Auftragsdatenverarbeitungsvereinbarung („ADV“) für Resale und Co-Delivery Services sowie Kommerzielle Verfahrensabwicklung

Gültig ab dem 15. Mai 2018 („Gültigkeitsdatum“)

von und zwischen („Kunde“) und Unify Software and Solutions GmbH & Co. KG („Unify)

Kunde und Unify nachfolgend jeweils als „Vertragspartei“ und gemeinsam als „Vertragsparteien“ bezeichnet. Beide Parteien nehmen zustimmend zur Kenntnis, dass je nach Zusammenhang, der Begriff „Kunde“ entweder den Endkunden oder den Partner meint.

Im Geschäft mit akkreditierten Vetriebspartnern betreibt Unify eine Reihe von kommerziellen Prozessen und Serviceprozessen für Unify Systeme und Lösungen, einschließlich kommerzieller Prozesse für Unify Cloud Services. In dem Maße, in dem Unify bei diesen Prozessen und Services Personenbezogene Daten verarbeitet, stimmen die Parteien ausdrücklich der Verwendung dieser ADV zu, in der beide Parteien die Rollen und Verantwortungen eines Verantwortlichen im Sinne der Anwendbaren Datenschutzgesetze teilen:

Unify

i. definiert die Mittel der Verarbeitung,
ii. definiert den Zweck der Verarbeitung
iii. ist verantwortlich für die Implementierung der Sicherheitsmaßnahmen, und
iv. ist verantwortlich, bei Bedarf die zuständigen Datenschutzbehörden über Verletzungen personenbezogener Daten zu benachrichtigen in Bezug auf Verstöße gegen Ziffer iii) oben.

Der Kunde

i. ist verantwortlich für die sachliche Richtigkeit der personenbezogenen Daten, und
ii. trägt die Verantwortung dafür, die betroffenen Personen über die Verarbeitung personenbezogener Daten und die Modalitäten für die Ausübung ihrer Rechte zu informieren.

Unify übernimmt zusätzlich die Rolle des Auftragsverarbeiters gemäß den Definitionen in Abschnitt 1. Diese Rollen und Zuständigkeiten werden weiter unten in Abschnitt 6 (Rollen und Verantwortlichkeiten) ausführlicher beschrieben.

Diese ADV bezieht sich auf alle Aktivitäten, bei denen Unify Mitarbeiter oder Dritte in Form von Unify beauftragten Subunternehmern Personenbezogene Daten des Kunden verarbeiten könnten, und die im Zusammenhang mit den folgenden Vereinbarungen stehen:

a) Allgemeine Bestimmungen für Resale und Co-Delivery Services wie von Unify freigegeben und akzeptiert von akkreditierten Vertriebspartnern und Endkunden unter http://go.unify.com/Dataprotection durch Click & Accept.

und wo anwendbar

b) Partnervertrag mit akkreditierten Vertriebspartnern für kommerzielle Verfahrensabwicklung
c) Allgemeine Bestimmungen die online von Vertriebspartnern bei der Anmeldung akzeptiert werden, die von Unify-akkreditierten Distributoren beziehen
d) Allgemeine Nutzungsbedingungen (ANB) für Unify Cloud Services wie sie von Unify freigegeben sind und von Endkunden bei der Anmeldung zu Unify Cloud Services direkt mit Unify oder mit Unify-akkreditierten Vertriebspartnern akzeptiert werden.

Diese Vereinbarungen werden im Folgenden als „Kontext“ dieser ADV bezeichnet.

Die ADV bezieht sich auf die oben beschriebenen Prozesse und Services, die von Unify zur Verfügung gestellt werden um das Geschäft zwischen Unify, akkreditierten Vertriebspartnern und Endkunden abwickeln zu können. Die ADV hat

Priorität gegenüber anderen in Kraft befindlichen Datenverarbeitungsvereinbarungen oder ähnlichen Vereinbarungen zwischen Unify und Kunde für Produkte, Standorte, Prozesse und Services

Der Kunde bestätigt, dass er alle Informationen erhalten hat, die er für notwendig hält, um festzustellen, dass Unify ausreichende Sicherheit in Bezug auf den Schutz personenbezogener Daten bietet

1. Definitionen

1.1 „Anwendbare Datenschutzgesetze“ bezeichnet die Gesetze und Vorschriften in Bezug auf die Verarbeitung und den Schutz personenbezogener Daten, die in dem Land gelten, in dem Unify einen Sitz hat. Insbesondere bezieht sich der Begriff „anwendbare Gesetze“ auf (a) die EU-Verordnung 2016/679 (Datenschutz-Grundverordnung, „**DSGVO**“), (b) die Gesetze oder Vorschriften der Mitgliedstaaten in Bezug auf die Verarbeitung und den Schutz personenbezogener Daten, welche die DSGVO umsetzen oder ergänzen, und (c) sonstige anwendbare Gesetze oder Vorschriften in Bezug auf die Verarbeitung und den Schutz personenbezogener Daten für die Zwecke dieser Vereinbarung.

1.2 „Auftragsverarbeiter“ bezeichnet eine natürliche Person oder Organisation, die im Auftrag des Kunden und im Sinne der Verarbeitung und dieser ADV personenbezogene Daten verarbeitet.

1.3 „Endkunde“ bedeutet das rechtlich selbständige Unternehmen, welches den Unify-akkreditierten Vertriebspartner oder Distributor für bestimmte Unify Produkte, Lösungen und Services unter Vertrag hat.

1.4 „Partner“ bedeutet einen Unify-akkreditierten Vertriebspartner oder Distributor, der involviert ist im Wiederverkauf von Unify Produkten, Lösungen und Services an Endkunden, einschließlich wo anwendbar, Unify Cloud Services.

1.5 „Personenbezogene Daten“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „**betroffene Person**“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.6 „Services“ bedeutet die spezifische Unify-Dienstleistung, die der Kunde vom Vertriebspartner bezogen hat.

1.7 „Verantwortlicher“ bezeichnet eine juristische Person oder Organisation, welche selbständig oder gemeinsam mit Dritten den Zweck und die Mittel für die Verarbeitung personenbezogener Daten bestimmt. Im Zusammenhang mit dem in der Präambel definierten Kontext im Rahmen dieser ADV wird wie oben beschrieben vereinbart, dass die Parteien die Rollen und Verantwortlichkeiten des Verantwortlichen wie folgt gemeinsam wahrnehmen („Gemeinsam Verantwortliche“).

1.8 „Verarbeitung“ bzw. „verarbeiten“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, das Speichern, die Anpassung oder Veränderung, das Abrufen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung sowie Einschränkung der Verarbeitung, Löschung oder Vernichtung.

