Auftragsdatenverarbeitungsvereinbarung (ADV) für Unify Cloud Services

Gültig ab dem 15. Mail 2018

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

Kunde und Unify nachfolgend jeweils als „Vertragspartei“ und gemeinsam als „Vertragsparteien“ bezeichnet.

Unify Cloud Services ermöglicht es dem Kunden und dessen Unify Cloud Services-Nutzern, Informationen in die als Service bereitgestellte Software einzugeben. Soweit diese Informationen personenbezogene Daten enthalten, vereinbaren die Parteien ausdrücklich, dass diese Auftragsdatenverarbeitungsvereinbarung (ADV) anzuwenden ist, wobei beide Parteien die Rollen und Verantwortlichkeiten eines Verantwortlichen wie folgt gemeinsam wahrnehmen:

- Der Kunde (i) definiert allein oder gemeinsam mit Dritten die Zwecke der Verarbeitung personenbezogener Daten, (ii) ist verantwortlich für die sachliche Richtigkeit der personenbezogenen Daten, (iii) trägt die Verantwortung dafür, die betroffenen Personen über die Verarbeitung personenbezogener Daten und die Modalitäten für die Ausübung ihrer Rechte zu informieren sowie (iv) bei Bedarf die zuständigen Datenschutzbehörden zu benachrichtigen (einschließlich der Meldung von Verletzungen des Schutzes personenbezogener Daten).
- Unify (i) definiert die Mittel der Verarbeitung und (ii) ist verantwortlich für die Implementierung der Sicherheitsmaßnahmen,

und Unify übernimmt zusätzlich die Rolle des Auftragsverarbeiters gemäß den Definitionen in Abschnitt 1. Diese Rollen und Zuständigkeiten werden weiter unten in Abschnitt 4 (Rollen und Verantwortlichkeiten) ausführlicher beschrieben.

Diese Vereinbarung über die Auftragsdatenverarbeitung (nachfolgend: „ADV“) gilt für sämtliche Tätigkeiten im Rahmen von Unify Cloud Services sowie der Allgemeinen Nutzungsbedingungen (ANB) von Unify für diese Unify Cloud Services http://go.unify.com/Dataprotection, bei denen Mitarbeiter von Unify oder von Unify beauftragte Dritte personenbezogene Daten des Kunden.

Die ADV gilt nicht für andere Online- oder Offline-Produkte, Websites oder Dienste von Unify. In Bezug auf Unify Cloud Services hat diese ADV Vorrang vor etwaigen sonstigen Auftragsdatenverarbeitungsvereinbarungen oder ähnlichen Vereinbarungen der Parteien.

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

1. Definitionen

Zusätzlich zu den an anderer Stelle in den TOSP definierten Begriffen gelten folgende 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 „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, physi-

ologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.3 „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.

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

1.5 „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 den Unify Cloud Services im Rahmen dieser ADV wird wie oben beschrieben vereinbart, dass die Parteien die Rollen und Verantwortlichkeiten des Verantwortlichen wie folgt gemeinsam wahrnehmen („Gemeinsam Verantwortliche“):

- Der Kunde (i) definiert allein oder gemeinsam mit Dritten die Zwecke der Verarbeitung personenbezogener Daten, (ii) ist verantwortlich für die sachliche Richtigkeit der personenbezogenen Daten, (iii) trägt die Verantwortung dafür, die betroffenen Personen über die Verarbeitung personenbezogener Daten und die Modalitäten für die Ausübung ihrer Rechte zu informieren sowie (iv) bei Bedarf die zuständigen Datenschutzbehörden zu benachrichtigen (einschließlich der Meldung von Verletzungen des Schutzes personenbezogener Daten).
- Unify (i) definiert die Mittel der Verarbeitung und (ii) ist verantwortlich für die Implementierung der Sicherheitsmaßnahmen,

2. Kategorien von personenbezogenen Daten im Sinne dieser ADV:

Die folgenden Arten bzw. Kategorien von personenbezogenen Daten werden in der Regel von Unify im Sinne der TOSP für die Erbringung von Dienstleistungen erhoben, verarbeitet und genutzt:

- Profildaten: Personenbezogene Daten über die Unify Cloud Services-Nutzer (nachfolgend „Nutzer“), insbesondere Nutzername, Passwort, E-Mail-Adresse, Zugriffsrechte;
- Aktivitätsdaten: Personenbezogene Daten, die aus der Nutzung von Unify Cloud Services durch den Nutzer abgeleitet werden, insbesondere Anrufjournaldaten, Datensätze zur Löschung oder Änderung von Inhalten oder Daten zur Nutzung des Dienstes (z. B. verwendete Endpunkte) durch den Nutzer, soweit diese Daten nicht anonymisiert wurden, um aggregierte Nutzungsdaten zu generieren
- Kurzlebige Daten und Sitzungsdaten: Personenbezogene Daten, die nicht in Unify Cloud Services gespeichert sind (z. B. Anwesenheits- oder Standortinformationen) oder die mit einer angemeldeten Sitzung in Unify Cloud Services in Verbindung stehen (z. B. IP-Adressen)

Ausgenommen von dieser ADV sind die folgenden Kategorien von personenbezogenen Daten:

- Personenbezogene Daten dritter Personen, die Nutzer von Unify Cloud Services in Unify Cloud Services über Textbeiträge, Dokumenten-Uploads oder Sprachaufnahmen eingeben. Solche Daten können von Unify Cloud Services nicht als personenbezogene Daten erkannt werden. Dem Kunden wird empfohlen, die Nutzung dieser personenbezogenen Daten von Unify Cloud Services durch geeignete Datenschutzrichtlinien zu regeln.
- Personenbezogene Daten Dritter Personen, die Nuzter von Unify Cloud Services in ihre Telefonieendgeräte eingeben, wie etwa Pesönliche Adressbücher. Solchen Daten werden nicht von Unify Cloud Services verarbeitet oder gespeichert, sondern verbleiben in den Endgeräten der Nutzer, außerhalb der Unify Cloud Services.

3. 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:

- Firmennutzer in der Cloud Service Tenancy des Kunden,
- Cross-Tenancy Gastnutzer mit Zugriff auf die Cloud Services Tenancy des Kunden (nur in der Cloud Services Tenancy des Kunden gespeicherte Aktivitätsdaten)
- Gastnutzer einer Sitzung mit Zugriff auf die Cloud Services Sitzung des Kunden

4. Rollen und Verantwortlichkeiten von Kunde und Unify

4.1 Rolle und Verantwortlichkeiten des Kunden:

4.1.1 **Zweck und Rechtmäßigkeit der Verarbeitung**: Der Kunde 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 den Cloud Services alle seine Verpflichtungen gemäß 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.

4.1.2 **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 4.2.9.

4.1.3 **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.

4.1.4 **Risikobewertung**: Der Kunde ist verantwortlich für die Bewertung der Risiken, die sich aus der Verarbeitung personenbezogener Daten ergeben

4.1.5 **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 4.2.1, 4.2.3 und 4.2.14 zu den Verantwortlichkeiten von Unify in diesem Zusammenhang sowie Artikel 4.1.12.

4.1.6 **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 4.2.1 und 4.2.3 zu den Verantwortlichkeiten von Unify in diesem Zusammenhang sowie Artikel 4.1.12.

4.1.7 **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 4.2.4.

4.1.8 **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 4.2.5 zu den Verantwortlichkeiten von Unify in diesem Zusammenhang.

4.1.9 **Änderungen in anwendbaren Gesetze:** Der Kunde muss Unify 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.

4.1.10 **Unregelmäßigkeiten oder Fehler bei der Verarbeitung personenbezogener Daten:** Der Kunde hat Unify unverzüglich und umfassend zu informieren, wenn ihm Fehler oder Unregelmäßigkeiten in Zusammenhang mit Datenschutzgesetzen zur Verarbeitung von personenbezogenen Daten bekannt werden.

4.1.11 **Benachrichtigung von Empfängern personenbezogener Daten über Berichtigung oder Löschung personenbezogener Daten bzw. Einschränkung der Verarbeitung**: Unify gibt personenbezogene Daten für keinen anderen Zweck weiter als für die Bereitstellung von Unify Cloud Services (siehe Abschnitt 8). Soweit der Kunde personenbezogene Daten an Empfänger weitergibt, z. B. durch die Verbindung von Unify Cloud Services mit anderen Cloud-Diensten zur Übermittlung personenbezogener Daten über Circuit-Schnittstellen außerhalb von Circuit, ist der Kunde verpflichtet, diese Empfänger über Anfragen von betroffenen Personen zur Berichtigung oder Löschung personenbezogener Daten bzw. zur Einschränkung der Verarbeitung in Kenntnis zu setzen.

