Datenschutzvereinbarung für Resale und Co-Delivery Services gem. Art. 26 DSGVO

Gültig ab dem 01. Mai 2019 („Gültigkeitsdatum“)

zwischen Kunde („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 Vertriebspartnern betreibt Unify eine Reihe von Geschäfts- und Serviceprozessen für Unify Systeme und Lösungen, gegebenenfalls auch für Unify Cloud Services.

Soweit Unify personenbezogene Daten bei der Bereitstellung solcher Prozesse und Services verarbeitet, vereinbaren die Parteien ausdrücklich, dass diese Datenschutzvereinbarung für „Gemeinsam für die Verarbeitung Verantwortliche (Joint Controllership)“ anzuwenden ist, wobei beide Parteien die Rollen und Pflichten eines Verantwortlichen wie folgt wahrnehmen:

Unify

i. definiert die Mittel der Verarbeitung,
ii. ist verantwortlich für die Implementierung der Sicherheitsmaßnahmen und
iii. ist verantwortlich für die Meldung von Datenschutzverletzungen an den Kunden.

Der Kunde

i. definierte den Zweck der Verarbeitung,
ii. ist verantwortlich für die sachliche Richtigkeit der personenbezogenen Daten, die Unify zur Verarbeitung zur Verfügung gestellt werden,
iii. ist dafür verantwortlich, die betroffenen Personen über die Verarbeitung ihrer personenbezogener Daten und die Modalitäten für die Ausübung ihrer Rechte zu informieren,
iv. ist verantwortlich für die Information der betroffenen Personen im Falle von Datenschutzverletzungen und
v. ist verantwortlich für die Meldung von Datenschutzverletzungen an die Datenschutzbehörden.

Die Rollen und Pflichten werden in Abschnitt 6 (Rollen und Pflichten) ausführlich beschrieben.

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

a) Allgemeine Geschäftsbedingungen von 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 Unify-akkreditierte Vertriebspartner kaufen, online akzeptiert werden.

Die Vereinbarung gilt für die oben genannten Prozesse und Services, die bereitgestellt werden, um die Geschäftstätigkeit zwischen Unify, akkreditierten Vertriebspartnern und Endkunden zu ermöglichen. Sie hat Priorität gegenüber ande-

ren in Kraft befindlichen Datenschutzvereinbarungen oder ähnlichen Vereinbarungen zwischen Unify und Kunde für Produkte, Websites, Prozesse und Services.

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

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 **„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 den Unify-akkreditierten Vertriebspartner für bestimmte Unify Produkte, Lösungen und Services unter Vertrag hat.

1.6 **"Partner" oder "involvierter Partner"** bezeichnet die Unify-akkreditierten Partner, die am Verkauf von Unify-Produkten, -Lösungen und –Services an Endkunden beteiligt sind, einschließlich wo anwendbar, Unify Cloud Services.

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. Zweck der Verarbeitung

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

3. Kategorien von personenbezogenen Daten

Die folgenden Kategorien von personenbezogenen Daten werden im Allgemeinen von Unify erfasst und verarbeitet, um die Prozesse und Services gemäß den entsprechenden Allgemeinen Geschäftsbedingungen durchzuführen:

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

Für jede Verarbeitungsvorgang stellt Unify detaillierte Informationen zur Verarbeitung unter https://unify.com/de/datenschutz-grundverordnung zur Verfügung.

4. Kategorien von betroffenen Personen

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 Unify fungiert oder sich gegebenenfalls für Unify Cloud Services oder im Unify Partner Portal anmeldet.
- **Rechnungskontakt:** Person, die als Kontakt auf Unify Rechnungen und für die Nachverfolgung von Zahlungen geführt wird.
- **Technischer Kontakt:** Jede andere Person, die im Rahmen einer geschäftlichen Transaktion mit Unify in Verbindung steht und von der persönliche Daten von Unify 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:** Nutzer bei Endkunden, welche Unify Produkte oder Lösungen verwenden, die Supportservices von Vertriebspartnern von Unify über ein Unify Service Tool erhalten.

