Datenschutzvereinbarung für Resale und Co-Delivery Services gem. Art. 28 DSGVO

Gültig ab dem 01. August 2020 („*Gültigkeitsdatum*“)

zwischen Partner („*Partner*“)

und

der Unify Software and Solutions GmbH & Co. KG („*Atos Unify*“),

Partner und Atos Unify nachfolgend jeweils als „*Partei*“ und gemeinsam als „*Parteien*“ bezeichnet.

Präambel
Im Geschäft mit akkreditierten Vertriebspartnern betreibt Atos Unify eine Reihe von Geschäfts- und Serviceprozessen für Atos Unify Systeme und Lösungen mit akkreditierten Vertriebspartnern.

Diese Datenschutzvereinbarung gilt für alle Verarbeitungstätigkeiten, bei denen Atos Unify-Mitarbeiter oder von Atos Unify beauftragte Dritte mit personenbezogenen Daten umgehen, die im Rahmen der folgenden Allgemeinen Geschäftsbedingungen durchgeführt werden, für die Dauer der betreffenden Beauftragung:

a) Allgemeine Geschäftsbedingungen von Atos Unify für Resale und Co-Delivery Services, die von akkreditierten Partnern und Endkunden auf https://unify.com/de/datenschutz-grundverordnung durch „click & accept“ angenommen werden.

und wo anwendbar

b) Partnervertrag mit akkreditierten Vertriebspartnern
c) Allgemeine Geschäftsbedingungen, die bei der Anmeldung von Partnern, die über Atos Unify-akkreditierte Vertriebspartner kaufen, online akzeptiert werden.

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 Atos 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 **„*Co-delivery Services*“** bedeutet die Bereitstellung von Remote-Support und Software-Upgrade-Berechtigung für Updates und zukünftige Versionen, sowie Zugriff auf umfassende Online-Ressourcen.

1.3 **„*Verantwortlicher*“** bezeichnet eine juristische Person oder Organisation, welche selbständig oder gemeinsam mit Dritten den Zweck und die Mittel für die Verarbeitung personenbezogener Daten bestimmt.

1.4 **„*Datenschutzverletzung*“** bezeichnet eine Sicherheitsverletzung die zu einer unbeabsichtigten oder rechtswidrigen Zerstörung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung, oder zum Zugriff auf personenbezogene Daten führt, die im Rahmen dieser Vereinbarung verarbeitet werden

1.5 „***Endkunde***“ bedeutet das rechtlich selbständige Unternehmen, welches der Atos Unify-akkreditierten Vertriebspartner für bestimmte Atos Unify Produkte, Lösungen und Services unter Vertrag hat.

1.6 **" *Partner*"** bezeichnet die Atos Unify-akkreditierten Vertriebspartner, die am Verkauf von Atos Unify-Produkten, -Lösungen und –Services an Endkunden beteiligt sind.

1.7 **„*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.

1.8 **„*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.

1.9 **„*Resale-Services*“** bedeutet die Bereitstellung umfassender, flexibler Support-Services für den Wiederverkauf durch den Partner. Die Pakete enthalten Software-Support mit SLA-Optionen für bestimmte Kundenanforderungen.

2. Anwendungsbereich und Verantwortlichkeit

2.1 Atos Unify verarbeitet personenbezogene Daten im Auftrag des Partners. Dies umfasst Tätigkeiten, die im Vertrag und in der jeweiligen Leistungsbeschreibung bzw. dem Service-Auftrag konkretisiert sind. Der Partner ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an Atos Unify sowie für die Rechtmäßigkeit der hinsichtlich der Datenverarbeitung von ihm Atos Unify erteilten Weisungen allein verantwortlich („***Verantwortlicher***“ im Sinne des Artikel 4 Nr. 7 DS-GVO).

