Auftragsverarbeitungsvereinbarung
im Sinne des Artikels 28 DSGVO
Für Cloud Services und zugehörige Professional Services

Zwischen
[Name]
„Kunde“

und

Unify Software and Solutions GmbH & Co. KG –
„Unify“ oder „Prozessor“

Inhaltsverzeichnis

Präambel

Diese Auftragsverarbeitungsvereinbarung (nachfolgend "AVV") ist Teil der Allgemeinen Servicebedingungen für den Unify Phone Service (nachfolgend "Vereinbarung"), die der Kunde mit der Unify Software and Solutions GmbH, Otto-Hahn-Ring 6, 81379 München, Deutschland („Auftragnehmer"), bei der Registrierung für den Cloud-Service mittels "Click and Accept" abschließt.

Der Kunde und der Auftragnehmer werden einzeln als "Partei" und gemeinsam als „Parteien" bezeichnet.

Diese AVV zur Vereinbarung beschreibt die Verpflichtungen der Parteien in Bezug auf die Verarbeitung personenbezogener Daten im Namen des Kunden durch den Auftragnehmer zum Zweck der Erbringung der im Vertrag festgelegten Dienstleistungen. Beide Parteien handeln in Übereinstimmung mit den geltenden Datenschutzgrundsätzen, gesetzlichen und vertraglichen Anforderungen.

1. Definitionen

1.1. In Großbuchstaben geschriebene Begriffe, die hier nicht anderweitig definiert sind, haben die Bedeutung, die ihnen in der Vereinbarung gegeben wird. Vorbehaltlich der nachstehenden Änderungen oder Ergänzungen behalten die Definitionen der Vereinbarung ihre volle Gültigkeit und Wirkung. Für die Zwecke der Auslegung dieser AVV haben die folgenden Begriffe die nachstehend angegebene Bedeutung:

Verb	Bedeutung
(a) "Anwendbare Gesetze"	bezeichnet alle gegenwärtigen und zukünftigen Gesetze und Vorschriften (die von Zeit zu Zeit geändert oder aktualisiert werden können), die auf die Verarbeitung personenbezogener Daten im Rahmen dieser Vereinbarung anwendbar sind, einschließlich der Gesetze der Europäischen Union, der Gesetze der Mitgliedstaaten (oder anderer anwendbarer Gesetze eines anderen Landes, einer Provinz, eines Staates oder einer Gerichtsbarkeit, denen die Verarbeitung der personenbezogenen Daten unterliegt). Für die Durchführung dieser Vereinbarung beziehen sich die anwendbaren Gesetze auf die DSGVO, das deutsche Bundesdatenschutzgesetz und alle anderen in Deutschland geltenden Gesetze und Verordnungen in Bezug auf die Verarbeitung und den Schutz von personenbezogenen Daten.

Verb	Bedeutung
(b) "für die Verarbeitung Verantwortlicher" (oder "Verantwortlicher")	ist die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über den Umfang, die Zwecke und die Mittel der Verarbeitung personenbezogener Daten entscheidet.
(c) "Auftragnehmer" (oder "Auftragsverarbeiter")	bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen und gemäß den schriftlichen Anweisungen des für die Verarbeitung Verantwortlichen verarbeitet.
(d) "DSGVO" oder "Datenschutz-Grundverordnung "	bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 "zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG" in ihrer jeweils geltenden Fassung.
(e) "Verarbeitung" (oder verwandte Begriffe)	ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
(f) "Personenbezogene Daten"	bezeichnet alle Informationen über eine identifizierte oder identifizierbare natürliche Person (eine "betroffene Person"), die Unify (bzw. die betroffenen Personen) betreffen und vom Dienstleister im Namen von Unify oder einem Unify-Kunden gemäß oder in Verbindung mit der Vereinbarung verarbeitet werden. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer

Verb	Bedeutung
	Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, ohne darauf beschränkt zu sein.
(g) "Verletzung des Schutzes personenbezogener Daten".	bedeutet eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden; jede Verletzung der Sicherheit, die ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum Zugriff auf personenbezogene Daten führt, die der Auftragnehmer im Namen des Kunden im Zusammenhang mit der Vereinbarung verarbeitet.
(h) "Unterauftragsverarbeiter" oder "Subunternehmer".	bezeichnet einen von einem Auftragsverarbeiter beauftragten Dritten, der Zugang zu den personenbezogenen Daten des Kunden hat oder potenziell Zugang zu diesen Daten hat oder diese verarbeiten wird.
(i) "Drittland"	jedes Land oder jede Gerichtsbarkeit außerhalb des Herkunftslandes oder des Europäischen Wirtschaftsraums ("EWR").

