Data Protection Agreement (“DPA”) for Resale and Co-Delivery Services in accordance to Art. 26 GDPR

Effective as of May 1st, 2019 (the “Effective Date”)

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

Customer and Unify each a “Party” and, collectively, the “Parties”. It is hereby understood and agreed that, as the case requires, Customer shall mean either the End-Customer or the Partner.

In the business with accredited partners, Unify uses a number of commercial and service processes for Unify systems and solutions, including commercial processes for Cloud Services, where applicable.

To the extent Unify processes Personal Data in the delivery of such processes and services, the Parties expressly agree that this DPA on Joint Controllership will apply, where both Parties share the roles and responsibilities of a Controller as follows:

Unify

i. Defines the means of Processing,
ii. Is responsible of implementing the security measures, and
iii. Is responsible for making notifications of Data Protection Breaches to Customer

Customer

i. Defines the purpose of Processing,
ii. Is responsible for the accuracy of Personal Data provided to Unify for Processing
iii. Is responsible for informing the data subjects about the processing of their Personal Data and the modalities for the exercise of their rights
iv. Is responsible for informing data subjects in case of Data Protection Breaches
v. Is responsible for making notifications of Data Protection Breaches to data protection authorities

The roles and responsibilities are further detailed in section 6 (Roles and Responsibilities) below.

This DPA applies to all processing activities whereby Unify employees or third parties sub-contracted by Unify handle Customer Personal Data, which are carried out within the framework of the following Terms and Conditions:

a) Terms and Conditions for Resale and Co-delivery Services released by Unify which are accepted by accredited Partners and End-Customers on https://unify.com/en/data-protection by click & accept

and where applicable

b) Partner Agreement with accredited Partners
c) Terms and Conditions accepted online at sign-up by partners purchasing through Unify-accredited Distribution Partners

This DPA applies to the processes and services as mentioned above, provisioned to facilitate the business between Unify, the accredited Partner and End-Customers. 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 processes and 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

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 **“Co-delivery Services”** means the provision of remote support and software upgrade entitlement to updates and future releases including comprehensive Online-Ressources.

1.3 **“Controller"** means a legal entity or organization which, independently or together with third parties, determines the purpose and means of processing personal data.

1.4 **“Data Protection Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to Personal Data processed for the purposes of this DPA.

1.5 **“End-Customer”** means the legal entity with which the Unify-accredited Partner has contracted for defined Unify products, solutions, and/or services.

1.6 **“Partner”** or **“involved Partner”** means the Unify-accredited Partners, involved in the resale of Unify products, solutions and services, including where applicable, Unify Cloud Services, to End-Customers.

1.7 **"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.

1.8 **“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

1.9 **”Resale-Services”** means the provision of comprehensive, flexible support services for Partner resale. Packages include software support with SLA options for specific customer needs.

1.10 **“Services”** means the specific Unify service offerings Customer has purchased from a Partner.

2. Purpose of the Processing

The purpose of the processing of Personal Data is the fulfilment of the business relationship contract for the relevant Terms and Conditions between Unify and the Partner and between the Partner and the End-Customer. This DPA covers processes and resale services that Unify delivers directly to End-Customers and processes and co-delivery services that Unify delivers to Partners.

3. Categories of Personal Data

The following categories of Personal Data are generally collected and processed by Unify to perform the processes and Services under the relevant Terms and Conditions:

- **User Profile Data**, such as name, phone number, job title, etc. which Unify collects to provide processes and services to Customers
- **Activity Data:** such as log-on time, commercial transactions, service transaction of Data Subject on Unify tools and processes as well as logging and tracing data which may be required for the resolution of faults of Unify systems and solutions reported by Customer. These data may include IP addresses, MAC addresses, type of user devices as well as activity records, such as log-in times, call detail records etc
- **Compliance Check Data:** Results of legally required compliance checks (Customer Contact only)
- **Payment Card Data:** In case payment cards are used for payment of Unify products, systems, and services, and where applicable, Unify Cloud Services
- **Session Data**: Personal Data are tied to a log-on session on our sign-up and commercial transaction tools (e.g. IP addresses).

For each processing stream, Unify publishes detailed Information on processing documents under https://unify.com/en/data-protection.

4. Categories of Data Subjects:

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

- **Customer Contact:** Individual who serves as a Customer contact on a contract with Unify or, where applicable, signs-up to Unify Cloud Services or Unify Partner Portal
- **Billing Contact:** Individual who serves as a contact on Unify invoices and for follow-up on payments
- **Technical Contact** Any other individual who is associated with a commercial transaction with Unify and of whom Personal Data are processed by Unify in the relevant Context.
- **Partner Tool User**: Individual belonging to a Unify sales partner who obtains access to a Unify sales, order, or service tools
- **Unify Product User**: Individual with an End-customer who uses a Unify products or solutions, whole is serviced by Partner using Unify service tools

5. Disclosure of Personal Data by Unify to involved Partners

Customer, who purchased Unify Solutions from Unify accredited Partners, agrees that Unify discloses Personal Data referred to in section 3 to involved Partners for the purpose of delivery of Services and Maintenance of customers' Unify Solutions.

6. Roles and Responsibilities of Customer and Unify

6.1 Customer Role and Responsibilities:

6.1.1 **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 Applicable Data Protection Law when processing Personal Data in connection with the above mentioned processes and services.

6.1.2 **Data Subjects Exercising Rights:** Customer shall be the primary contact for Data Subjects to exercise their rights as per applicable Data Protection Legislation.

6.1.3 **Accuracy, Quality, Legality Reliability of Personal Data:** Customer shall have the sole responsibility for the accuracy, quality, legality and reliability of Personal Data provided to Unify for processing, and of the means by which it acquires such Personal Data.

6.1.4 **Records of processing activities:** To the extent required by applicable law, Customer shall be responsible for keeping and maintaining Records of processing activities for Controllers**.**

6.1.5 **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 Law.

6.1.6 **Information on Split of Responsibilities to Data Subjects:** Customer is responsible to inform Data Subjects about the responsibility split between the contracting parties as per this DPA.

6.1.7 **Data Protection Breach Notification:** Upon notification by Unify or Partner about a Data Protection Breach Customer shall comply with any Data Protection 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 Protection Breach to the Data Subjects and the Data Protection Authorities.

6.1.8 **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.

6.1.9 **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.

6.2 Unify Role and Responsibilities

6.2.1 **Means of Processing:** Unify shall be responsible for defining the means of Processing and, in reference to articles 6.1.4 and 6.1.5, to provide information about those means to Customer, specifically to allow Customer to complete records of processing activities and to inform Data Subjects as required by Applicable Data Protection Law. This information is presented at the Unify Data Protection Information Webpage https://unify.com/en/data-protection#resale-co-delivery.

6.2.2 **Scope of Processing by Unify:** Unify collects and processes Personal Data only within the framework of this DPA. Material changes to the scope of Data Processing must be agreed jointly and must be documented**.**

6.2.3 **Implementation of Security Measures:** Unify shall be responsible for the implementation of security measures for the Processing of Personal Data in conjunction with the 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 Protection 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, specifically to allow Customer to complete records of processing activities and to inform Data Subjects as required by Applicable Data Protection Law.

6.2.4 **Information on the Parties Split of Responsibilities to Data Subjects:** Unify is responsible to make the standard DPA document accessible to Data Subjects. 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.

6.2.5 **Data Protection Breach Notification:** In context of article 6.1.7, in the event of a Data Protection Breach, 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.

6.2.6 **Retention of Personal Data:** For legal reasons, information on contracts, commercial transactions as well as compliance information of Contact Persons including has to be retained for 10 years after the transaction or the end of the contract. Therefore Unify deletes data at latest at the end of the 10th year after the last year in which the contract ends. On other processes, such as system traces pulled in the case of a service delivery for example, Unify deletes personal data earlier. As there are different timelines around these retention periods, please consult the respective process section on the Information of processing (IoP) pages. https://unify.com/en/data-protection#resale-co-delivery

6.2.7 **Data Subjects Exercising Rights:** In the event Unify receives a request from a Data Subject to exercise rights as per Applicable Data Protection Law, 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.

6.2.8 **Notification of Recipients of Personal Data about Rectification, Erasure or Personal Data, or Restriction of Processing:** In the event Unify executes a request related to a Data Subject exercising Data Subject Rights under Applicable Data Protection Law, Unify shall notify involved Partners as required by Applicable Data Protection Law – see section5.

6.2.9 **Effects of Deletion of Personal Data:** Customer confirms and acknowledges that in the event Customer requests Unify to delete Personal Data or restrict its processing; this may render the provision of Services impossible. Unify shall notify Customer of such consequence before the execution of such request.

6.2.10 **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.

6.2.11 **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.

7. Mutual Agreements and Responsibilities

7.1 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.

7.2 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.

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

7.4 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.

7.5 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 the Customer's sole disposition, and that Customer is the responsible body pursuant to Applicable Law.

7.6 Customer acknowledges that changes to the TOMs as laid out in Annex 1 as per Customer's instruction may lead to higher costs for Unify to deliver Services. In this case Unify has the right to increase the price of Services to Customer accordingly. Unify shall not implement the instruction before having notified Customer of and obtained agreement by customer on such a price increase.

8. Requests from supervisory authorities

8.1 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 Data Protection Laws.

8.2 Where Unify has to assist the Customer to meet Customer's legal obligations, Customer shall reimburse Unify any reasonable additional costs associated with the provision of such assistance.

9. Audit Rights

9.1 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.

9.2 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.

10. Sub-processors

10.1 Customer hereby acknowledges and accepts that Unify may engage subcontractors for the provision of Services. Such sub-contractors may be entities of the Atos Group ("Internal Subcontractors") or third party subcontractors ("External Subcontractors"). Where Unify commissions subcontractors, Unify shall be responsible for ensuring that Unify's obligations on data protection resulting from the Agreement are valid and binding upon subcontractor by appropriate agreements (contracts, binding internal regulations on data protection, code of conduct, etc.). A list of sub-contractors within the relevant processes and Services as of the Effective Date of this DPA is provided on Unify Data Processing Information Website at https://unify.com/en/data-protection#resale-co-delivery. Unify will notify Partner of changes in the list of subcontractors. However it is also Partner's responsibility to inform the end customer about these changes in the list of subcontractors.

10.2 Transfers of Personal Data to Third Party Countries:

10.2.1 Customer hereby expressly acknowledges and accepts that Personal Data may be transferred and / or processed to External Subcontractors as provided for in article 10.1 above, including when these External Subcontractors are located outside the EEA.

10.2.2 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.

10.2.3 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.

11. Changes to this DPA

11.1 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 the contracting parties, or b) limits the rights of Customer, or c) requires consent as per Applicable Data Protection Law. In other cases a change requires only information to Customer.

11.2 In case of a change which requires consent by Customer, Unify will notify Customer or Partner about the change, 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.

11.3 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.

12. Liability

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

12.2 Customer shall have full liability for any breach of its obligations in section 6.1 above, as well as its obligations as set out in section 7 above.

12.3 Unify shall have full liability for any breach of its obligations in section 6.2 above, as well as its obligations as set out in section 7 above, subject to any dependency from Customer.

12.4 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.

12.5 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**.**

13. Miscellaneous

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.

Annex 1
Technical and Organizational Measures

1. Implementation of technical and organizational measures to ensure the confidentiality, Integrity, Availability and resilience of processing systems pursuant to Article 32 of the General Data Protection Regulation

1.1 **Confidentiality (Art. 32 Section 1 lit. b GDPR)**

In order to ensure the confidentiality of the data and systems, physical, logical and application access, to systems that store, process, transfer or transmit personal data are strictly regulated and controlled. In addition, appropriate procedures of separate processing and / or pseudo anonymization of the data are used to ensure the confidentiality of the data and systems to the appropriate extent.

1.1.1 Physical access control

The goal of physical access control is to deny unauthorized persons access to those data processing systems that process or use personal data.

All Atos Data Center sites are secured against unauthorized access through automated access control systems. The security service performs regular patrols at night.
A clearly defined concept for authorized access to Atos facilities is in place. Employee's access to administrative areas is controlled by employee badges and card readers at office and/or floor entrances (electronic access control). The given access rights are monitored and reviewed periodically. Security and reception personnel are present, too. Visitors and third parties are recorded in visitor lists and are only permitted to access to Atos premises accompanied by Atos staff.

Access to Atos Data Center rooms is additionally secured:

- Automated access control is supplemented by other established methods of access authorization, such as biometrics, Pin-Pads, DES dongle, permanent security personnel, etc.
- Data Center rooms are partitioned on a multi-layer basis.
- Access to internal security areas is only permitted for a small, selected number of employees and technicians.

Beyond data centers operated by Atos, Unify uses data center services from other sub-contractors which are listed by processing stream under https://unify.com/en/data-protection in the respective Information on Processing documents. These sub-contractors have equivalent measures in place.

1.1.2 Logical access Control

The goal of logical access control is to prevent unauthorized persons from using data processing systems that process and use personal data.

Data terminals (PC, servers, network components) are accessed by means of authorization and authentication in all systems. Access control regulations include the following measures:

- Passwords (lower and upper case letters, special characters, numbers, minimum 8 characters, changed regularly, password history)
- Company ID with PKI encryption (two-stage security)
- Role-based rights are tied to access ID (classified according to administrator, user, etc.)
- Screen lock with password activation in user's absence
- Encryption of data storage devices while in transit (including notebook hard drives)
- Use of firewalls and antivirus software including regular security updates and patches.

1.1.3 Application Access Control

Application access control measures prevent unauthorized activities (e.g. unauthorized reading, copying, modification or removal) in data processing systems by persons without the required authorization.

Atos ensures the system-wide authentication of all users and data terminals including access regulations and user authorizations by technical measures.
Application access control incorporates the following measures:

- Access privileges are restricted based on defined roles
- A clear desk policy is in place
- Data storage devices in all mobile systems are encrypted while in transit (including notebook hard drives)
- Use of firewalls and antivirus software including regular security updates and patches
- A regular review of all existing privileged accounts is carried out.

1.1.4 Separation Control

The goal of separation control is to ensure that data collected for different purposes can be processed separately.

The following measures are implemented:

- Use of multi-tenant systems with logical client separation
- Development and quality assurance systems are completely separate from productive systems in order to ensure productive operation. The only exchange that takes place is in the form of files that are needed for processing data (program files, parameter files, etc.)
- Customer systems are only accessed by authorized personnel of Unify or involved Partner.

1.1.5 Encryption measures

The aim of the measures for the encryption of personal data is to protect the transmission and storage of personal data from unauthorized access and alteration.

Appropriate techniques for encryption are provided and implemented by Unify or subcontractors. The following common encryption technologies, among others, are used in practice by Unify:

- Consistently encrypted data transfer between systems
- Encryption of data before it is stored on systems or before it is transferred to databases
- Encryption of database backups

2. Integrity (Art. 32 Section 1 lit. b GDPR)

The integrity of the data on the systems is ensured in particular by regulations and controls with regard to the systems on which personal data are entered and from which this data is transferred or passed on.

2.1 Transmission Control

The goal of transmission control is to ensure that Personal Data cannot be read, copied, modified or removed while being transmitted, transported or saved to a data storage medium, and that it is possible to verify and establish to which bodies personal data may be transmitted using data transmission equipment.

Data can be transmitted from Customer to Unify using appropriate secure transmission types which must be agreed between the parties.

2.2 Input Control

The goal of input control is to ensure by means of appropriate measures that the circumstances surrounding data input can be subsequently verified and established.

Unify has implemented access regulations and user authorizations that enable the identification of all users and data terminals in the system. The activities of users are traceable through extensive logging functions and are stored via remote logging outside of the monitored system. Modifications are logged on servers or programs.
All monitoring and logging measures are adapted to the state of the art and the criticality of the data to be protected and carried out in the associated economic framework.
Input in database systems is controlled as part of the standard procedures supplied with the database systems, which, depending on the system, can include having all the entries captured.

3. Availability and resilience (Art. 32 Section 1 lit. b GDPR)

3.1 Availability control

The goal of availability control is to ensure that personal data is protected from accidental destruction or loss.
The following measures are implemented depending on the respective protection requirements of the personal data:

- The data backups (i.e. online/ offline; on-site/ off-site) will be done on a regular basis according to existing service agreements.
- The systems are powered without interruption (UPS).

3.2 Resilience / rapid recovery

For the so-called catastrophe case an emergency planning / crisis planning in connection with emergency and restart plans for the data centers is available. The plans are documented in service continuity and backup / recovery or emergency concepts. The functionality of these concepts is tested at regular intervals (usually annually).
The emergency plans are subject to a regular and continuous audit and improvement process.

4. 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)

4.1 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.

4.2 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.

4.3 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.

4.4 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 analyzed 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.

4.5 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.