Unify

i. definiert die Mittel der Verarbeitung,
ii. definiert den Zweck der Verarbeitung
iii. ist verantwortlich für die Implementierung der Sicherheitsmaßnahmen, und
iv. ist verantwortlich, bei Bedarf die zuständigen Datenschutzbehörden über Verletzungen personenbezogener Daten zu benachrichtigen in Bezug auf Verstöße gegen Ziffer iii) oben.

Der Kunde

i. ist verantwortlich für die sachliche Richtigkeit der personenbezogenen Daten und
ii. trägt die Verantwortung dafür, die betroffenen Personen über die Verarbeitung personenbezogener Daten und die Modalitäten für die Ausübung ihrer Rechte zu informieren.

2. Zweck der Verarbeitung

Der Zweck der Verarbeitung Personenbezogener Daten im Kontext (siehe Präambel) ist die Abwicklung der Leistungsbeziehung zwischen Unify und Partner und zwischen Partner und Endkunde. Diese ADV deckt Prozesse und Resale Services ab, die Unify direkt an den Endkunden liefert oder Prozesse und Co-Delivery Services, die Unify an den Partner liefert.

3. Kategorien von personenbezogenen Daten im Sinne dieser ADV:

Die folgenden Arten bzw. Kategorien von personenbezogenen Daten werden in der Regel von Unify im Sinne des Kontexts (siehe Präambel) für die Erbringung von Dienstleistungen erhoben, verarbeitet und genutzt:

- Nutzerprofildaten: wie Name, Telefonnummer. Position, Passwort, E-Mail-Adresse, Zugriffsrechte; etc.
- Aktivitätsdaten: wie etwa Log-on Zeiten, kommerzielle Transaktionen, Service Transaktionen von betroffenen Personen an Unify Tools und in Unify Prozessen, wie auch Logging und Tracing Daten, die verwendet werden und Fehler in Unify Lösungen und Systeme, die vom Kunden gemeldet wurden, beseitigen zu können. Diese Daten können IP Adressen, MAC Adressen, Typen von Nutzerendgeräten, oder auch Aktivitätsdaten wie Anrufdaten oder Log-on Zeiten beinhalten.
- Daten von Compliance-Überprüfungen“ ‚Resultate von gesetzlich vorgeschriebenen Compliance Überprüfungen
- Daten von Bezahlkarten (Kreditkarten): Im Falle dass Bezahlkarten (Kreditkarten) verwendet werden, für die Bezahlung von Unify Produkten, Systemen, oder Services, und, wo zutreffend, Unify Cloud Services
- Sitzungsdaten: Personenbezogene Daten, die an eine Log-on Sitzung eines Tool Nutzers oder einem Anmeldevorgang bzw. einer kommerziellen Transaktion anfallen (wie z.B. die IP Adresse.)

Für jede Prozesskette stellt Unify detaillierte Informationen zur Verarbeitung unter http://go.unify.com/Dataprotection zur Verfügung, die zeigen, welche Kategorien von Personenbezogenen Daten in diesen Prozesskette tatsächlich verarbeitet werden.

4. Kategorien von betroffenen Personen im Sinne dieser ADV:

Die folgenden Kategorien von betroffenen Personen sind von der Verarbeitung ihrer personenbezogenen Daten im Sinne dieser ADV betroffen:

- **Kundenkontakt:** Personen, die als Kundenkontakte auf einem Vertrag oder einer Bestellung mit Unify geführt werden oder die als Kundenkontakt Anmeldungen des Kunden für Unify Cloud Services oder für das Unify Partner Portal machen.
- **Rechnungskontakt:** Personen, die als Kontakt auf Unify Rechnungen und für die Nachverfolgung von Zahlungen geführt werden
- **Technischer Kontakt:** Jede andere Person, die verbunden ist mit einem kommerziellen Vorgang bei Unify und von der Personenbezogene Daten von Unify im Kontext (siehe Präambel) verarbeitet werden.
- **Partner / Kunden Tool User:** Personen bei Partnern und Endkunden, die Zugang zu einem von Unify bereitgestellten Vertriebs-. Auftrags-, oder Service Tool bekommen
- **Unify Product User:** Personen von Endkunden, welche Unify Produkte, oder Lösungen verwenden, die Supportservices von Vertriebspartnern von Unify über ein Unify Service Tool erhalten.

5. Personenbezogene Daten, die Unify Vertriebspartnern und Distributoren zur Verfügung stellt

Der Kunde stimmt ausdrücklich zu, dass Unify Personenbezogene Daten, wie in Abschnitt 2 dargestellt, den involvierten Vertriebspartnern (die einen Unify-akkreditierten Distributor einschließen können) zum Zwecke der Lieferung von Produkten und Services weitergegeben werden können. Die Identität des Distributors ist Unify und dem Vertriebspartner des Kunden bekannt, und kann dort erfragt werden. Der Kunde akzeptiert, dass Vertriebspartner sich frei entscheiden können, mit Distributoren zusammenzuarbeiten, so lange sie für ein bestimmtes Territorium von Unify akkreditiert werden, und dass Unify keine Kontrolle über die Auswahl des Distributors

durch den Vertriebspartner hat. Fragen in diesem Zusammenhang sind zwischen Kunde und Vertriebspartner direkt zu klären.

6. Rollen und Verantwortlichkeiten von Kunde und Unify

6.1 Rolle und Verantwortlichkeiten des Kunden:

6.1.1 **Information von betroffenen Personen über die Aufteilung der Verantwortlichkeiten zwischen den Gemeinsam Verantwortlichen**: Der Kunde ist dafür verantwortlich, die betroffene Person über die Aufteilung der Verantwortlichkeiten zwischen den Gemeinsam Verantwortlichen gemäß dieser ADV zu informieren. Informationen zu den Verantwortlichkeiten von Unify in diesem Zusammenhang finden Sie in Artikel 6.2.7

6.1.2 **Ausübung von Rechten durch betroffene Personen**: Der Kunde ist der Hauptansprechpartner für betroffene Personen in Bezug auf die Ausübung ihrer Rechte gemäß den anwendbaren Datenschutzgesetzen. Informationen zu den Verantwortlichkeiten von Unify in diesem Zusammenhang finden Sie in Artikel 6.2.12.

6.1.3 **Verzeichnis von Verarbeitungstätigkeiten**: Soweit gesetzlich vorgeschrieben, ist der Kunde dafür verantwortlich, für alle Verantwortlichkeiten des Verantwortlichen, die dem Kunden durch diese ADV übertragen werden, ein **Verzeichnis von Verarbeitungstätigkeiten** für Verantwortliche zu führen und zu verwalten. Siehe auch Artikel 6.2.16 zu den Verantwortlichkeiten von Unify in diesem Zusammenhang.

6.1.4 **Richtigkeit, Qualität, Rechtmäßigkeit, und Verlässlichkeit personenbezogener Daten**: Der Kunde trägt die alleinige Verantwortung für die Richtigkeit, Qualität, Rechtmäßigkeit und Verlässlichkeit personenbezogener Daten sowie für die Mittel, mit denen er personenbezogene Daten zur Verarbeitung durch Unify Cloud Services beschafft.

6.1.5 **Information von betroffenen Personen**: Der Kunde ist dafür verantwortlich, betroffenen Personen die gemäß den anwendbaren Datenschutzgesetzen erforderlichen Informationen zur Verarbeitung personenbezogener Daten zur Verfügung zu stellen. Siehe auch Artikel 6.2.1 bis 6.2.3 zu den Verantwortlichkeiten von Unify in diesem Zusammenhang.

6.1.6 **Meldung von Verletzungen des Schutzes personenbezogener Daten**: Der Kunde muss sämtliche Pflichten in Bezug auf die Meldung von Verletzungen des Schutzes personenbezogener Daten erfüllen, die sich aus den anwendbaren Datenschutzbestimmungen ergeben. Soweit durch anwendbare Datenschutzgesetze vorgeschrieben, ist der Kunde für die Meldung von Verletzungen des Schutzes personenbezogener Daten an die betroffenen Personen und die Datenschutzbehörden verantwortlich. Siehe auch Artikel 6.2.5 zu den Verantwortlichkeiten von Unify in diesem Zusammenhang.

6.1.7 **Änderungen anwendbarer Gesetze:** Der Kunde muss Unify's Datenschutzbeauftragten (dp.it-solutions@atos.net) rechtzeitig über Änderungen an gesetzlichen Bestimmungen informieren, die sich auf die vertraglichen Pflichten von Unify im Rahmen dieser ADV auswirken und unter Umständen eine Änderung dieser ADV und der vereinbarten Vergütung erfordern. Unify kann dem Kunden auch Vorschläge unterbreiten, wenn Unify eine bestimmte Änderung als erforderlich erachtet, um die anwendbaren Gesetze weiterhin einzuhalten.

6.1.8 **Unregelmäßigkeiten oder Fehler bei der Verarbeitung personenbezogener Daten:** Der Kunde hat Unify's Datenschutzbeauftragten (dp.it-solutions@atos.net) unverzüglich und umfassend zu informieren, wenn ihm Fehler oder Unregelmäßigkeiten in Zusammenhang mit Datenschutzgesetzen zur Verarbeitung von personenbezogenen Daten bekannt werden.

6.2 Rolle und Verantwortlichkeiten von Unify

6.2.1 **Zweck und Rechtmäßigkeit der Verarbeitung**: Unify ist verantwortlich für die Festlegung des Zwecks der Verarbeitung personenbezogener Daten, für die Rechtmäßigkeit der Übermittlung personenbezogener Daten an Unify sowie für die Rechtmäßigkeit der Datenverarbeitung. Der Kunde verpflichtet sich und seine Tochtergesellschaften oder Auftragnehmer dazu, bei der Verarbeitung personenbezogener Daten in Verbindung mit dem Kontext (siehe Präambel) alle seine Verpflichtungen ge-

mäß den Datenschutzgesetzen zu erfüllen. Diesbezüglich muss der Kunde insbesondere sicherstellen, dass alle notwendigen Registrierungen oder Genehmigungen bei den zuständigen Datenschutzbehörden sowie gültige rechtliche Grundlagen zur Verarbeitung personenbezogener Daten vorliegen und aufrechterhalten werden. Siehe auch die Artikel 6.1.3 und 6.1.5.

6.2.2 **Mittel zur Verarbeitung:** Unify ist für die Festlegung der Mittel zur Verarbeitung sowie in Bezug auf die Artikel 6.1.3 und 6.1.5 für die Bereitstellung von Informationen zu diesen Mitteln für den Kunden verantwortlich, insbesondere damit der Kunde Aufzeichnungen über die Verarbeitung führen und betroffene Personen gemäß den anwendbaren Datenschutzgesetzen informieren kann. Die „Informationen zur Verarbeitung" finden Sie unter http://go.unify.com/Dataprotection.

6.2.3 **Umfang der Verarbeitung durch Unify**: Unify darf personenbezogene Daten nur im Rahmen des Kontexts (siehe Präambel) dieser ADV verarbeiten Wesentliche Änderungen am Umfang der Datenvereinbarung müssen gemeinsam vereinbart und dokumentiert werden. Siehe auch die Artikel 6.1.3 und 6.1.5.

6.2.4 **Risikobewertung**: Unify ist verantwortlich für die Bewertung der Risiken, die sich aus der Verarbeitung Personenbezogener Daten ergeben.

6.2.5 **Meldung von Verletzungen des Schutzes personenbezogener Daten**: Im Zusammenhang mit Artikel 6.1.8 unterstützt Unify den Kunden im Falle von Verletzungen des Schutzes personenbezogener Daten und stellt ihm alle notwendigen Informationen zur Verfügung, auf die es Zugriff hat, um dem Kunden die Einhaltung seiner Verpflichtungen zu ermöglichen. Unify hat den Kunden unverzüglich zu benachrichtigen, wenn es Verletzungen des Schutzes von personenbezogenen Daten des Kunden feststellt.

6.2.6 **Benachrichtigung von Empfängern personenbezogener Daten über Berichtigung oder Löschung personenbezogener Daten bzw. Einschränkung der Verarbeitung**: Im Falle, dass Unify eine solche Forderung einer betroffenen Person in Ausübung ihrer Rechte unter den anwendbaren Datenschutzgesetzen ausführt, wird Unify den Distributor bzw. den Vertriebspartner entsprechend der Anforderungen der anwendbaren Datenschutzgesetze davon in Kenntnis setzen.

6.2.7 **Implementierung von Sicherheitsmaßnahmen**: Unify ist verantwortlich für die Implementierung von Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten im Kontext (siehe Präambel) dieser ADV. Unify ergreift die geeigneten Technischen und Organisatorischen Maßnahmen (TOMs), wie sie in Anlage 1 beschrieben sind, um die personenbezogenen Daten des Kunden vor Missbrauch und Verlust oder sonstigen Verletzungen des Datenschutzes gemäß den anwendbaren Datenschutzgesetzen zu schützen. Dem Kunden ist bewusst, dass die TOMs entsprechend dem technischen Fortschritt und der weiteren Entwicklung Änderungen unterliegen. In diesem Zusammenhang ist es Unify gestattet, geeignete alternative Maßnahmen zu ergreifen und die Kunden darüber zu informieren, indem auf Anfrage eine Beschreibung dieser Maßnahmen bereitgestellt wird. Insbesondere, damit der Kunde ein **Verzeichnis von Verarbeitungstätigkeiten** führen und betroffene Personen gemäß den anwendbaren Datenschutzgesetzen informieren kann.