2. Rollen und Pflichten der Parteien

2.1. Zum Zweck der Verarbeitung personenbezogener Daten erkennen beide Parteien an, dass sie an die Aufgaben und Verpflichtungen der anwendbaren Gesetze und die nachfolgenden Bedingungen gebunden sind.

2.2. Der Zweck dieser AVV ist es, die Verarbeitung personenbezogener Daten in Verbindung mit den Bedingungen der Vereinbarung zu regeln, ungeachtet des Herkunftslandes, des Ortes der Verarbeitung, des Standorts der betroffenen Personen oder eines anderen Faktors.

2.3. Die Parteien vereinbaren ausdrücklich, dass (i) der Kunde der Datenverantwortliche für die personenbezogenen Daten ist, die zum Zweck der Erbringung der vertragsgemäßen Dienstleistungen verarbeitet werden,

und (ii) der Auftragnehmer der Auftragsverarbeiter ist, wenn er bei der Erbringung der Dienstleistungen personenbezogene Daten im Namen und auf schriftliche Anweisung des Kunden verarbeitet.

3. Garantien für die Bearbeitung durch den Kunden

3.1. Der Kunde als für die Datenverarbeitung Verantwortlicher garantiert, dass alle vom Auftragnehmer in seinem Namen für die Zwecke dieser Vereinbarung verarbeiteten personenbezogenen Daten (im Folgenden "personenbezogene Daten des Kunden") in Übereinstimmung mit den geltenden Datenschutzgesetzen verarbeitet werden, einschließlich, aber nicht beschränkt auf seine eigenen Verpflichtungen in Bezug auf die Rechtmäßigkeit der Verarbeitung, die Kategorien der verarbeiteten Daten, die Rechte der betroffenen Personen (einschließlich der Information), die Festlegung und Umsetzung angemessener Aufbewahrungsfristen, die Erledigung etwaiger einschlägiger Formalitäten sowie etwaige Überprüfungen und Zusicherungen in Bezug auf die Angemessenheit der von Unify gegebenen Garantien für die Verarbeitung und den Schutz der personenbezogenen Daten des Kunden. In diesem Zusammenhang garantiert der Kunde, dass er alle notwendigen Schritte unternommen hat, um sicherzustellen, dass seine eigenen Verpflichtungen gemäß den geltenden Rechtsvorschriften eingehalten werden.

4. Austausch von Geschäftsdaten und Kommunikation zwischen den Parteien

4.1. Im Rahmen der Durchführung der Vereinbarung kann es erforderlich sein, dass die Parteien zu Kommunikationszwecken die folgenden Informationen austauschen:

4.1.1. Persönliche Daten: Vorname, Nachname;

4.1.2. Kommunikationsdaten: Telefon, E-Mail, Briefpost; und/oder

4.1.3. Andere: Personenbezogene Daten, zu denen eine Partei der anderen zum Zwecke der Kommunikation zwischen den Parteien Zugang gewährt.

4.2. Beide Parteien verpflichten sich, dass jede Partei als unabhängiger Verantwortlicher handelt, um die oben genannten personenbezogenen Daten für ihre eigenen Mittel und Zwecke zu verarbeiten. Daher erfüllen die Parteien die Verpflichtungen eines für die Verarbeitung Verantwortlichen, wie sie in den geltenden Gesetzen vorgeschrieben sind, um die oben genannten personenbezogenen Daten zu schützen und zu sichern.

5. Weisungen des Kunden

5.1. Als für die Datenverarbeitung Verantwortlicher hat der Kunde dem Auftragnehmer schriftliche und rechtmäßig dokumentierte Weisungen bezüglich der Verarbeitung personenbezogener Daten zu erteilen. Die Parteien sind sich darüber einig, dass die Weisungen des Kunden eine Voraussetzung dafür sind, dass der Auftragnehmer den Kunden bei der Einhaltung seiner Pflichten gemäß den anwendbaren Gesetzen unterstützen kann.

5.2. Die Parteien kommen überein, dass die anfänglichen Weisungen des Kunden für die Verarbeitung personenbezogener Daten in (i) der Vereinbarung und (ii) dieser AVV, einschließlich (a) der Beschreibung der

Verarbeitung personenbezogener Daten (Anhang 1) und (b) der technischen und organisatorischen Maßnahmen (Anhang 3), festgelegt sind.

5.3. Vorbehaltlich der Bestimmungen dieser AVV und im gegenseitigen Einvernehmen der Parteien kann der Kunde zusätzliche schriftliche Weisungen erteilen, die mit den Bestimmungen dieser Vereinbarung übereinstimmen.

5.3.1. In diesem Fall wird der Kunde den Auftragnehmer mindestens dreißig (30) Tage vor dem gewünschten Ausführungstermin schriftlich benachrichtigen, um die vom Kunden vorgeschlagenen zusätzlichen Weisungen zu bewerten und die Durchführbarkeit des Ausführungszeitrahmens zu beurteilen. Um jeden Zweifel auszuschließen, werden alle zusätzlichen Weisungen zwischen den Parteien durch Ausfüllen und Unterzeichnung von Anhang 2 vereinbart.

5.4. Für den Fall, dass der Kunde die Durchführung von Änderungen oder Ergänzungen seiner Weisungen verlangt, vereinbaren die Parteien ausdrücklich, dass dies direkte Auswirkungen auf die Erbringung der Dienstleistungen haben kann, die eine Überprüfung und Änderung der Vereinbarungsbedingungen, insbesondere des Umfangs der Dienstleistungen und der Kosten für die Durchführung, erfordern können. In diesem Fall wenden die Parteien die in Abschnitt 15 der Vereinbarung festgelegten Änderungskontrollverfahren oder das in Abschnitt 5.2 beschriebene Verfahren für zusätzliche Weisungen an.

6. Pflichten des Auftragnehmers

6.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Kunden ausschließlich und nur in Übereinstimmung mit den vom Kunden erhaltenen Weisungen, wie sie in Anhang 1 dieser AVV dokumentiert sind.

6.2. Wenn der Auftragnehmer feststellt, dass die ihm vom Kunden erteilte(n) Weisung(en) einen Verstoß gegen geltendes Recht darstellen oder darstellen könnten, wird er den Kunden unverzüglich in schriftlicher Form über diesen tatsächlichen oder möglichen Verstoß informieren.

6.3. Der Auftragnehmer wird alle neuen rechtmäßigen oder geänderten Weisungen des Kunden befolgen, vorbehaltlich Abschnitt 4.3 dieser AVV. Falls die Weisungen des Kunden im Widerspruch zu den geltenden Gesetzen stehen oder stehen könnten, stellt der Auftragnehmer die Verarbeitung oder den Teil der Verarbeitung ein, der gegen das geltende Recht verstößt, und informiert den Kunden darüber, um neue, überarbeitete und rechtmäßige Weisungen zu erhalten.

6.4. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie des Risikos unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen wird der Auftragnehmer geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen, dass die Verarbeitung der personenbezogenen Daten des Kunden gemäß den geltenden gesetzlichen Datenschutzanforderungen erfolgt, wie sie in den Anhängen zu dieser AVV dargelegt sind.

6.5. Der Auftragnehmer bestätigt, dass sein Personal, das für die Verarbeitung personenbezogener Daten im Rahmen der Vereinbarung zuständig ist, einer angemessenen Verpflichtung zur Vertraulichkeit der Verarbeitung personenbezogener Daten unterliegt. Der Auftragnehmer stellt außerdem sicher, dass sein Personal, das für die Verarbeitung personenbezogener Daten im Rahmen der Vereinbarung zuständig ist, an einer obligatorischen Schulung oder einem E-Learning über den Schutz der Privatsphäre und personenbezogenen Datenschutz teilnimmt.

7. Verzeichnis von Verarbeitungstätigkeiten

7.1. Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von durchgeführten Tätigkeiten der Verarbeitung, die im Auftrag des Kunden im Zusammenhang mit den im Rahmen der Vereinbarung erbrachten Dienstleistungen durchgeführt werden, sofern dies nach geltendem Recht erforderlich ist. Auf Anfrage des Kunden oder einer zuständigen Aufsichtsbehörde (wie nach geltendem Recht vorgeschrieben) stellt der Auftragnehmer unverzüglich und in jedem Fall innerhalb von fünfzehn (15) Werktagen nach einer solchen Anfrage oder innerhalb des durch geltendes Recht festgelegten Zeitrahmens eine Kopie dieses Verzeichnisses von Verarbeitungstätigkeiten zur Verfügung.

8. Rechte der betroffenen Personen

8.1. Während der Kunde dafür verantwortlich ist, die Art und Weise zu bestimmen, in der er Anfragen der betroffenen Personen zur Ausübung ihrer Rechte nach dem geltenden Datenschutzrecht beantwortet, unterstützt der Auftragnehmer den Kunden in Übereinstimmung mit dem geltenden Datenschutzrecht und unter Berücksichtigung der Art der Verarbeitung durch geeignete Verfahren bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Rechte der betroffenen Person nachzukommen, insbesondere:

8.1.1. den Kunden unverzüglich zu benachrichtigen, wenn ein Empfänger personenbezogener Daten eine Anfrage erhält, die von einer betroffenen Person nach geltendem Recht in Bezug auf personenbezogene Daten an den Kunden hätte gerichtet werden müssen;

8.1.2. sicherstellen, dass der Empfänger personenbezogener Daten nicht auf die Anfrage antwortet, es sei denn, der Kunde und der Auftragnehmer haben sich darauf geeinigt, dass der Auftragnehmer diese Aufgabe übernimmt, oder dies ist nach geltendem Recht, dem der Empfänger personenbezogener Daten unterliegt, erforderlich; in diesem Fall muss der Auftragnehmer den Kunden, soweit dies nach geltendem Recht zulässig ist, über diese rechtliche Anforderung informieren, bevor der Empfänger personenbezogener Daten auf die Anfrage antwortet; und

8.1.3. alle dokumentierten Weisungen des Kunden bezüglich der Reaktion auf Anträgen auf Wahrnehmung von Rechten der betroffenen Personen gemäß den geltenden Gesetzen zu befolgen.

8.1.4. In diesem Zusammenhang übermitteln die Parteien personenbezogene Daten in einem strukturierten, allgemein gebräuchlichen und maschinenlesbaren Format.

9. Interaktionen mit Aufsichtsbehörden

9.1. Auf Verlangen des Kunden unterstützt der Auftragnehmer den Kunden bei der Erfüllung seiner Pflichten gegenüber den zuständigen Datenschutzbehörden, soweit dies erforderlich ist:

9.1.1. Erteilung von Auskünften über eine Verarbeitung, wenn diese zur Unterstützung eines Antrags auf Genehmigung oder Zulassung einer Verarbeitung erforderlich sind;

9.1.2. Bereitstellung von Informationen im Zusammenhang mit einer Verarbeitung, um Informationsanfragen, Kontrollen oder Untersuchungen nachzukommen; und/oder

9.1.3. Bereitstellung von Informationen im Falle einer Verletzung des Schutzes personenbezogener Daten, wie in Abschnitt 14 dieser AVV dargelegt.

10. Sicherheit der Verarbeitung

10.1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen unterstützt der Auftragnehmer den Kunden in Übereinstimmung mit den geltenden Gesetzen bei der Erfüllung seiner Pflicht, geeignete technische und organisatorische Maßnahmen festzulegen und umzusetzen, um die Sicherheit und Vertraulichkeit der im Rahmen dieser AVV verarbeiteten personenbezogenen Daten zu gewährleisten.

11. Datenschutz-Folgenabschätzungen

11.1. Der Auftragnehmer stellt dem Kunden alle Informationen zur Verfügung, die für die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Kunden relevant sind, damit der Kunde die erforderlichen Unterlagen (z. B. eine Datenschutz-Folgenabschätzung) ausfüllen kann.

12. Subunternehmer (weitere Auftragsverarbeiter)

12.1. Der Mitel-Konzern besitzt und betreibt das Unify-Geschäft. Der Kunde bestätigt hiermit ausdrücklich und erkennt an, dass er dem Auftragnehmer seine schriftliche Zustimmung erteilt hat, um personenbezogene Daten ganz oder teilweise an andere Unternehmen des Mitel-Konzerns oder an dritte Unterauftragnehmer für die Verarbeitung personenbezogener Daten zu übermitteln, die zur Erfüllung seiner Verpflichtungen aus der Vereinbarung erforderlich sind. Der Auftragnehmer informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf. Widerspricht der Kunde nicht innerhalb einer Frist von 10 (zehn) Arbeitstagen, gilt die Zustimmung als erteilt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und sofern eine einvernehmliche Lösungsfindung zwischen den Vertragsparteien nicht möglich ist, steht dem Kunden ein Sonderkündigungsrecht zu.

12.2. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer durch geeignete Vereinbarungen (Verträge, verbindliche interne Datenschutzvorschriften, Verhaltensregeln, usw.) zu übertragen.

12.3. Beinhaltet eine solche Übermittlung eine Übermittlung personenbezogener Kundendaten außerhalb des EWR, so gelten die Bestimmungen des nachstehenden Abschnitts 13 dieser AVV.

12.4. Die Liste der zugelassenen Unterauftragnehmer des Auftragnehmers in Bezug auf die vertraglich vereinbarte Leistungserbringung ist in Anlage 1 zu dieser AVV enthalten.

13. Übermittlung von personenbezogenen Kundendaten in Drittländer

13.1. Der Auftragnehmer und seine verbundenen Unternehmen sind an die EU-Standardvertragsklauseln ab dem 4. