# Data Protection Agreement (“DPA”) for Resale and Co-Delivery Services in accordance to Art. 28 GDPR

Effective as of August 1st, 2020 (the “Effective Date”)

By and between Partner (“Partner”)

and

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

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

**Preamble**

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

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, for the duration of the respective commission:

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

## 1. Definitions

**“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.

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

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

**“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.

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

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

**"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 partic-ular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

**“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 alter-ation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

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

## 2. Scope of application and responsibilities

**2.1** Unify shall process Data on behalf of Partner. Such Contract Processing shall include all activities detailed in the Agreement and its statement of work or service order. Within the scope of this Annex, Partner shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Unify and the lawfulness of having Data processed on behalf of Partner. Partner shall be the **»controller«** in accordance with Article 4 no. 7 of the GDPR.

**2.2** According to its role as controller Partner shall issue instructions to Unify as precondition for the processing of Partner’s Data. Partner’s individual instructions on Contract Processing shall, initially, be as detailed in the Agreement and its statement of work or service order. Partner shall, subsequently, be entitled to, in writing or in a machine-readable format (in text form), modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Unify. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes in the framework of the change request procedure. Partner shall, without undue delay, confirm in writing or in text form any instruction issued orally.

## 3. Purpose of the Processing

The purpose of the processing of Personal Data is the fulfilment of the business relationship between Unify and Partner and between Partner and 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.

## 4. Categories of Personal Data

**4.1** The following categories of Personal Data are generally collected and processed by Unify to perform the processes and Services according to the agreed terms.

- **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 Unify sign-up and commercial transaction tools (e.g. IP addresses).

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

- **End-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 Unify sales, order, or service tools.
- **Unify Product User**: Individuals at an End-customer who uses Unify products or solutions being serviced by Partner using Unify service tools

## 5. Disclosure of Personal Data by Unify to accredited Partners

End-Customer, who purchased Unify Solutions from Unify accredited Partners, must agree that Unify discloses Personal Data referred to in section 3 to accredited Partners in order for the Services and Maintenance of End-Customers' Unify Solutions to be provided.

## 6. Obligations of Unify and Partner

### 8.1 Unify's obligations

6.1.1 Except where expressly permitted by Article 28 para 3 a) of the GDPR, Unify shall process data subjects' Data only within the scope of the Contract Processing and the instructions issued by Partner. Where Unify believes that an instruction is not accomplishable for Unify for whatever reason or would be in breach of applicable laws, Unify shall notify Partner without undue delay. In such case, the Parties will agree on appropriate modifications or amendments of the instruction. Unify shall be entitled to suspending performance on such instruction until confirmed or modified by Partner. As far as Unify complies with the instructions issued by Partner, Unify shall not be liable for any violation of existing laws, in particular data protection laws, resulting from the compliance with the respective instruction and Partner shall indemnify Unify from any claims raised by third parties in this regard.

6.1.2 Unify shall, within its scope of responsibility, organise its internal organisation so it satisfies the specific requirements for data protection. Unify shall implement technical and organisational measures to ensure adequate protection of Personal Data, which measures shall fulfil the requirements of the GDPR (Article 32). Unify shall implement technical and organisational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services (see Annex 1). Partner is familiar with these technical and organisational measures, and it shall be Partner's responsibility that such measures ensure a level of security appropriate to the risk. With regard to compliance with the protective measures and safeguards agreed upon and their verified effectiveness, the Parties refer to the existing certification relating to DIN ISO 27001 presented to and sufficient for Partner as proof of the appropriate guarantees.Unify reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

6.1.3 Unify shall support Partner, insofar as is agreed upon by the parties, and where possible for Unify, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR. Internal costs incurred by Unify shall be paid by the Partner according to the generally agreed rates, unless Unify has itself given reason for the request or claim.

6.1.4 Unify warrants that all employees involved in the Processing of Personal Data and other such persons as may be involved in the Processing within Unify's scope of responsibility shall be prohibited from processing Personal Data outside the scope of the instructions issued by Partner. Furthermore, Unify warrants that any person entitled to process Personal Data on behalf of Partner has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.

6.1.5 Unify shall notify Partner, without undue delay, if Unify becomes aware of a Data Protection Breach.

6.1.6 Data protection officer (DPO): Unify provides the contact details of its data protection officer (DPO) on the Internet. At the effective date of this Agreement, the DPO's current e-mail address is as follows: dp.it-solutions@atos.net.

6.1.7 Unify warrants that it fulfils its obligations under Article 32 para. 1d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of the Technical and Organisational Measures for ensuring the security of the processing.

6.1.8 Unify shall correct or erase Data if so instructed by Partner and where covered by the scope of the instructions permissible. Where an erasure, consistent with data protection requirements, or a corresponding restriction of processing is impossible, Unify shall, based on Partner's instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to Partner. In specific cases designated by Partner, such Data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement.

6.1.9 Where a data subject asserts any claims against Partner in accordance with Article 82 of the GDPR, Unify shall support Partner in defending against such claims, where possible. Internal costs incurred by Unify shall be paid by the Partner according to the generally agreed rates, unless Unify has itself given reason for the assertion or claim.

6.1.10 On request by Partner, Unify will support Partner in the framework of the change request procedure to comply with Partner's obligation to define appropriate technical and organizational measures to ensure security and confidentiality of Data processed on the basis of the Agreement, in consideration of the applicable data protection law and the type of processing.

6.1.11 On request by Partner, Unify will provide Partner with all information available to Unify which is required to enable Partner to comply with its legal obligations like performance of a data protection impact assessment or provision of evidence on the technical and organizational measures taken in order to ensure data security. Partner will compensate Unify for all internal efforts incurring to that effect based on the contractually agreed rates.

**6.2** Partner's Obligations:

6.2.1 Partner as data controller will make sure that the Processing by Unify on behalf of Partner is performed in accordance with applicable data protection law and that Partner will meet its own obligations regarding the Processing by Unify.

6.2.2 Partner shall notify Unify, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Partner pertaining to the Processing by Unify under this agreement.

6.2.3 Section 6.1 para. 9 above shall apply, mutatis mutandis, to claims asserted by data subjects against Unify in accordance with Article 82 of the GDPR.
If the Partner processes personal data of Unify employees, the provisions pursuant to § 6 shall apply mutatis mutandis to the Partner, as far as they are applicable to the Partner.

## 7. Enquiries by data subjects

Where a data subject asserts claims for rectification, erasure or access against Unify, and where Unify is able to correlate the data subject to Partner, based on the information provided by the data subject, Unify shall refer such data subject to Partner. Unify shall forward the data subject's claim to Partner without undue delay. Unify shall support Partner, where possible, and based upon Partner's instruction insofar as agreed upon. Unify shall not be liable in cases where Partner fails to respond to the data subject's request in total, correctly, or in a timely manner.

## 8. Inspection Rights

**8.1** Unify shall document and prove to Partner Unify's compliance with the obligations agreed upon in this exhibit by appropriate measures, i. e. internal self-audits, binding corporate rules or certifications on data protection and/or information security (e.g. ISO 27001).

**8.2** Where, in individual cases, audits and inspections by Partner or an auditor appointed by Partner are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with Unify's operations, upon prior notice, and observing an appropriate notice period. Unify shall be entitled to rejecting auditors which are competitors of Unify.

- Partner hereby consents to the appointment of an independent external auditor by Unify, provided that Unify provides a copy of the audit report to Partner.

- Unify shall be entitled to requesting remuneration for Unify's support in conducting inspections, unless has itself given objective reason for the inspection.

**8.3** Where a data protection supervisory authority or another supervisory authority with statutory competence for Company conducts an inspection, para. 2 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

## 9. Sub-contractors

**9.1** Partner hereby acknowledges and accepts that Unify may engage subcontractors for the provision of the 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.).

**9.2** A complete list of sub-contractors 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.

**9.3** Unify shall obtain Partner's consent prior to the use of new or the replacement of existing subcontractors. Partner shall be entitled to refuse its consent only for material reasons related to statutory data protection regulations. If Partner will not disagree within a term of ten working days, the consent will be considered as given. If there will be a material reason related to data protection and, as far as an amicable agreement between the parties cannot be reached, Unify shall be entitled to terminate with immediate effect.

**9.4** The consent by Company shall be considered as given, as far as Unify deploys affiliated companies of the Atos Group as subcontractors within the European Union / the European Economic Area or deploys affiliated companies of the Atos Group as subcontractors outside of the European Union / the European Economic Area which are bound by the Binding Corporate Rules of the Atos Group.

**9.5** Transfers of Personal Data to Third Party Countries:)
Partner hereby expressly acknowledges and accepts that Personal Data may be transferred and / or processed to External Subcontractors, including when these External Subcontractors are located outside the EEA.
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"). Partner 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..
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.

## 10. Liability

The liability of the parties for damages incurred by third parties (e.g. pain compensation for Data Subjects) shall be governed by the statutory provisions. The liability of the parties to each other, however, is governed by the provisions of the main contract.

## 11. Miscellaneous

**11.1** Changes and amendments to this Agreement and all its components shall require a written agreement, which may also be in an electronic format (text form), and an express reference to the fact that they constitute a change or amendment to these Terms and Conditions. This also applies to the waiver of this formal requirement.

**11.2** In the event of any contradictions, provisions of this DPA shall take precedence over the provisions of the Agreement. Should individual parts of this appendix be invalid, this shall not affect the validity of the remaining parts of the appendix.

# Appendix Technical and Organizational Measures

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. 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. 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.

### 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.

1.3. 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.

1.4. 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.

1.5. 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 Unify companies are certificated represented in the following Atos Multisite Certificates (EY):

- DIN EN ISO 9001: 2015 (Quality Management)
- ISO / IEC 27001: 2013 (Information Security Management)
- ISO / IEC 20000-1:2011 (IT Service Management)

### 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.