6.2.8 **Information von betroffenen Personen über die Aufteilung der Verantwortlichkeiten zwischen den Gemeinsam Verantwortlichen:** Unify ist dafür verantwortlich, das ADV-Standarddokument ohne Änderungen für alle betroffenen Personen öffentlich zugänglich zu machen. Falls die ADV vom Kunden beantragte Änderungen am ADV-Standarddokument enthält, trägt Unify die Verantwortung dafür, die Änderungen betroffenen Personen zugänglich zu machen.

6.2.9 **Aufbewahrung personenbezogener Daten/Beschränkung der Löschung**: Im Kontext (siehe Präambel) verarbeitete personenbezogene Daten werden in der Regel aufbewahrt wie von Unify dargestellt unter http://go.unify.com/Dataprotection. Der Kunde kann die Löschung personenbezogener Daten insoweit nicht verlangen, als Diese gesetzlichen Aufbewahrungspflichten unterliegen. Wenn Unify personenbezogene Daten aufbewahren muss, ist deren Verarbeitung durch Unify einzuschränken, bis die geltende Aufbewahrungsfrist abgelaufen ist. Außerdem wird die Verarbeitung personenbezogener Daten eingeschränkt, statt die Daten zu löschen, soweit dies nach den anwendbaren Datenschutzbestimmungen zulässig ist, insbesondere wenn die Löschung nicht sinnvoll oder aufgrund der speziellen

Art der Speicherung nur mit unverhältnismäßigen Kosten durchführbar ist. Der Kunde nimmt zustimmend zur Kenntnis, dass einige Anfragen zusätzliche Vergütungsansprüche seitens Unify mit sich bringen können. Der Unify informiert den Kunden hierüber, bevor Unify die Anfrage ausführt.

6.2.10 **Kundenanfragen in Bezug auf personenbezogene Daten:** Unify ist dafür verantwortlich, Kundenanfragen zur Korrektur, Löschung, Einschränkung der Verarbeitung und Bereitstellung personenbezogener Daten sowohl während der Laufzeit als auch bei Beendigung der unter Kontext in der Präambel referenzierten Vereinbarungen nachzukommen. Details sind unter http://go.unify.com/dataprotection zu finden. Ausnahmen und Einschränkungen finden Sie in Artikel 6.2.9.

6.2.11 **Ausübung von Rechten durch betroffene Personen**: Falls Unify von einer betroffenen Person eine Anfrage zur Ausübung von Rechten gemäß den anwendbaren Datenschutzgesetzen erhält, muss Unify diese Anfrage an den Kunden weiterleiten, der Unify unverzüglich Anweisungen zum weiteren Vorgehen zu erteilen hat. Der Kunde erkennt an, dass im Falle eines Konflikts zwischen der betroffenen Person und dem Kunden Unify aufgrund der anwendbaren Gesetze unter Umständen dazu gezwungen ist, der Anfrage der betroffenen Person gegen den Einspruch des Kunden nachzukommen. Unify ergreift derartige Maßnahmen jedoch nicht ohne Erörterung der Rechtslage mit dem Kunden.

6.2.12 **Auswirkungen der Löschung personenbezogener Daten**: Der Kunde bestätigt und erkennt an, dass eine Anfrage des Kunde an Unify, personenbezogenen Daten zu löschen oder deren Verarbeitung einzuschränken, dazu führen kann, dass die Bereitstellung von Produkten oder Dienstleistungen bzw. die Anmeldung dazu unmöglich wird. Unify benachrichtigt den Kunden über diese Auswirkungen, bevor er eine entsprechende Anfrage ausführt.

6.2.13 **Sicherungskopien personenbezogener Daten**: Unify hat das Recht, Sicherungskopien personenbezogener Daten zu erstellen, soweit sie erforderlich sind, um eine korrekte Verarbeitung personenbezogener Daten zu gewährleisten, und kann personenbezogene Daten kopieren und verwahren, die erforderlich sind, damit der Kunde bzw. Unify seine gesetzlich vorgeschriebenen Pflichten zur Aufbewahrung von Dokumenten einhält.

6.2.14 **Verarbeitung von Medien und Testmaterial**: Unify speichert und verarbeitet ihm vom Kunden zur Verfügung gestellte Medien und alle Kopien oder Reproduktionen davon mit Umsicht, sodass sie Dritten nicht zugänglich werden. Unify ist auf einzelne Anfrage des Kunden verpflichtet, auf Kosten des Kunden für die ordnungsgemäße Vernichtung von Materialien zu sorgen, die zur Löschung bestimmte personenbezogene Daten enthalten.

6.2.15 **Datenschutzbeauftragter (DPO):** Unify stellt die Kontaktdaten seines Datenschutzbeauftragten (DPO) im Internet zur Verfügung. Zum Gültigkeitsdatum dieser ADV lautet die aktuelle E-Mail-Adresse des DPO wie folgt: dp.it-solutions@atos.net.

6.2.16 **Verzeichnis von Verarbeitungstätigkeiten**: Unify ist dafür verantwortlich, für alle Verantwortlichkeiten des Verantwortlichen, die dem Kunden durch diese ADV übertragen werden, Aufzeichnungen über die Verarbeitung für Verantwortliche und für Auftragsverarbeiter zu führen und zu verwalten. Siehe auch Artikel 6.1.3 zu den Verantwortlichkeiten des Kunden in diesem Zusammenhang. Unify stellt die entsprechenden Informationen unter „Informationen zur Verarbeitung“ zur Verfügung: http://go.unify.com/Dataprotection.

7. Gegenseitige Vereinbarungen und Verantwortlichkeiten

7.1 Die Parteien vereinbaren, dass vom Kunden ausgegebene Anfragen in Bezug auf personenbezogene Daten in schriftlicher und ausdrücklicher Form erfolgen müssen. Falls solche Anfragen eine Änderung der Dienstleistungen erfordern, werden diese Änderungen sowie der damit verbundene Preis von beiden Parteien in gutem Glauben neu ausgehandelt.

7.2 Jede der Parteien sorgt dafür, dass ihr jeweiliges Personal an rechtliche Pflichten gebunden ist, den Datenschutzverpflichtungen nachzukommen und die Vertraulichkeit von Daten zu wahren, und dass es über andere anwendbare Bestimmungen zum Schutz personenbezogener Daten, insbesondere des Telekommunikationsgeheimnisses, informiert wird. Die Verpflichtung zur Wahrung der Vertraulichkeit von Daten besteht auch nach Beendigung des Arbeits- oder Anstellungsvertrags fort.

7.3 Wenn Unify der Ansicht ist, dass die Erfüllung von Kundenanfragen zu einem Verstoß gegen anwendbare Datenschutzgesetze führen könnte, muss es den Kunden unverzüglich darüber in Kenntnis setzen. Unify ist berechtigt, die Umsetzung der betreffenden Anfrage auszusetzen, bis diese vom Kunden bestätigt oder geändert worden ist.