2.2 Als Verantwortlicher hat der Partner Atos Unify als Voraussetzung für dessen Verarbeitung von personenbezogenen Daten Weisungen zu erteilen. Die Weisungen werden anfänglich durch den Vertrag und in der jeweiligen Leistungsbeschreibung bzw. Service-Auftrag festgelegt und können vom Partner danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die von Atos Unify bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung im Rahmen des Änderungsverfahrens behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

3. Zweck der Verarbeitung

Der Zweck der Verarbeitung personenbezogener Daten ist die Abwicklung der Leistungsbeziehung zwischen Atos Unify und Partner und zwischen dem Partner und dem Endkunden. Diese Vereinbarung umfasst Prozesse und Resale Services, die Atos Unify direkt an den Endkunden liefert, sowie Prozesse und Co-Delivery Services, die Atos Unify an den Partner liefert.

4. Kategorien von personenbezogenen Daten

4.1 Die folgenden Kategorien von personenbezogenen Daten werden im Allgemeinen von Atos Unify erfasst und verarbeitet, um die betreffenden Prozesse und Services durchzuführen:

- **Profildaten**: Personenbezogene Daten wie Name, Telefonnummer, Position etc., die Atos Unify sammelt, um Prozesse und Services für Kunden bereitzustellen.
- **Aktivitätsdaten**: wie etwa Log-on Zeiten, geschäftliche Transaktionen, Service-Transaktionen von betroffenen Personen an Atos Unify Tools und in Atos Unify Prozessen, wie auch Logging- und Tracing-Daten, die für die Behebung von Fehlern an Atos Unify-Systemen und -Lösungen, die vom Kunden gemeldet wurden, erforderlich sein 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 (nur Kundenkontakt)
- **Daten von Bezahlkarten (Kreditkarten)**: Falls Bezahlkarten für die Bezahlung von Atos Unify-Produkten,
  -Systemen und -Services verwendet werden und falls zutreffend, Atos Unify Cloud Services.
- **Sitzungsdaten**: Personenbezogene Daten, die mit einer Anmeldung an einem Atos Unify Anmelde- und Abwicklungstools (z.B. IP-Adressen) verbunden sind.

4.2 Die folgenden Kategorien von betroffenen Personen sind von der Verarbeitung ihrer personenbezogenen Daten im Rahmen dieser Datenschutzvereinbarung betroffen:

- **Kundenkontakt:** Person, die als Kundenkontakt in einem Vertrag mit Atos Unify fungiert oder sich gegebenenfalls für Atos Unify Cloud Services oder im Atos Unify Partner Portal anmeldet.

- **Rechnungskontakt:** Person, die als Kontakt auf Atos Unify Rechnungen und für die Nachverfolgung von Zahlungen geführt wird.
- **Technischer Kontakt:** Jede andere Person, die im Rahmen einer geschäftlichen Transaktion mit Atos Unify in Verbindung steht und von der persönliche Daten von Atos Unify verarbeitet werden.
- **Partner / Kunden Tool User:** Personen bei Partnern und Endkunden, die Zugang zu einem von Atos Unify bereitgestellten Vertriebs-. Auftrags- oder Service Tool bekommen.
- **Atos Unify Product User:** Nutzer bei Endkunden, welche Atos Unify Produkte oder Lösungen verwenden, die Supportservices von Vertriebspartnern von Atos Unify über ein Atos Unify Service Tool erhalten.

5. Weitergabe personenbezogener Daten durch Atos Unify an akkreditierten Partner

Der Kunde, der Atos Unify-Lösungen von Atos Unify akkreditierten Partnern erworben hat, erklärt sich damit einverstanden, dass Atos Unify die in Abschnitt 3 genannten personenbezogenen Daten an akkreditierten Partner zum Zwecke der Erbringung von Services und der Wartung der Atos Unify-Lösungen der Kunden weitergibt.

6. Pflichten von Atos Unify und des Partners

6.1 Pflichten von Atos Unify

6.1.1 Atos Unify darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Partners verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikels 28 Abs. 3 a) DS-GVO vor. Atos Unify informiert den Partner unverzüglich, wenn Atos Unify der Auffassung ist, dass eine Weisung für Atos Unify aus welchen Gründen auch immer nicht erfüllbar ist oder gegen anwendbare Gesetze verstößt. Die Parteien werden sich in einem solchen Fall auf angemessene Änderungen oder Ergänzungen der Weisung verständigen. Atos Unify ist berechtigt, die Umsetzung der Weisung solange auszusetzen, bis sie vom Partner bestätigt oder geändert wurde. Soweit Atos Unify Weisungen des Partners einhält, haftet Atos Unify nicht für einen daraus resultierenden Verstoß gegen geltendes Recht, insbesondere geltendes Datenschutzrecht und der Partner wird Atos Unify freistellen, soweit Atos Unify diesbezüglich von Dritten in Anspruch genommen wird.

6.1.2 Atos Unify wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie wird technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten treffen, die den Anforderungen der Datenschutz-Grundverordnung (Artikel 32 DS-GVO) genügen. Atos Unify hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen (siehe Anhang).
Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfte Wirksamkeit wird auf die vorliegende Zertifizierung nach DIN ISO 27001 verwiesen, deren Vorlage dem Partner für den Nachweis geeigneter Garantien ausreicht. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt Atos Unify vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

6.1.3 Atos Unify unterstützt, soweit vereinbart, den Partner im Rahmen ihrer Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der DS-GVO sowie bei der Einhaltung der in Artikel 33 bis 36 DS-GVO genannten Pflichten. Interne Aufwände, die Atos Unify dabei entstehen, sind vom Partner nach den allgemein vereinbarten Sätzen zu vergüten

6.1.4 Atos Unify gewährleistet, dass ihren mit der Verarbeitung der Daten befassten Mitarbeitern und anderen für Atos Unify tätigen Personen untersagt ist, die Daten außerhalb der Weisungen des Partners zu verarbeiten. Ferner gewährleistet Atos Unify, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

6.1.5 Atos Unify unterrichtet den Partner unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten, des betroffenen Endkunden bekannt werden.

6.1.6 Datenschutzbeauftragter (DPO): Atos Unify stellt die Kontaktdaten ihres Datenschutzbeauftragten (DPO) im Internet zur Verfügung. Zum Gültigkeitsdatum dieser Vereinbarung lautet die aktuelle E-Mail-

Adresse des DPO wie folgt: dp.it-solutions@atos.net .

6.1.7 Atos Unify gewährleistet, ihren Pflichten nach Artikel 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen

6.1.8 Atos Unify berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Partner dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt Atos Unify die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Partner oder gibt diese Datenträger an den Partner zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Partner zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Die Vergütung und Schutzmaßnahmen für die Vernichtung bzw. Aufbewahrung oder Übergabe sind gesondert zu vereinbaren.

6.1.9 Im Falle einer Inanspruchnahme des Partners durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Artikel 82 DS-GVO, verpflichtet sich Atos Unify, den Partner bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Interne Aufwände, die Atos Unify dabei entstehen, sind vom Partner nach den allgemein vereinbarten Sätzen zu vergüten, es sei denn, Atos Unify hat selbst konkreten Anlass zu der Inanspruchnahme gegeben.

6.1.10 Auf Anfrage des Partners wird Atos Unify den Partner – unter Berücksichtigung des geltenden Datenschutzrechts sowie der Art der Verarbeitung – zur Einhaltung von dessen Verpflichtung, geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit der im Rahmen des Vertrages verarbeiteten personenbezogenen Daten zu definieren, im Rahmen des Änderungsverfahrens unterstützen.

6.1.11 Auf Anfrage des Partners wird Atos Unify dem Partner die bei ihr vorhandenen Informationen zur Verfügung stellen, die erforderlich sind, damit der Partner seinen gesetzlichen Verpflichtungen, wie z.B. die Durchführung einer Datenschutz-Folgenabschätzung oder die Erbringung des Nachweises über die getroffenen technischen und organisatorischen Maßnahmen zwecks Gewährleistung der Datensicherheit, erfüllen kann. Interne Aufwände, die Atos Unify dabei entstehen, sind vom Partner nach den allgemein vereinbarten Sätzen zu vergüten

6.2 Pflichten des Partners

6.2.1 Der Partner wird als Verantwortlicher dafür sorgen, dass die von Atos Unify in seinem Auftrag verarbeiteten personenbezogenen Daten im Einklang mit geltendem Datenschutzrecht verarbeitet werden und dass er seinen eigenen Verpflichtungen in Bezug auf die Auftragsverarbeitung der personenbezogenen Daten nachkommt.

6.2.2 Der Partner hat Atos Unify unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten hinsichtlich datenschutzrechtlicher Bestimmungen feststellt.

6.2.3 Im Falle einer Inanspruchnahme von Atos Unify durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Artikel 82 DS-GVO, gilt Ziffer 6.1.9 entsprechend .

Soweit der Partner personenbezogene Daten von Atos Unify-Mitarbeitern verarbeitet, gelten die Bestimmungen gemäß § 6 entsprechend für den Partner, soweit sie im Verhältnis zum Partner anwendbar sind.

7. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an Atos Unify, wird Atos Unify die betroffene Person an den Partner verweisen, sofern eine Zuordnung an den Partner nach Angaben der betroffenen Person möglich ist. Atos Unify leitet den Antrag der betroffenen Person unverzüglich an den Partner weiter. Atos Unify unterstützt den Partner im Rahmen ihrer Möglichkeiten auf Weisung. Atos Unify haftet nicht, wenn das Ersuchen der betroffenen Person vom Partner nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8. Überprüfungsrechte

8.1 Atos Unify weist dem Partner auf Anfrage die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach, z. B. durch Durchführung eines Selbstaudits, unternehmensinterne Verhaltensregeln, Zertifikat zu Datenschutz oder Informationssicherheit (z. B. ISO 27001).

8.2 Sollten im Einzelfall Inspektionen durch den Partner oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Sollte der durch den Partner beauftragte Prüfer in einem Wettbewerbsverhältnis zu Atos Unify stehen, hat Atos Unify gegen diesen ein Einspruchsrecht.

→ Der Partner stimmt der Benennung eines unabhängigen externen Prüfers durch Atos Unify zu, sofern Atos Unify eine Kopie des Auditberichts zur Verfügung stellt.

→ Für die Unterstützung bei der Durchführung einer Inspektion ist Atos Unify berechtigt, eine Vergütung zu verlangen.

8.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Partners eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

9. Subunternehmer (weitere Auftragsverarbeiter)

9.1 Der Partner nimmt zustimmend zur Kenntnis, dass Atos Unify Subunternehmer für die Erbringung von Services beauftragen kann. Solche Subunternehmer können verbundene Unternehmen der Atos-Gruppe („***interne Subunternehmer***“) oder externe Unternehmen („***externe Subunternehmer***“) sein. Erteilt Atos Unify Aufträge an Subunternehmer, so obliegt es Atos Unify, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer durch geeignete Vereinbarungen (Verträge, verbindliche interne Datenschutzvorschriften, Verhaltensregeln, usw.) zu übertragen. Der Einsatz von Dritten als weitere Auftragsverarbeiter ist jedoch nur zulässig, wenn der Partner vorher zugestimmt hat.

9.2 Eine vollständige Liste der Subunternehmer zum Zeitpunkt des Inkrafttretens dieser Vereinbarung, steht unter https://unify.com/de/datenschutz-grundverordnung#resale-co-delivery zur Verfügung. Diese gilt mit Abschluss dieser Vereinbarung als genehmigt. Atos Unify benachrichtigt den Partner über Änderungen in der Liste der Subunternehmer. Es liegt jedoch in der Verantwortung des Partners, den Endkunden über diese Änderungen in der Liste der Subunternehmer zu informieren.

9.3 Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt Atos Unify die Zustimmung des Partners ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf. Widerspricht der Partner nicht innerhalb einer Frist von zehn Arbeitstagen, gilt die Zustimmung als erteilt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, steht dem Auftragnehmer ein Sonderkündigungsrecht zu.

9.4 Die Zustimmung des Partners gilt als erteilt, soweit der Atos Unify mit ihm verbundene Unternehmen innerhalb der EU / des EWR als Subunternehmer einsetzt oder mit ihm verbundene Unternehmen außerhalb der EU / des EWR einsetzt, die den Binding Corporate Rules der Atos Gruppe unterliegen.

9.5 Übermittlung von personenbezogenen Daten in Drittländer:
Der Partner bestätigt und akzeptiert hiermit ausdrücklich, dass Atos Unify personenbezogene Daten an externe Subunternehmer übertragen bzw. von solchen verarbeiten lassen kann, auch wenn diese externen Subunternehmer sich außerhalb des Europäischen Wirtschaftsraumes (EWR) befinden.

Interne Subunternehmer sind an die Verbindlichen Internen Datenschutzvorschriften (Binding Corporate Rules, „die BCR“) der Atos Gruppe gebunden, deren Genehmigung die Atos Gruppe durch die EU Kommission eingeholt hat, und die unter https://atos.net/content/dam/global/documents/atos-binding-corporate-rules.pdf verfügbar sind. Der Partner erkennt an, dass im Falle einer Übertragung von personenbezogenen Daten an jedwedes außerhalb des EWRs befindlichen Unternehmens der Atos Gruppe die BCR eine ausreichende Garantie darstellen, dass diese Unternehmen einen angemessenen Schutz der personenbezogenen Daten sicherstellen im Sinne der anwendbaren Datenschutzgesetze.
Der Partner stimmt daher ausdrücklich zu, dass personenbezogene Daten an jedes Unternehmen der Atos Gruppe übertragen werden können, die an die BCR gebunden sind.

Übermittelt Atos Unify personenbezogene Daten an einen externen Subunternehmer außerhalb des EWR, der nicht in den Geltungsbereich der Atos BCR fällt, erteilt der Partner Atos Unify hiermit ausdrücklich das Mandat, entsprechende Vereinbarungen zu treffen, um sicherzustellen, dass die empfangende Stelle ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, das von den zuständigen europäischen oder lokalen Behörden anerkannt ist.

10. Haftung

Die Haftung der Parteien für bei Dritten entstandene Schäden (z.B. Betroffenen-Schmerzensgeld) richtet sich nach den gesetzlichen Regelungen. Die Haftung der Parteien untereinander hingegen richtet sich nach den Regelungen des Hauptvertrags.

11. Schlussbestimmungen

11.1 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

11.2 Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anhang über technische und organisatorische Maßnahmen

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

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. 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.

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
- Datenschutzvereinbarung für Resale- and Co-Delivery Services, Version 01. Mai 2019
- Verschlüsselung mobiler Datenträger (auch Festplatten der Notebooks)
- Einsatz von Firewalls und Antivirussoftware inkl. regelmäßiger Sicherheitsupdates und Patches.

1.3. Regelung und Kontrolle des Zugriffs

Die Maßnahmen zur Regelung und Kontrolle des Zugriffs sind darauf ausgerichtet, unerlaubte Tätigkeiten (z.B. unbefugtes lesen, kopieren, verändern oder entfernen) in DV-Systemen außerhalb eingeräumter Berechtigungen zu verhindern.

Bei Atos ist die Authentifizierung aller Benutzer und Datenstationen im System inkl. Zugangsregelungen und Benutzerberechtigungen durch technische Maßnahmen gewährleistet.

Im Rahmen der Zugriffskontrolle sind folgende Maßnahmen implementiert:

- Zugriffsberechtigungen sind eingeschränkt auf Basis definierter Rollen
- Eine Clear Desk Policy ist für alle Atos Mitarbeiter bindend
- Verschlüsselung mobiler Datenträger (auch Festplatten der Notebooks) auf allen mobilen Systemen ist umgesetzt
- Firewall und Antivirussoftware inkl. regelmäßiger Sicherheitsupdates und Patches sind im Einsatz
- Regelmäßiges Review der vorhandenen Administrationskonten (privileged accounts).

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 Atos Unify oder beteiligten Partnern.

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 Atos Unify oder Subunternehmern bereitgestellt und implementiert. Folgende gängige Verschlüsselungstechniken werden u.a. in der Praxis von Atos 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. 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 Atos 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 Umstände der Dateneingabe, Datenveränderung und Datenlöschung überprüft und festgestellt werden können.

Atos 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. 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 Atos 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, Services 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 **Atos Unify Gesellschaften** sind in folgenden Atos-Multisite-Zertifikaten (EY) abgebildet

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

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 Atos Unify-Gesellschaften befinden sich derzeit im Onboarding-Prozess zu diesem Incident Response Management.