5. Weitergabe personenbezogener Daten durch Unify an involvierte Partner

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

6. Rollen und Pflichten des Kunden und von Unify

6.1 Rolle und Pflichten des Kunden

6.1.1 **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 verbundenen Unternehmen und Auftragnehmer dazu, bei der Verarbeitung personenbezogener Daten in Verbindung mit den oben genannten Prozessen und Services alle seine Verpflichtungen gemäß den geltenden Datenschutzgesetzen zu erfüllen.

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.

6.1.3 **Richtigkeit, Qualität, Rechtmäßigkeit, und Verlässlichkeit personenbezogener Daten:** Der Kunde trägt die alleinige Verantwortung für die Richtigkeit, Qualität, Rechtmäßigkeit und Verlässlichkeit der personenbezogenen Daten, die Unify zur Verarbeitung zur Verfügung gestellt werden, sowie für die Mittel, mit denen er diese personenbezogenen Daten beschafft.

6.1.4 **Verzeichnis von Verarbeitungstätigkeiten:** Soweit gesetzlich vorgeschrieben, ist der Kunde dafür verantwortlich, ein Verzeichnis von Verarbeitungstätigkeiten zu führen und zu verwalten.

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.

6.1.6 **Information von betroffenen Personen über die Aufteilung der Pflichten:** Der Kunde ist dafür verantwortlich, betroffene Personen über die Aufteilung der Pflichten zwischen den Vertragsparteien gemäß dieser Vereinbarung zu informieren.

6.1.7 **Meldung von Verletzungen des Schutzes personenbezogener Daten:** Nach der Benachrichtigung durch Unify oder Partner über eine Datenschutzverletzung muss der Kunde sämtliche Pflichten in Bezug auf die Meldung von Datenschutzverletzungen erfüllen, die sich aus den anwendbaren Datenschutzbestimmungen ergeben. Soweit durch anwendbare Datenschutzgesetze vorgeschrieben, ist der Kunde für die Meldung von Datenschutzverletzungen an die betroffenen Personen und die Datenschutzbehörden verantwortlich.

6.1.8 **Änderungen anwendbarer Gesetze:** Der Kunde muss Unify rechtzeitig über Änderungen an gesetzlichen Bestimmungen informieren, die sich auf die vertraglichen Pflichten von Unify im Rahmen dieser Vereinbarung auswirken und unter Umständen eine Änderung dieser Vereinbarung 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.

6.1.9 **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.

6.2 Rolle und Pflichten von Unify

6.2.1 **Mittel zur Verarbeitung:** Unify ist für die Festlegung der Mittel zur Verarbeitung sowie in Bezug auf Abschnitt 6.1.4 und 6.1.5 für die Bereitstellung von Informationen zu diesen Mitteln für den Kunden verantwortlich, insbesondere damit der Kunde das Verzeichnis von Verarbeitungstätigkeiten führen und betroffene Personen gemäß den anwendbaren Datenschutzgesetzen informieren kann. Die „Informationen zur Verarbeitung“ finden Sie unter https://unify.com/de/datenschutz-grundverordnung#resale-co-delivery .

6.2.2 **Umfang der Verarbeitung durch Unify**: Unify darf personenbezogene Daten nur im Rahmen dieser Vereinbarung verarbeiten. Wesentliche Änderungen am Umfang der Datenverarbeitung müssen gemeinsam vereinbart und dokumentiert werden.

6.2.3 **Implementierung von Sicherheitsmaßnahmen**: Unify ist verantwortlich für die Implementierung von Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten im Rahmen dieser Vereinbarung. 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 dem technischen Fortschritt und der Weiterentwicklung unterliegen. In diesem Zusammenhang ist es Unify gestattet, geeignete alternative Maß-

nahmen 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.

6.2.4 **Information von betroffenen Personen über die Aufteilung der Pflichten:** Unify ist dafür verantwortlich, diese Datenschutzvereinbarung ohne Änderungen für alle betroffenen Personen öffentlich zugänglich zu machen. Falls diese Vereinbarung vom Kunden gewünschte Änderungen enthält, trägt Unify keine Verantwortung dafür, die Änderungen betroffenen Personen zugänglich zu machen.

