective personnel are bound by a legal obligation to comply with Data Protection obligations and to maintain data confidentiality, and that they are informed about other applicable provisions concerning the protection of Personal Data, in particular telecommunications secrecy. The obligation to maintain data secrecy continues to apply after termination of their work or employment contract.

5.3 Where Unify believes that compliance with Customer's requests could result in a violation of applicable Data Protection Laws, Unify shall promptly notify Customer thereof. Unify shall be entitled to suspend the im-

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

plementation of the relevant request until it has been confirmed or amended by Customer.

5.4 Both Parties hereby acknowledge that the security measures detailed in Annex 1 (Technical and Organizational Measures) are providing sufficient guarantees to the Processed Personal Data. Customer understands that the technical and organizational measures are subject to technical progress and further development. In this respect, Unify shall be permitted to use alternative, suitable measures.

5.5 In the event Customer's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties, Unify shall inform Customer without undue delay, if permitted by law. Unify shall, without undue delay, notify all parties pertinent in such action that Personal Data affected by their measures is the Customer's sole property and at Customer's sole disposition, and that Customer is the responsible body pursuant to Applicable Data Protection Law.

## 6. Requests from supervisory authorities

6.1 Where required by Law, both Parties shall keep records of the Personal Data processed for the purposes of this DPA, cooperate and provide all necessary information for the fulfilment of the above obligations and notification duty under the Applicable Data Protection Law.

6.2 Where Unify has to assist Customer to meet Customer’s legal obligations as stated in section 6, Customer shall reimburse Unify any reasonable additional costs associated with the provision of such assistance.

## 7. Audit Rights

7.1 No more than once per year and upon a sixty (60) day prior written request, each Party shall have the right to conduct an audit of the other Party’s compliance with this DPA, by reviewing the technical and organizational measures implemented by the audited party. Evidence for the implementation of such measures that do not relate exclusively to this specific DPA or the Agreement may also be furnished by submitting a current certificate, reports or extracts from reports by independent third parties, e.g. by certified public accountants, account auditors, the audited Party’s internal and/or external data protection officer(s), IT security department, internal and external data protection auditors, quality auditors, or by a suitable certificate issued after the audited Party’s IT security or data protection were audited by a third party.

7.2 Each Party reserves the right to refuse to provide the other Party with business and trade secrets, operational know-how and any information the audit of which would pose a security risk for the audited Party or its customers, or which the audited Party is prohibited to provide or disclose such as data being protected by law or the data of other customers.

## 8. Sub-processors

8.1 Customer hereby acknowledges and accepts that Unify may engage subcontractors for the provision of Unify Cloud Services. Such sub-contractors may be entities of the Atos Group (“Internal Subcontractors”) or third party subcontractors (“External Subcontractors”). A complete list of approved sub-contractors as of the Effective Date of this DPA is provided under http://go.unify.com/Dataprotectionincluding the applicable safeguards for adequate protection of Personal Data.

8.2 In case Unify intends to engage a new external sub-contractor which is not identified in the list of approved subcontractors as of the Effective Date of this DPA, articles 9.2 and 9.3 shall apply. For the avoidance of doubt, it is expressly agreed that Internal Subcontractors shall not be governed by this provision and Customer is deemed not to object to the use of Internal Subcontractors.

8.3 Transfers of Personal Data to Third Party Countries:

8.3.1 Customer hereby expressly acknowledges and accepts that Personal Data may be transferred to and / or processed by External Subcontractors as provided for in article 8.1 above, including when these External Subcontractors are located outside the European Economic Area (EEA).

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

8.3.2 Internal Subcontractors are part of the Atos Group and therefore are bound by Binding Corporate Rules as approved by the European data protection authorities and which are available at https://atos.net/content/dam/global/documents/atos-binding-corporate-rules.pdf (the "BCR"). Customer acknowledges that, in the event that Unify transfers Personal Data to any entity of the Atos group located outside the EEA, the BCR constitute a sufficient safeguard to establish that such entities provide an adequate protection to Personal Data as required under Applicable Data Protection Law. Accordingly, Customer hereby expressly consents that Personal Data may be transferred to any of the Atos Group entities bound by the terms of the BCR as listed in Annex 2 of the BCR. Unify shall make available by any appropriate means to Customer any updates to Annex 2 of the BCR. Customer commits to provide adequate information to Data Subjects regarding the BCR.

8.3.3 Where Unify transfers Personal Data to an External Subcontractor located outside the EEA which does not fall within the scope of the BCR, Customer hereby expressly grants Unify a mandate to enter into any relevant agreements to ensure that the receiving entity implements an adequate level of protection to Personal Data acknowledged as appropriate by the competent European or local authorities.

## 9. Changes to this DPA

9.1 Customer acknowledges that terms in this DPA and in Annex 1 are subject to changes by Unify. A change requires consent by Customer if it a) affects the responsibility split between Controller and Co-Controller as per section 4, or b) limits the rights of Customer, or c) requires consent as per applicable Data Protection legislation. In other cases a change requires only information to Customer.

9.2 In case of a change which requires consent by Customer, Unify will notify Customer about the change via email to tenant administrator under which the Customer's Cloud Service Tenancy is registered at Unify, or via Unify's accredited sales partner with whom Customer holds the Cloud Services agreement for a Unify Cloud Service, and will make relevant information available to Customer for review at least thirty (30) calendar days prior to the change becoming effective. Unify will give Customer the opportunity to give consent or to object. If no objections by Customer is received by Unify after a response period indicated on the change notification, which is shall be at least ten (10) calendar days following the date of notification, Customer's consent shall be deemed given. In emergency situations, notice and response periods might be shorter.

9.3 Customer shall not object to a change without providing to Unify detailed written explanation of the grounds for such objection. Unify shall undertake commercially reasonable efforts to address Customer's concerns. Both Parties shall cooperate in good faith to reach an agreement. If no agreement can be reached, the Unify Cloud Services contracted by Customer will be terminated.

## 10. Liability

10.1 Unify and Customer shall perform their respective obligations as set forth in this DPA and the Applicable Data Protection Law.

10.2 Customer shall have full liability for any breach of its obligations in section 4.1 above, as well as its obligations as set out in section 5 above.

10.3 Unify shall have full liability for any breach of its obligations in section 4.2 above, as well as its obligations as set out in section 5 above, subject to any dependency from Customer.

10.4 Where acting as the processor, Unify shall be liable for the damage caused by processing only where it has not complied with obligations of the Applicable Data Protection Law directed to processors or where it has acted outside or contrary to lawful instructions of Customer.

10.5 The breaching Party shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

10.6 Where Customer and Unify are responsible for any damage caused in breach of an obligation in this DPA, each Party shall be held liable for the entire damage in order to ensure effective compensation of the Data Subject. The Party which has paid full compensation for the damage suffered shall be entitled to claim back from the other Party involved that part of the compensation corresponding to its part of responsibility for the damage.

## 11. Miscellaneous

11.1 If any individual provision of the DPA is illegal, invalid, void, voidable or unenforceable, the remainder of the DPA will continue in full force and effect. The Parties shall agree upon an effective provision that, insofar as legally possible, most closely reflects the Parties' intent.

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

# Annex 1

**Unify's General Technical and Organizational Measures**

At Unify, the technical and organisational measures required by law are implemented on the basis of Unify's Data Privacy and Information Security Framework (the "DIS Framework"), which defines policy standards (level 2) and operational procedures (level 3) in accordance with the international standard ISO27001 on the basis of Unify's corporate policy "Unify Data Privacy and Information Security Policy". The documents are available to Customer upon request.

The following description of the status quo of the elementary measures regarding the protection of data cannot cover any and all security measures in place at Unify. In particular in the context of data protection and data security, it is also not feasible to provide detailed descriptions of confidential measures, as the protection of security measures against unauthorised disclosure is as least as important as the security measure itself.

Customer is encouraged to discuss any individual questions relating to the technical and organizational measures with Customer's account manager at Unify, Unify's DPO and, where relevant, Unify's Chief Information Security Officer (CISO).

## 1. Entrance Control

Technical or organizational measures regarding access control, especially regarding legitimation of authorized persons:

The aim of the entrance control is to prevent unauthorised people from physically accessing such data processing equipment which processes or uses Personal Data.

Due to their respective security requirements, business premises and facilities are subdivided into different security zones with different access authorizations. They are monitored by security personnel. Access for employees is only possible with an encoded ID with a photo on it. All other persons have access only after having registered before (e.g. at the main entrance).

Access to special security areas such as the service centre for remote maintenance is additionally protected by a separate access area. The constructional and substantive security standards comply with the security requirements for data centres

## 2. System Access Control

Technical (password protection) and organizational (user master data) measures regarding the user ID and authentication:

The aim of the system access control is to prevent unauthorized use of data processing systems which are used for the processing and the use of Personal Data.

Each employee's user master data and individual identification code are registered in the global contact directory. Admission to the data processing systems is only possible after identification and authentication by using the identification code and the password for the particular system.

Additional technical protections are in place using firewalls and proxy servers.

In order to guarantee admission control, encryption technologies are used (e.g. remote access to the company network via VPN tunnel). The suitability of an encryption technology is measured against the protective purpose.

## 3. Data Access Control

On-demand structure of the authorization concept and of the data access rights as well as their monitoring and recording:

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

Measures regarding data access control are to be targeted on the fact that only such data can be accessed for which an access authorization exists and that Personal Data cannot be read, copied, changed or deleted in an unauthorized manner during the processing, use and after the saving of such data.

Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorization concept. In accordance to the "need-to-know" principle, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person.

In order to ensure data access control, an encryption technology is used (e.g. remote access to the company network via VPN tunnel). The suitability of an encryption technology is measured against the protective purpose.

**4. Transmission Control**

Measures regarding the transport, transfer, transmission or storage of Personal Data on data media (manually or electronically) as well as regarding the subsequent review:

The aim of the transmission control is to ensure that Personal Data cannot be read, copied, changed or deleted without authorization during their transfer or while stored on data media, and that it can be monitored and determined to which recipients a transfer of Personal Data is intended.

The measures necessary to ensure data security during transport, transfer and transmission of Personal Data as well as any other company or customer data are detailed in the policy on the protection of confidential business information. In this policy, there is a detailed description of the entire processing of data, from the creation of such data to their deletion, including the handling of such data in accordance with their classification.

In order to ensure transfer control, an encryption technology is used (e.g. remote access to the company network via VPN tunnel). The suitability of an encryption technology is measured against the protective purpose.

The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service provider) is only made if a corresponding contract exists, and only for a specific purpose. If Personal Data are transferred to companies with their seat outside the EU/EEA, Unify provides that an adequate level of data protection exists at the target location or organization in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the EU model contract clauses.

**5. Data Entry Control**

Measures regarding the subsequent review, whether and by whom data were entered, altered or deleted:

The aim of the data entry control is to make sure with the help of appropriate measures that the circumstances of the data entry can be reviewed and monitored retroactively.

System inputs are recorded in the form of log files. By doing so, it is possible at a later stage to review whether and by whom Personal Data was entered, altered or deleted.

**6. Data Processing Control**

The aim of data processing control is to ensure that Unify only processes Personal Data in accordance with the Terms of Service Production (ToSP) issued by Unify for the contracted cloud service, and the provisions set forth in the Data Processing Agreement for Unify Cloud Services.

Personal Data processed in Unify Cloud Services only accessible to the technical support and operation organization. Unify has policies in place to prevent this organization from using Personal Data for any other purpose or to disclose Personal Information to any other organization or third party except upon instruction by Customer.

A transfer of Personal Data to a third party, such as a subcontractor, is only made under consideration of contractual arrangements and Applicable Data Protection Law.

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

## 7. Availability Control

Measures regarding data backup (physical/logical):

The aim of the availability control is to ensure that Personal Data are protected against accidental destruction and loss.

If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.

Due to technical reasons, copies of Personal Data may be present in backup files and may be made by mirroring of services. Subject to Unify's own statutory data retention obligation (see Processing Agreement), such copies are also deleted - if necessary, with a technically caused delay. The availability of the systems themselves is ensured in accordance with the necessary security level by corresponding security measures (e.g. mirroring of hard drives, RAID systems, USV).

## 8. Separation Control

Measures regarding the separate processing (saving, changing, deletion, and transfer) of data with different purposes:

The aim of the separation control is to ensure that data which have been collected for different purposes can be processed separately.

Personal Data are used for internal purposes only (e.g. as part of the respective customer relationship). A transfer to a third party such as a subcontractor is solely made under consideration of contractual arrangements and data protection regulations.

Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability, the separation of functions as well as the separation of testing and production systems are used for this purpose.

## 9. Additional procedures for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing (Art. 32 Section 1 lit. d GDPR; Art. 25 Section 2 GDPR)

### 9.1 Data Protection Management

The data protection at Atos is organized in a global organization with data protection officers and legal experts for the individual Global Business Units (GBU) and countries.
The GBU Germany has a data protection office with three appointed Data Protection Officers and at least one legal expert. The Data Protection Office is part of the data protection and information security organization, which regularly exchanges on its topics.
The Group Data Protection Policy is the basis for data protection at Atos, which describes the principles of data protection as well as the processes concerning the rights of the persons concerned, audits, training and awareness raising and refers to the global information security policy with its further regulations.
The Data Protection Office provides predefined documents in the Atos Integrated Management System (AIMS), such as forms, checklists, manuals, and work instructions used in HR and business processes. All employees are committed to data secrecy and the observance of company and business secrets and are dependent on GDPR, Articles 29 and 32 (4) to process personal data only on the instructions of the data controller. In addition, they were obliged to comply with the Telecommunications Act (Section 88) and, if appropriate, to safeguard social secrecy and / or bank secrecy.
In annual mandatory training sessions, Atos employees must update their privacy awareness.
The technical and organizational measures for data protection pursuant to GDPR, Article 32, are regularly reviewed within the scope of the ISO certification and the ISAE3402 audits. In addition, internal process audits also take account of data protection-relevant issues.

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.

### 9.2 Risk and Security Management

Atos conducts its services on the basis of a security management system. This includes, among other things, documented guidelines and guidelines for the IT / Data Center operation. They are based on statutory as well as internally established regulations. The security processes used are regularly checked. The guidelines are also binding for subcontractors. The Atos employees are trained every year in obligatory training sessions on security awareness.
Atos has implemented a risk management process across all company levels and has appointed dedicated risk managers at various levels of the organization to ensure the implementation of risk management.
The risk management processes are divided into operational risk management, which is relevant for proposals, contracts (from the transfer of the service to Atos or the start of the project to the completion of the project or the end of the service) and the operational area, i.e. the relevant locations, services and processes.
Risks, their assessment and the follow-up of the defined measures are documented in risk registers and regularly reviewed and updated by the responsible persons, with the involvement of the responsible risk manager and relevant experts. Controls are defined and documented for all inherent risks in the business. For each of these controls are responsible defined to regularly monitor the effectiveness.

### 9.3 Certification

The German Atos companies are certificated according to
- DIN EN ISO 9001: 2015 (Quality Management)
- ISO / IEC 27001: 2013 (Information Security Management)
- ISO / IEC 20000-1: 2011 (IT Service Management)

by Ernst & Young CertifyPoint B.V.
The Unify companies are currently in the onboarding process.

### 9.4 Incident Response Management

Security events are addressed by Atos to standard operating procedures and tool-based processes, which are based on "ITIL Best Practice", in order to restore fault-free operation as soon as possible. Security incidents are monitored and analysed promptly by the Atos Security Management organization. Depending on the nature of the event, the appropriate and necessary service teams and specialists will participate in the process, including the Atos "Computer Security Incident Response Team" (CSIRT). The Unify companies are currently in the onboarding process to this Incident Response Management.

### 9.5 Privacy by Design and Privacy by Default (Art. 25 Section 2 GDPR)

Data protection at Atos is taken into account at the earliest possible date by data protection-friendly presets ("Privacy by Design and by Default") in order to prevent unlawful processing or the misuse of data. Appropriate technical presetting is intended to ensure that only the Personal Data that is actually required for the specific purpose ((Data Minimization principle) is collected and processed.
Defaults for Privacy by Design and Privacy by Default are defined in the Atos Secure Coding Guideline and the Atos Secure Coding Policy.
In order to achieve a low-risk processing of personal data, inter alia the following protective measures are in place:

- Minimize the amount of personal data
- Pseudo anonymize or encrypt data as early as possible
- Create transparency with regard to procedures and processing of data
- Delete or anonymize data as early as possible
- Minimize access to data
- Preset existing configuration options to the most privacy-friendly values
- Document the assessment of the risks to the persons concerned.

Copyright © Unify Software and Solutions GmbH & Co. KG, 2018. All rights reserved.