4.1.12 **Offenlegung personenbezogener Daten**: Unify legt personenbezogene Daten nur gegenüber Empfängern offen, an welche die personenbezogenen Daten zum Zwecke der Verarbeitung weitergegeben werden müssen. Weitere Informationen finden Sie unter „Informationen zur Verarbeitung“ (http://go.unify.com/Dataprotection). Bestimmte Funktionen von Unify Cloud Services ermöglichen es Kunden und Nutzern, personenbezogene Daten an Dritte weiterzugeben. Soweit der Kunde oder Nutzer des Kunden sich dieser Funktionen bedienen, ist der Kunde dafür verantwortlich, die betroffenen Personen zu informieren (Artikel 4.1.6) und diese Nutzung in die Aufzeichnungen über die Verarbeitung (Artikel 4.1.5) aufzunehmen.

4.2 **Rolle und Verantwortlichkeiten von Unify**

4.2.1 **Mittel zur Verarbeitung:** Unify ist für die Festlegung der Mittel zur Verarbeitung sowie in Bezug auf Artikel 4.1.5 und 4.1.6 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.

4.2.2 **Umfang der Verarbeitung durch Unify**: Unify darf personenbezogene Daten nur im Rahmen dieser ADV und der TOSP erfassen und verarbeiten, die für die dem Kunden zur Verfügung gestellten Unify Cloud Services gelten, sowie um diese Dienste zu verbessern und zu aktualisieren. Wesentliche Änderungen am Umfang der Datenvereinbarung müssen gemeinsam vereinbart und dokumentiert werden. Unify bestätigt ausdrücklich, dass es personenbezogene Daten nur zur Bereitstellung von Unify Cloud Services sowie zur Verbesserung und Aktualisierung solcher Dienste verarbeitet.

4.2.3 **Implementierung von Sicherheitsmaßnahmen**: Unify ist verantwortlich für die Implementierung von Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten im Rahmen von Unify Cloud Services. 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 Schutzes personenbezogener Daten gemäß den anwendbaren Datenschutzgesetzen zu schützen. Dem Kunden ist bewusst, dass die TOMs vom technischen Fortschritt und von der weiteren Entwicklung abhängig sind. 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. In Bezug auf Artikel 4.1.5 und 4.1.6 sind Informationen zu diesen TOMs für den Kunden bereitzustellen, insbesondere damit der Kun-

de ein **Verzeichnis von Verarbeitungstätigkeiten** führen und betroffene Personen gemäß den anwendbaren Datenschutzgesetzen informieren kann.

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

4.2.5 **Meldung von Verletzungen des Schutzes personenbezogener Daten**: Im Zusammenhang mit Artikel 4.1.8 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.

4.2.6 **Aufbewahrung personenbezogener Daten/Beschränkung der Löschung**: Von Unify Cloud Services verarbeitete personenbezogene Daten werden in der Regel aufbewahrt, bis a) sie vom Kunden oder Unify Cloud Services-Nutzern gelöscht werden oder b) eine vom Kunden angewiesene Aufbewahrungsfrist abgelaufen ist oder c) die Vereinbarung mit dem Kunden über Unify Cloud Services beendet wird (siehe Artikel 4.2.7 zu den Auswirkungen der Kündigung). Der Kunde kann die Löschung personenbezogener Daten insoweit nicht verlangen, als Unify von Gesetzes wegen verpflichtet ist, Materialien, die personenbezogene Daten enthalten, aufzubewahren. 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 durchführbar ist oder aufgrund der speziellen Art der Speicherung nur mit unverhältnismäßigen Kosten. Der Kunde nimmt zustimmend zur Kenntnis, dass einige Anfragen zusätzliche Vergütungsansprüche seitens Unify mit sich bringen können. Der Unify informiert den Kunden hierüber, bevor er die Anfrage ausführt.

4.2.7 **Löschung und Export personenbezogener Daten bei Beendigung der Cloud Services-Vereinbarung**: Unify ist dafür verantwortlich, alle Daten, die der Kunde und die Unify Cloud Services-Nutzer in die durch Unify Cloud Services zur Verfügung gestellten Softwareanwendungen eingegeben haben („Tenancy-Daten“), einschließlich personenbezogener Daten, am Ende des Kalendermonats nach Ablauf oder Kündigung der Nutzung der Unify Cloud Services durch den Kunden oder jederzeit auf Anfrage des Kunden zu löschen. Auf Anfrage des Kunden hat Unify einen Export von Tenancy-Daten in einem Datenformat bereitzustellen, das vom Kunden zur Übertragung an andere Cloud-Dienste bearbeitet werden kann. Ausnahmen und Einschränkungen finden Sie in Artikel 4.2.6.

4.2.8 **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 Vereinbarung nachzukommen. Ausnahmen und Einschränkungen finden Sie in Artikel 4.2.6.

4.2.9 **Ausübung von Rechten durch betroffener 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.

4.2.10 **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.

4.2.11 **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.

4.2.12 **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.

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

4.2.14 **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 4.1.5 zu den Verantwortlichkeiten des Kunden in diesem Zusammenhang. Unify stellt die entsprechenden Informationen unter „Informationen zur Verarbeitung“ zur Verfügung: http://go.unify.com/Dataprotection.

5. Gegenseitige Vereinbarungen und Verantwortlichkeiten

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

6. Anfragen von Aufsichtsbehörden

6.1 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.

6.2 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.

7. Überprüfungsrechte

7.1 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.

7.2 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.

8. Subunternehmer

8.1 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 Zeitpunkt des Inkrafttretens dieser ADV, einschließlich der anwendbaren Maßnahmen für einen angemessenen Schutz personenbezogener Daten, steht unter http://go.unify.com/Dataprotection zur Verfügung.

8.2 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 9.2 und 9.3. Zur Ausräumung von Zweifeln wird ausdrücklich vereinbart, dass interne Subunternehmer dieser Bestimmung nicht unterliegen und der Kunde keine Einwände gegen den Einsatz interner Subunternehmer erhebt.

8.3 Übermittlung fon Personenbezogenen Daten in Drittländer:

8.3.1 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.

8.3.2 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.

8.3.3 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.

9. Änderungen an dieser ADV

9.1 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.

9.2 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.

9.3 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.

10. Haftung

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

10.2 Der Kunde haftet vollumfänglich für Verstöße gegen seine Pflichten gemäß Abschnitt 4.1 sowie gemäß Abschnitt 5.

10.3 Unify haftet vollumfänglich für Verstöße gegen seine Pflichten gemäß Abschnitt 4.2 sowie gemäß Abschnitt 5, vorbehaltlich etwaiger Abhängigkeiten vom Kunden.

10.4 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.

10.5 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.

10.6 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.

11. Verschiedenes

11.1 Falls eine einzelne Bestimmung dieser ADV gesetzwidrig, ungültig, nichtig, anfechtbar oder nicht durch-

setzbar 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.

Anlage 1

Allgemeine Technische und Organisatorische Maßnahmen von Unify

Bei Unify wurden die gesetzlich geforderten technischen und organisatorischen Maßnahmen auf Grundlage des Datenschutz- und Informationssicherheitsrahmens von Unify (der „DIS-Rahmen“) eingeführt, der die geschäftspolitischen Grundsätze (Stufe 2) und die betrieblichen Verfahren (Stufe 3) entsprechend der internationalen Norm ISO27001 auf Grundlage der Unify-Unternehmensrichtlinie „Richtlinien von Unify zum Datenschutz und zur Datensicherheit“ beschreibt. Die Dokumente sind auf Anfrage für den Kunden zugänglich.

Die folgende Beschreibung des derzeitigen Stands der grundlegenden Maßnahmen zum Schutz von Daten kann nicht alle von Unify getroffenen Sicherheitsmaßnahmen abdecken. Insbesondere im Zusammenhang mit Datenschutz und Datensicherheit ist es zudem nicht möglich, detaillierte Beschreibungen geheimer Maßnahmen bereitzustellen, denn der Schutz von Sicherheitsmaßnahmen gegen unbefugte Weitergabe ist mindestens ebenso wichtig wie die Sicherheitsmaßnahmen selbst.

Der Kunde kann Fragen zu technischen und organisatorischen Maßnahmen mit dem Account-Manager des Kunden, dem Datenschutzbeauftragten von Unify und ggf. mit dem Chief Informationen Security Officer (CISO) von Unify erörtern.

1. Zutrittskontrolle

Technische und organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere hinsichtlich der Legitimation befugter Personen:

Ziel der Zutrittskontrolle ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Aufgrund unterschiedlicher Sicherheitsanforderungen werden Geschäftsgebäude und Einrichtungen in verschiedene Sicherheitszonen mit unterschiedlichen Zutrittsberechtigungen unterteilt. Sie werden von Sicherheitspersonal überwacht. Der Zutritt für Mitarbeiter ist nur mit einem verschlüsselten Ausweis mit Foto möglich. Alle anderen Personen haben nur nach vorheriger Registrierung (z. B. im Haupteingangsbereich) Zutritt.

Zutritt zu besonderen Sicherheitsbereichen (wie dem Service-Zentrum für Wartung per Fernzugriff) wird zusätzlich durch einen separaten Zugangsbereich geschützt. Die baulichen und materiellen Sicherheitsstandards entsprechen den Sicherheitsanforderungen für Rechenzentren.

2. Zugangskontrolle

Technische (Schutz durch Passwörter) und organisatorische (Nutzer-Masterdaten) Maßnahmen bezüglich Nutzer-ID und Berechtigung:

Ziel des Systems der Zugangskontrolle ist es zu verhindern, dass Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, von Unbefugten genutzt werden können.

Die Nutzer-Masterdaten jedes Mitarbeiters und der individuelle Identifizierungscode sind im globalen Kontaktverzeichnis registriert. Zugang zu den Datenverarbeitungssystemen ist nur nach Identifizierung und Berechtigung mithilfe des Identifikationscodes und des Passworts für das jeweilige System möglich.

Außerdem wurden zusätzliche technische Schutzmaßnahmen wie Firewalls und Proxy-Server ergriffen.

Um eine Zugangskontrolle zu gewährleisten, werden Verschlüsselungstechnologien verwendet (z. B. Fernzugriff auf das Unternehmensnetzwerk durch VPN-Tunnel). Es erfolgt eine Beurteilung der Eignung der Verschlüsselungstechnologie für den Schutzzweck.

3. Zugriffskontrolle

Nachfragestruktur des Berechtigungskonzepts und der Datenzugriffsrechte sowie deren Überwachung und Aufzeichnung:

Maßnahmen bezüglich Zugriffskontrolle zielen darauf ab, dass ausschließlich auf Daten zugegriffen werden kann, für die eine Zugriffsberechtigung vorliegt, und personenbezogene Daten bei Verarbeitung und Nutzung und nach Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Zugriff auf für die Ausführung einer bestimmten Aufgabe erforderliche Daten wird innerhalb der Systeme und Anwendungen durch ein Rollen- und Berechtigungskonzept gesichert. Jede Rolle hat nach dem Grundsatz „Need to know“ nur die Rechte, die für die Erfüllung der von der jeweiligen Person auszuübenden Aufgabe erforderlich sind.

Um eine Zugriffskontrolle zu gewährleisten, werden Verschlüsselungstechnologien verwendet (z. B. Fernzugriff auf das Unternehmensnetzwerk durch VPN-Tunnel). Es erfolgt eine Beurteilung der Eignung der Verschlüsselungstechnologie für den Schutzzweck.

4. Weitergabekontrolle

Maßnahmen bezüglich des Transports, des Transfers, der Übermittlung oder Speicherung personenbezogener Daten auf Datenträger (manuell oder elektronisch) sowie bezüglich nachfolgender Überprüfung:

Ziel der Weitergabekontrolle ist es zu gewährleisten, dass personenbezogene Daten während ihres Transfers oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.

Die zur Gewährleistung der Datensicherheit während des Transports, des Transfers und der Übermittlung personenbezogener Daten sowie sonstiger Unternehmens- oder Kundendaten erforderlichen Maßnahmen werden in der Richtlinie zum Schutz vertraulicher geschäftlicher Informationen detailliert beschrieben. Diese Richtlinie enthält eine detaillierte Beschreibung der gesamten Datenverarbeitung von der Erzeugung der Daten bis zu deren Löschung, einschließlich des Umgangs mit solchen Daten entsprechend ihrer Einstufung.

Um eine Weitergabekontrolle zu gewährleisten, werden Verschlüsselungstechnologien verwendet (z. B. Fernzugriff auf das Unternehmensnetzwerk durch VPN-Tunnel). Es erfolgt eine Beurteilung der Eignung der Verschlüsselungstechnologie für den Schutzzweck.

Die Übermittlung personenbezogener Daten an Dritte (z. B. Kunden, Subunternehmer, Dienstanbieter) erfolgt nur, wenn ein entsprechender Vertrag vorhanden ist, und nur für einen bestimmten Zweck. Wenn personenbezogene Daten an Unternehmen mit Geschäftssitz außerhalb der EU/des EWR übermittelt werden, stellt Unify sicher, dass im Zielland oder in der Zielorganisation ein angemessenes Datenschutzniveau entsprechend den EU-Datenschutzanforderungen vorhanden ist, z. B. durch Verwendung von Verträgen auf Grundlage der EU-Musterklauseln.

5. Eingabekontrolle

Maßnahmen bezüglich der nachfolgenden Überprüfung, ob oder von wem Daten eingegeben, verändert oder entfernt worden sind:

Ziel der Eingabekontrolle ist es, mithilfe von angemessenen Maßnahmen zu gewährleisten, dass die Eingabe von Daten nachträglich überprüft und überwacht werden kann.

Systemeingaben werden in Protokolldateien verzeichnet. Dadurch kann zu einem späteren Zeitpunkt überprüft werden, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht wurden.

6. Datenverarbeitungskontrolle

Ziel der Datenverarbeitungskontrolle ist es, sicherzustellen, dass Unify personenbezogene Daten nur in Übereinstimmung mit den von Unify für die vertraglich vereinbarten Cloud-Dienste herausgegebenen Terms of Service Production (TOSP) und den Bestimmungen Datenverarbeitungsvereinbarung (ADV) für Unify Cloud Services verarbeitet.

In Unify Cloud Services verarbeitete personenbezogene Daten sind nur für den technischen Support und die

Betriebsorganisation zugänglich. Unify verfügt über Richtlinien, um zu verhindern, dass dieses Unternehmen personenbezogene Daten für andere Zwecke verwendet oder personenbezogene Daten entgegen den Anweisungen des Kunden an andere Unternehmen oder Dritte weitergibt.

Eine Übermittlung personenbezogener Daten an Dritte, beispielsweise einen Subunternehmer, erfolgt nur unter Berücksichtigung vertraglicher Vereinbarungen und anwendbarer Datenschutzgesetze.

7. Verfügbarkeitskontrolle

Maßnahmen bezüglich der Datensicherung (physisch/logisch):

Ziel der Verfügbarkeitskontrolle ist es zu gewährleisten, dass personenbezogene Daten gegen zufällig Zerstörung oder Verlust geschützt sind.

Wenn personenbezogene Daten nicht mehr für den Zweck benötigt werden, für den sie verarbeitet wurden, werden sie unverzüglich gelöscht. Wir weisen darauf hin, dass bei jeder Löschung die personenbezogenen Daten zunächst nur gesperrt und dann innerhalb einer bestimmten Frist endgültig gelöscht werden. Es wird so verfahren, um zufällige Löschungen oder eine mögliche beabsichtigte Beschädigung zu verhindern.

Aus technischen Gründen können personenbezogene Daten in Sicherheitskopien weiter vorhanden sein und durch Spiegelung von Diensten erzeugt werden. Vorbehaltlich der gesetzlichen Datenaufbewahrungspflicht von Unify (siehe ADV) werden diese Kopien, falls erforderlich, ebenfalls mit einer technisch bedingten Verzögerung gelöscht. Die Verfügbarkeit der Systeme selbst wird entsprechend dem erforderlichen Sicherheitsniveau durch entsprechende Sicherheitsmaßnahmen gewährleistet (z. B. Spiegelung von Festplatten, RAID-Systeme, USV).

8. Trennungsgebot

Maßnahmen bezüglich der getrennten Verarbeitung (Speichern, Ändern, Löschen und Übermitteln) von Daten, die zu unterschiedlichen Zwecken erhoben werden:

Ziel des Trennungsgebots ist es zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Personenbezogene Daten werden nur für interne Zwecke verwendet (z. B. als Bestandteil der jeweiligen Kundenbeziehung). Eine Übermittlung an Dritte, beispielsweise einen Subunternehmer, erfolgt nur unter Berücksichtigung vertraglicher Vereinbarungen und anwendbarer Datenschutzgesetze.

Mitarbeiter werden angewiesen, personenbezogene Daten nur innerhalb des Rahmens und für Zwecke ihrer Pflichten (z. B. Erbringung von Dienstleistungen) zu erheben, zu verarbeiten und zu nutzen. Auf technischer Ebene – Multi-Client-Capability – wird für diesen Zweck die Trennung von Funktionen sowie von Test- und Produktionssystemen verwendet.

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

9.1 **Datenschutz-Management**

Der Datenschutz bei Atos 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.

9.2 **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.

9.3 **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.

9.4 **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).

9.5 **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**

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. Über angemessene technische Voreinstellungen soll sichergestellt werden, dass grundsätzlich nur die personenbezogenen Daten erhoben und verarbeitet werden, die für den konkreten Zweck auch tatsächlich erforderlich sind (Data Minimization principle).
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