6.2.5 **Meldung von Verletzungen des Schutzes personenbezogener Daten**: Im Zusammenhang mit Abschnitt 6.1.7 unterstützt Unify den Kunden im Falle von Datenschutzverletzungen 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 **Aufbewahrung personenbezogener Daten**: Aus rechtlichen Gründen sind Informationen über Verträge, geschäftliche Transaktionen sowie Compliance-Informationen von Ansprechpartnern 10 Jahre nach der Abwicklung oder dem Vertragsende aufzubewahren. Unify löscht daher Daten spätestens am Ende des 10. Jahres nach dem letzten Jahr, in dem der Vertrag endet. Bei anderen Prozessen, wie z.B. System-Traces, die bei einer Servicebereitstellung gezogen werden, löscht Unify personenbezogene Daten früher. Da es sich bei diesen Speicherfristen um unterschiedliche Zeiträume handelt, beachten Sie bitte den jeweiligen Prozessabschnitt auf den Seiten Information of Processing (IoP). https://unify.com/de/datenschutz-grundverordnung#resale-co-delivery .

6.2.7 **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.

6.2.8 **Benachrichtigung von Empfängern personenbezogener Daten über Berichtigung oder Löschung personenbezogener Daten bzw. Einschränkung der Verarbeitung**: Im Falle, dass Unify eine solche Anforderung einer betroffenen Person in Ausübung ihrer Rechte unter den anwendbaren Datenschutzgesetzen ausführt, wird Unify den Vertriebspartner entsprechend der Anforderungen der anwendbaren Datenschutzgesetze davon in Kenntnis setzen – siehe Abschnitt 5.

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

6.2.10 **Verarbeitung von Medien und Testmaterial**: Unify speichert und verarbeitet die ihm vom Kunden zur Verfügung gestellten Medien und alle Kopien oder Reproduktionen davon mit Sorgfalt, sodass sie für Dritte nicht zugänglich sind. Unify ist verpflichtet, die Vernichtung von Testmaterial und anderem Material mit personenbezogenen Daten, das gesetzeskonform entsorgt werden soll, nur auf individuelle Anfrage des Kunden und auf dessen Kosten zu veranlassen.

6.2.11 **Datenschutzbeauftragter (DPO):** Unify stellt die Kontaktdaten seines 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.

7. Gegenseitige Vereinbarungen und Pflichten

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 Services 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 eine gesetzliche Verpflichtung zur Einhaltung der Datenschutzverpflichtungen und zur Wahrung des Datengeheimnisses gebunden ist 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 ausreichende Garantien für die verarbeiteten personenbezogenen Daten 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 diesen Maßnahmen betroffenen personenbezogenen Daten alleiniges Eigentum des Kunden sind, er allein verfügungsberechtigt und gemäß den anwendbaren Gesetzen die verantwortliche Stelle ist.

7.6 Der Kunde erkennt an, dass eine Anweisung des Kunden zur Änderungen an den, für die Erbringung von Services durch Unify festgelegten TOMs (Anlage 1) zu höheren Kosten führen können. In diesem Fall ist Unify berechtigt, den Preis der Services für den Kunden entsprechend zu erhöhen. Unify wird die Anweisung nicht umsetzen, bevor der Kunde über eine solche Preiserhöhung informiert und die Zustimmung des Kunden eingeholt wurde.

8. Anfragen von Aufsichtsbehörden

8.1 Soweit gesetzlich vorgeschrieben, führen beide Parteien Aufzeichnungen über die für die Zwecke dieser Vereinbarung 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 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 Überprüfung der Einhaltung dieser Vereinbarung durch die Gegenpartei durchzuführen, indem sie die von der geprüften Partei durchgeführten technischen und organisatorischen Maßnahmen überprüft. Nachweise über die Umsetzung dieser Maßnahmen, die sich nicht ausschließlich auf diese Vereinbarung 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, interne und/oder externe Datenschutzbeauftragte(n) der geprüften Partei, IT-Sicherheitsabteilung, interne und externe Datenschutzprüfer, Qualitätsprüfer oder durch ein entsprechendes Zertifikat, das nach Prüfung der IT-Sicherheit oder des Datenschutzes der geprüften Partei durch Dritte erstellt wurde.

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

10.2 Der Kunde nimmt zustimmend zur Kenntnis, dass Unify Subunternehmer für die Erbringung von Services beauftragen kann. Solche Subunternehmer können Unternehmen der Atos-Gruppe („interne Subunternehmer“) oder externe Unternehmen („externe Subunternehmer“) sein. Erteilt Unify Aufträge an Subunternehmer, so obliegt es Unify, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer durch geeignete Vereinbarungen (Verträge, verbindliche interne Datenschutzvorschriften, Verhaltensregeln, usw.) zu übertragen.
Eine Liste der Subunternehmer innerhalb der relevanten Prozesse und Dienste zum Datum des Inkrafttretens dieser Datenschutzvereinbarung finden Sie auf der Unify Data Processing Information Website unter https://unify.com/de/data-protection#resale-co-delivery. Unify benachrichtigt den Partner über Änderungen in der Liste der Subunternehmer. Es liegt jedoch auch in der Verantwortung des Partners, den Endkunden über diese Änderungen in der Liste der Subunternehmer zu informieren. Übermittlung von personenbezogenen Daten in Drittländer:

10.2.1 Der Kunde bestätigt und akzeptiert hiermit ausdrücklich, dass Unify personenbezogene Daten nach Abschnitt 10.1 an externe Subunternehmer übertragen bzw. von solchen verarbeiten lassen kann, auch wenn diese externen Subunternehmer sich außerhalb des Europäischen Wirtschaftsraumes (EWR) befinden.

10.2.2 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 eine 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.

10.2.3 Übermittelt Unify personenbezogene Daten an einen externen Subunternehmer außerhalb des EWR, der nicht in den Geltungsbereich der Atos BCR fällt, erteilt der Kunde 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 als anerkannt ist.

11. Änderungen an dieser Vereinbarung

11.1 Der Kunde bestätigt, dass die in der vorliegenden Vereinbarung sowie in Anlage 1 aufgeführten Bedingungen von Unify geändert werden können. Eine Änderung bedarf der Zustimmung des Kunden, wenn sie a) die Aufteilung der Pflichten zwischen den Verantwortlichen 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 der Zustimmung des Kunden bedarf, wird Unify den Kunden oder Partner über die Änderung informieren und dem Kunden mindestens dreißig (30) Kalendertage vor Inkrafttreten der Änderung relevante Informationen zur Überprüfung zur Verfügung stellen. Unify gibt dem Kunden die Möglichkeit, seine Zustimmung zu erteilen oder zu widersprechen. Erhält Unify nach einer in der Änderungsmitteilung angegebenen Reaktionszeit, die mindestens zehn (10) Kalendertage nach dem Datum der Mitteilung beträgt, keine Einwände des Kunden, gilt die Zustimmung des Kunden als erteilt. In Notfallsituationen können Benachrichtigungs- und Reaktionszeiten kürzer sein.

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.

12. Haftung

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

12.2 Der Kunde haftet vollumfänglich für Verstöße gegen seine Pflichten gemäß Abschnitt 6.1 sowie gemäß Abschnitt 7.

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 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.

12.5 Wenn der Kunde und Unify für einen Schaden verantwortlich sind, der durch Verstoß gegen eine in dieser Vereinbarung 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 berechtigt, von der jeweiligen Gegenpartei den Teil des Schadenersatzes zurückzufordern, der deren Anteil an der Verantwortung für den Schaden entspricht.

13. Schlussbestimmungen

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

Anlage 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: https://unify.com/de/datenschutz-grundverordnung 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 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).

1.1.4 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. 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 Umstände 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. 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, 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 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.