7.4 Beide Parteien bestätigen, dass die in Anlage 1 (Technische und Organisatorische Maßnahmen) aufgeführten Sicherheitsmaßnahmen den verarbeiteten personenbezogenen Daten ausreichende Garantien bieten. Dem Kunden ist bewusst, dass die Technischen und Organisatorischen Maßnahmen vom technischen Fortschritt und von der weiteren Entwicklung abhängig sind. In diesem Zusammenhang ist es Unify gestattet, geeignete alternative Maßnahmen zu ergreifen.

7.5 Falls die personenbezogenen Daten des Kunden Gegenstand einer Durchsuchung und Beschlagnahme, eines Pfändungsbeschlusses, einer Beschlagnahme im Rahmen eines Insolvenzverfahrens bzw. ähnlicher Ereignisse oder Maßnahmen Dritter werden, teilt Unify dies, sofern rechtlich zulässig, dem Kunden unverzüglich mit. Unify benachrichtigt unverzüglich alle an dieser Maßnahme beteiligten Parteien, dass die von ihren Maßnahmen betroffenen personenbezogenen Daten alleiniges Eigentum des Kunden sind und er allein verfügungsberechtigt ist und dass der Kunde gemäß den anwendbaren Gesetzen die zuständige Stelle ist.

8. Anfragen von Aufsichtsbehörden

8.1 Soweit gesetzlich vorgeschrieben, führen beide Parteien Aufzeichnungen über die für die Zwecke dieser ADV verarbeiteten personenbezogenen Daten, kooperieren und stellen alle erforderlichen Informationen zur Erfüllung der oben genannten Verpflichtungen und der Meldepflicht gemäß den Datenschutzgesetzen zur Verfügung.

8.2 Wenn Unify dem Kunden bei der Erfüllung der gesetzlichen Verpflichtungen des Kunden gemäß Abschnitt 6 behilflich sein muss, erstattet der Kunde Unify alle vertretbaren zusätzlichen Kosten, die mit der Bereitstellung dieser Hilfe verbunden sind.

9. Überprüfungsrechte

9.1 Nicht mehr als einmal jährlich und nach schriftlicher Anfrage mit einer Vorlaufzeit von sechzig (60) Tagen ist jede Partei berechtigt, eine Prüfung der Einhaltung dieser ADV durch die Gegenpartei durch Überprüfung der von der geprüften Partei durchgeführten technischen und organisatorischen Maßnahmen durchzuführen. Nachweise über die Einführung dieser Maßnahmen, die sich nicht ausschließlich auf diese ADV oder auf den Vertrag beziehen, können durch Vorlage aktueller Zertifikate, Berichte oder Auszüge aus Berichten von unabhängigen Dritten ergänzt werden, z. B. durch amtlich zugelassene Wirtschaftsprüfer, Buchprüfer, den/die internen und/oder externen Datenschutzbeauftragten der geprüften Partei, die IT-Abteilung der geprüften Partei, den/die internen und/oder externen Datenschutzprüfer der geprüften Partei oder Qualitätsprüfer bzw. durch entsprechendes Zertifikat, das nach Prüfung der IT-Sicherheit oder des Datenschutzes der geprüften Partei durch Dritte erstellt wird.

9.2 Jede Partei behält sich das Recht vor, der Gegenpartei Geschäfts- und Betriebsgeheimnisse, Betriebswissen und alle Informationen vorzuenthalten, deren Prüfung ein Sicherheitsrisiko für die geprüfte Partei oder ihre Kunden darstellen würde oder welche die geprüfte Partei nicht zur Verfügung stellen oder offenlegen darf, z. B: gesetzlich geschützte Daten oder die Daten anderer Kunden.

10. Subunternehmer

10.1 Der Kunde nimmt zustimmend zur Kenntnis, dass Unify Subunternehmer für die Bereitstellung von Unify Cloud Services beauftragen kann. Solche Subunternehmer können Unternehmen der Atos-Gruppe („interne Subunternehmer“) oder externe Unternehmen („externe Subunternehmer“) sein. Eine vollständige Liste genehmigter Subunternehmer zum Gültigkeitsdatum dieser ADV, einschließlich der anwendbaren Maßnahmen für einen angemessenen Schutz personenbezogener Daten, steht unter **http://go.unify.com/Dataprotection** zur Verfügung.

10.2 Falls Unify beabsichtigt, einen neuen externen Subunternehmer zu beauftragen, der zum Zeitpunkt der Annahme dieser ADV durch den Kunden nicht in der Liste der genehmigten Subunternehmer aufgeführt ist, gelten die Artikel 11.2 und 11.3. Zur Ausräumung von Zweifeln wird ausdrücklich vereinbart, dass interne Subunternehmer dieser Bestimmung nicht unterliegen und der Kunde keine Einwände gegen den Einsatz interner Subunterneh-

mer erhebt.

10.3 Übermittlung fon Personenbezogenen Daten in Drittländer:

10.3.1 Der Kunde bestätigt und akzeptiert hiermit ausdrücklich, dass Unify Personenbezogene Daten nach Artikel 8.1 an externe Subunternehmer übertragen bzw. von solchen verarbeiten lassen kann, auch wenn diese externen Subunternehmer sich außerhalb der Europäischen Wirtschaftsraumes (EWR) befinden.

10.3.2 Interne Subunternehmer sind Teil der Atos Gruppe und daher an die Verbindlichen Internen Datenschutzvorschriften (Binding Corporate Rules, „die BCR“) der Atos Gruppe gebunden, deren Genehmigung durch die EU Commission die Atos Gruppe eingeholt hat, und die unter https://atos.net/content/dam/global/documents/atos-binding-corporate-rules.pdf verfügbar sind. Der Kunde erkennt an, dass im Falle einer Übertragung von personenbezogenen Daten an jedwedes außerhalb des EWRs befindlichen Unternehmens der Atos Gruppe die BCR einen ausreichende Garantie darstellen, dass diese Unternehmen einen angemessenen Schutz der Personenbezogenen Daten sicherstellen im Sinne der Anwendbaren Datenschutzgesetze. Der Kunde stimmt daher ausdrücklich zu dass Personenbezogene Daten an jedes Unternehmen der Atos Gruppe übertragen werden können, die an die BCR gebunden und als solche in Annex 2 der BCR aufgeführt sind. Der Kunde verpflichtet sich die betroffenen Personen hinsichtlich der Atos BCR angemessen zu informieren.

10.3.3 Für den Fall, dass Unify Personenbezogene Daten an externe Subunternehmer außerhalb des EWR überträgt, die nicht durch die Atos BCR abgedeckt sind, erteilt der Kunde Unify ausdrücklich das Mandat, in entsprechende Vereinbarungen zu treten, soweit diese sicherstellen, dass das empfangende Unternehmen ein von relevanten EU oder lokalen Aufsichtsbehörden als angemessen anerkanntes Ausmaß an Schutz der Personenbezogenen Daten gewährleistet.

11. Änderungen an dieser ADV

11.1 Der Kunde bestätigt, dass die in der vorliegenden ADV sowie in Anlage 1 aufgeführten Bedingungen von Unify geändert werden können. Eine Änderung bedarf der Zustimmung des Kunden, wenn sie a) die Aufteilung der Verantwortlichkeiten zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Abschnitt 4 betrifft oder b) die Rechte des Kunden einschränkt oder c) die Zustimmung gemäß den anwendbaren Datenschutzgesetzen erfordert. In anderen Fällen bedarf eine Änderung nur der Benachrichtigung des Kunden.

11.2 Im Falle einer Änderung, die die Zustimmung des Kunden erfordert, benachrichtigt Unify den Kunden per E-Mail an den Tenancy-Administrator, unter dem die Cloud-Service-Tenancy des Kunden bei Unify registriert ist, oder über den akkreditierten Vertriebspartner von Unify, mit dem der Kunde den Cloud Services-Vertrag für Unify Cloud Services abgeschlossen hat, über die Änderung und stellt dem Kunden relevante Informationen mindestens dreißig (30) Kalendertage vor Inkrafttreten der Änderung zur Überprüfung zur Verfügung. Unify gibt dem Kunden die Möglichkeit, seine Zustimmung zu erteilen oder Einwände zu erheben. Erhält Unify nach Ablauf einer auf der Änderungsmitteilung angegebenen Frist, die mindestens zehn (10) Kalendertage nach dem Datum der Mitteilung betragen muss, keine Einwände des Kunden, so gilt die Zustimmung des Kunden als erteilt. Im Notfall können die Kündigungs- und Antwortzeiten kürzer ausfallen.

11.3 Der Kunde darf nur mit ausführlicher schriftlicher Erläuterung gegenüber Unify Einwände gegen eine Änderung erheben. Unify unternimmt Anstrengungen im wirtschaftlich vertretbaren Rahmen, um Bedenken des Kunden Rechnung zu tragen. Beide Parteien arbeiten in gutem Glauben zusammen, um zu einer Einigung zu gelangen. Wird keine Einigung erzielt, so wird die Bereitstellung der im Vertrag mit dem Kunden beschriebenen Unify Cloud Services eingestellt.

12. Haftung

12.1 Unify und der Kunde erfüllen ihre jeweiligen Verpflichtungen im Sinne dieser ADV und der anwendbaren Datenschutzgesetze.

12.2 Der Kunde haftet vollumfänglich für Verstöße gegen seine Pflichten gemäß Abschnitt 6.1 sowie gemäß Abschnitt 5.

12.3 Unify haftet vollumfänglich für Verstöße gegen seine Pflichten gemäß Abschnitt 6.2 sowie gemäß Abschnitt 7, vorbehaltlich etwaiger Abhängigkeiten vom Kunden.

12.4 Als Auftragsverarbeiter haftet Unify nur dann für den durch die Verarbeitung verursachten Schaden, wenn es Pflichten, die anwendbare Datenschutzgesetze Auftragsverarbeitern auferlegen, nicht erfüllt hat oder wenn es außerhalb der bzw. entgegen den rechtlich zulässigen Anweisungen des Kunden gehandelt hat.

12.5 Die schadensverursachende Partei wird von der Haftung befreit, wenn sie nachweist, dass sie in keinerlei Verantwortung für das Ereignis trägt, durch das der Schaden eingetreten ist.

12.6 Wenn der Kunde und Unify für Schaden verantwortlich sind, der durch Verstoß gegen eine in dieser ADV beschriebene Pflicht hervorgerufen wurde, haftet jede Partei für den gesamten Schaden, um eine wirksame Entschädigung der betroffenen Person zu gewährleisten. Die Partei, die vollständigen Schadenersatz für den erlittenen Schaden geleistet hat, ist sie berechtigt, von der jeweiligen Gegenpartei den Teil des Schadenersatzes zurückzufordern, der deren Anteil an der Verantwortung für den Schaden entspricht.

13. Verschiedenes

Falls eine einzelne Bestimmung dieser ADV gesetzwidrig, ungültig, nichtig, anfechtbar oder nicht durchsetzbar ist, bleibt der Rest der ADV uneingeschränkt in Kraft. Die Parteien vereinbaren eine wirksame Bestimmung, die, soweit rechtlich möglich, der Absicht der Parteien am nächsten kommt.

Annex 1
Technische und Organisatorische Maßnahmen

1. Umsetzung der technischen und organisatorischen Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gemäß Artikel 32 der EU Datenschutzgrundverordnung

1.1 Vertraulichkeit (gem. Art. 32 Abs. 1 lit. b DS-GVO)

Um die Vertraulichkeit der Daten und Systeme zu sicherzustellen, sind Zutritt, Zugriff und Zugang zu Systemen, die personenbezogene Daten speichern, verarbeiten oder weitergeben streng geregelt und werden regelmäßig überprüft. Des Weiteren sind angemessene Verfahren getrennter Verarbeitung und/oder Pseudonymisierung der Daten im Einsatz, um die Vertraulichkeit der Daten und Systeme im jeweils angemessenen Umfang zu sicherzustellen.

1.1.1 Regelung und Kontrolle des Zutritts

Ziel der Regelung und Kontrolle des Zutritts ist, dass Unbefugten der räumliche Zutritt zu solchen Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogener Daten verarbeitet oder genutzt werden.

Alle Rechenzentrumsstandorte von Atos sind durch automatisierte Zutrittskontrollsysteme vor unbefugtem Zutritt gesichert. Die Zutrittsüberwachung erfolgt durch Sicherheitsdienste und/oder automatisierte Schrankensysteme. Nachts werden in den Rechenzentren regelmäßige Rundgänge durch den Sicherheitsdienst vorgenommen.

Es existiert ein klar definiertes Zutrittsberechtigungskonzept zu den Atos Objekten. Der Zutritt der Mitarbeiter zu administrativen Bereichen wird über einen Firmenausweis und Ausweisleser an Büro und/oder Etagenzugängen (elektronische Zutrittskontrolle) kontrolliert. Die erteilten Zutrittsberechtigungen unterliegen regelmäßigen Reviews. Weiterhin sind in den Rechenzentren Pförtner bzw. Empfangspersonal vorhanden. Besucher bzw. Dritte werden in eine Besucherliste eingetragen und haben nur in Begleitung Zutritt zu Räumlichkeiten der Atos.

Der Zutritt zu Rechenzentrumsräumen wird zusätzlich abgesichert:

- Ergänzend zur automatisierten Zutrittskontrolle sind je nach Bedarf weitere Faktoren, wie Biometrie, Pin-Pads, DES-Dongle, permanentes Wachpersonal, etc. zur Zutrittsberechtigung eingerichtet.
- Die Aufteilung der Rechenzentren erfolgt nach dem Schalenprinzip.
- Zutritt für innere Sicherheitsbereiche wird nur einer kleinen, definierten Zahl von Mitarbeitern und Technikern erlaubt.

Über die von Atos betriebenen Rechenzentren hinaus nutzt Unify Rechenzentrumsdienste anderer Unterauftragnehmer, die nach dem Prozess-Stream aufgelistet sind unter: http://go.unify.com/Dataprotection in den jeweiligen Informationen zur Bearbeitung von Dokumenten. Diese Unterauftragnehmer verfügen über gleichwertige Regelungen.

1.1.2 Regelung und Kontrolle des Zugangs

Ziel der Regelung und Kontrolle des Zugangs ist es zu verhindern, dass Datenverarbeitungssysteme, mit denen die Verarbeitung und Nutzung personenbezogener Daten durchgeführt werden, von Unbefugten genutzt werden.

Der Zugang zu Datenstationen (PC, Server, Netzkomponenten) erfolgt durch Berechtigungsvergabe und Authentifizierung in allen Systemen. Die Zugangsregelungen umfassen folgende Maßnahmen:

- Passwortvergabe (Klein- und Großbuchstaben, Sonderzeichen, Zahlen, mindestens 8 Zeichen, regelmäßiger Wechsel, Passworthistorie)
- Firmenausweis mit PKI-Verschlüsselung (2-Faktor-Authentifizierung)
- Rollenbezogene Rechte sind an Zugangskennungen gebunden (Einteilung nach Administrator, Benutzer, etc.)
- Bildschirmsperre bei Abwesenheit mit Passwort-Aktivierung

- Verschlüsselung mobiler Datenträger (auch Festplatten der Notebooks)
- Einsatz von Firewalls und Antivirussoftware inkl. regelmäßiger Sicherheitsupdates und Patches.

1.1.3 Regelung und Kontrolle des Zugangs

Ziel der Regelung und Kontrolle des Zugangs ist es zu verhindern, dass Datenverarbeitungssysteme, mit denen die Verarbeitung und Nutzung personenbezogener Daten durchgeführt werden, von Unbefugten genutzt werden.

Der Zugang zu Datenstationen (PC, Server, Netzkomponenten) erfolgt durch Berechtigungsvergabe und Authentifizierung in allen Systemen. Die Zugangsregelungen umfassen folgende Maßnahmen:

- Rollenbezogene Rechte sind an Zugangskennungen gebunden (Einteilung nach Administrator, Benutzer, etc.)
- Eine eindeutige clear desk policy ist vorhanden.
- Verschlüsselung mobiler Datenträger (auch Festplatten der Notebooks)
- Einsatz von Firewalls und Antivirussoftware inkl. regelmäßiger Sicherheitsupdates und Patches
- Eine regelmäßige Überprüfung aller bestehenden privilegierten Accounts wird durchgeführt.

1.1.4 Regelung und Kontrolle zur getrennten Verarbeitung

Ziel der Regelung und Kontrolle zur getrennten Verarbeitung von Daten ist es zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (können).

Es kommen folgende Maßnahmen zum Einsatz:

- Verwendung von mandantenfähigen Systemen mit logischer Mandantentrennung.
- Zur Sicherstellung des Produktivbetriebs sind Entwicklungs- und Qualitätssicherungssystem vollständig getrennt von den Produktivsystemen. Ein Austausch findet ausschließlich im für die Verarbeitung erforderlichen Rahmen und Umfang statt (Programmdateien, Parameterdateien, etc).
- Der Zugriff auf die Kundensysteme erfolgt nur durch autorisiertes Personal von Unify oder beteiligten Partnern.

1.1.5 Maßnahmen zur Verschlüsselung der Daten

Ziel der Maßnahmen zur Verschlüsselung von personenbezogenen Daten ist, die Übertragung und Speicherung personenbezogener Daten vor unerlaubter Einsicht und Veränderung zu schützen.

Angemessene Verschlüsselungstechniken werden von Unify oder Subunternehmern bereitgestellt und implementiert. Folgende gängige Verschlüsselungstechniken werden u.a. in der Praxis von Unify eingesetzt:

- Durchgängig verschlüsselte Datenübertragung zwischen den Systemen
- Verschlüsselung der Daten vor bei der Speicherung auf Systemen oder vor der Einbringung in Datenbanken
- Verschlüsselung der Datenbank Backups.

2. Integrity Integrität (Art. 32 Abs. 1 lit. b GDPR)

Die Integrität der Daten auf den Systemen wird insbesondere gewährleistet durch Regelungen und Kontrollen bzgl. der Systeme, auf denen personenbezogene Daten eingegeben und von denen diese Daten transferiert bzw. weitergegeben werden.

2.1 Regelung und Kontrolle zur Weitergabe

Ziel der Regelung und Kontrolle zur Weitergabe personenbezogener Daten ist, dass bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Die Daten können vom Kunden an Unify unter Verwendung geeigneter sicherer Übertragungsarten übermittelt werden, die zwischen den Parteien vereinbart werden müssen.

2.2 Eingabekontrolle

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass nachträglich die näheren Um-

ستände der Dateneingabe, Datenveränderung und Datenlöschung überprüft und festgestellt werden können.

Unify hat Zugangsregelungen und Benutzerberechtigungen im Einsatz, wodurch die Identifizierung aller Benutzer und Datenstationen im System möglich ist. Aktivitäten auf den Systemen sind über umfangreiche Logging-Funktionen nachvollziehbar und werden in der Regel per remote Logging außerhalb des zu überwachenden Systems gespeichert. Auf den Servern bzw. in den Programmen werden Änderungen protokolliert.
Die Eingabekontrolle in Datenbanksystemen erfolgt im Rahmen der mit den Datenbanksystemen gelieferten Standardverfahren, die je nach Datenbanksystem bis zur Erfassung aller Eingaben erfolgen kann.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b GDPR)

3.1 Regelungen zur Sicherstellung der Verfügbarkeit

Die eingesetzten Maßnahmen zur Sicherstellung der Verfügbarkeit dienen zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust von Daten.

Folgende Maßnahmen werden in Abhängigkeit vom jeweiligen Schutzbedarf der personenbezogenen Daten umgesetzt:

- Die Sicherung der Daten (Backup-Strategie wie z.B. online/offline; on-site/off-site) erfolgt in regelmäßigen Zyklen gemäß geschlossener Service-Vereinbarungen.
- Die Stromversorgung der Systeme erfolgt unterbrechungsfrei (USV).

3.2 Rasche Wiederherstellbarkeit

Für den sogenannten Katastrophenfall (K-Fall) ist eine Notfallplanung / Krisenplanung in Verbindung mit Notfall- und Wiederanlaufplänen für die Rechenzentren vorhanden. Die Pläne sind überwiegend Data Center-, bzw. Service- oder Kundenspezifisch und in Service Continuity- und Backup-/Recovery- bzw. Notfallkonzepten dokumentiert. Die Funktionsfähigkeit dieser Konzepte wird in regelmäßigen Abständen (meist jährlich) getestet.
Die Notfallpläne unterliegen einem regelmäßigen und kontinuierlichen Prüf- und Verbesserungsprozess.

4. 5.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 2 GDPR)

4.1 Datenschutz-Management

Der Datenschutz bei Atos, und Unify als Teil der Atos Gruppe, besteht aus einer globalen Organisation mit Datenschutzbeauftragten und Legal Experts für die einzelnen Global Business Units (GBU) und Länder.
Die GBU Deutschland verfügt über ein Data Protection Office mit drei bestellten Datenschutzbeauftragten und mindestens einem Legal Expert. Das Data Protection Office ist Bestandteil der Datenschutz- und Informationssicherheitsorganisation, die sich regelmäßig zu ihren Themen austauscht.
Basis für den Datenschutz bei Atos ist die Group Data Protection Policy, welche die Grundsätze zum Datenschutz, aber auch die Prozesse hinsichtlich Rechte der betroffenen Personen, Audits, Schulungen und Bewusstseinsbildung beschreibt und auf die globale Information Security Policy mit ihren weiteren Regularien verweist.

Das Data Protection Office stellt im Atos Integrated Management System (AIMS) Vorgabedokumente, wie Formulare, Checklisten, Handbücher und Arbeitsanweisungen zur Verfügung, die in den HR- und Business-Prozessen verwendet werden. Alle Mitarbeiter sind auf das Datengeheimnis und die Einhaltung von Betriebs- und Geschäftsgeheimnissen verpflichtet worden und sind gemäß DS-GVO, Artikel 29 und 32 (4) angewiesen, personenbezogene Daten nur auf Anweisung des Verantwortlichen zu verarbeiten. Des Weiteren wurden sie auf das Telekommunikationsgesetz § 88 und bei entsprechendem Einsatz auf die Wahrung des Sozialgeheimnisses und/oder Bankgeheimnisses verpflichtet.
In jährlichen verpflichtenden Trainings müssen die Atos-Mitarbeiter ihr Datenschutzbewusstsein aktualisieren.
Die technischen und organisatorischen Maßnahmen zum Datenschutz gemäß DS-GVO, Artikel 32, werden im Rahmen der ISO-Zertifizierung und der ISAE3402-Audits regelmäßig überprüft. Darüber hinaus finden bei internen Prozessaudits auch datenschutzrelevante Fragestellungen Berücksichtigung.

4.2 Security- und Risikomanagement

Atos wickelt ihre Leistungen auf Grundlage eines Sicherheitsmanagementsystems ab. Dieses beinhaltet unter anderem schriftlich dokumentierte Richtlinien und Leitfäden zum IT- / Rechenzentrumsbetrieb. Sie bauen auf gesetzlichen sowie auf intern gefestigten Regelungen auf. Die eingesetzten Sicherheitsprozesse werden regelmäßig überprüft. Die Richtlinien sind auch verbindlich für beauftragte Subunternehmer. Die Atos-Mitarbeiter werden jährlich in verpflichtenden Trainings zur Security Awareness geschult.
Atos hat über alle Unternehmensebenen einen Risiko-Management Prozess implementiert und auf den verschiedenen Ebenen der Organisation dedizierte Risk Manager benannt, welche die Umsetzung des Risk Management sicherstellen.
Die Risiko-Management-Prozesse teilen sich auf in das operative Risiko-Management, welches relevant ist für Ausschreibungen, Verträge (von der Übergabe der Leistung an Atos oder Projektbeginn bis hin zum Projektabschluss oder Ende der Serviceerbringung) und den operativen Bereich, also die relevanten Standorte, Dienstleistungen und Prozesse.
Risiken, ihre Bewertung sowie die Nachverfolgung der definierten Maßnahmen werden in Risk Registern dokumentiert und regelmäßig durch die Verantwortlichen unter Einbindung des verantwortlichen Risk Managers und relevanten Fachleuten überprüft und aktualisiert. Für alle mit der Geschäftstätigkeit verbundenen inhärenten Risiken sind Kontrollen definiert und dokumentiert. Für jede dieser Kontrollen sind Verantwortliche definiert, die die Effektivität regelmäßig überwachen.

4.3 Zertifizierung

Die deutschen Atos Gesellschaften sind nach
- DIN EN ISO 9001:2015 (Qualitätsmanagement)
- ISO / IEC 27001:2013 (Information Security Management)
- ISO / IEC 20000-1:2011 (IT Service Management)

von Ernst & Young CertifyPoint B.V. zertifiziert.
Die Unify Gesellschaften befinden sich derzeit im Onboarding-Prozess.

4.4 Incident Response Management

Auftretende Security Ereignisse werden von Atos nach standardmäßigen, an „ITIL Best Practice“ angelehnte Betriebsverfahren und toolgestützten Prozessen bearbeitet, um möglichst zeitnah einen störungsfreien Betrieb wiederzuerlangen. Security Incidents werden von der Atos Security Management-Organisation zeitnah überwacht und analysiert. Abhängig von der Art des Ereignisses nehmen an deren Bearbeitung zuständige und notwendige Service Teams und Spezialisten teil, ggf. unter Einbeziehung des Atos „Computer Security Incident Response Team“ (CSIRT). Die Unify-Gesellschaften befinden sich derzeit im Onboarding-Prozess zu diesem Incident Response Management. Die Unify-Gesellschaften befinden sich derzeit im Onboarding-Prozess zu diesem Incident Response Management.

4.5 Datenschutzfreundliche Voreinstellung (Art. 25 Absatz 2 GDPR)

Durch datenschutzfreundliche Voreinstellungen („Privacy by Design and by Default“) wird dem Datenschutz bei Atos schon zu einem möglichst frühen Zeitpunkt Rechnung getragen, um eine unrechtmäßige Verarbeitung oder den Missbrauch von Daten präventiv zu verhindern.
Vorgaben zu Privacy by Design und Privacy by Default sind in der Atos Secure Coding Guideline und in der Atos Secure Coding Policy festgelegt.
Um eine möglichst risikoarme Verarbeitung personenbezogener Daten zu erreichen, werden u. a. folgende Schutzmaßnahmen umgesetzt:

- Menge der personenbezogenen Daten minimieren
- Daten so früh wie möglich pseudonymisieren oder verschlüsseln
- Transparenz in Bezug auf die Funktionen und die Verarbeitung Daten herstellen
- Daten so früh wie möglich löschen oder anonymisieren
- Zugriffsmöglichkeiten auf Daten minimieren
- Vorhandene Konfigurationsmöglichkeiten auf die datenschutzfreundlichsten Werte voreinstellen
- Bewertung der Risiken für die betroffenen Personen dokumentieren.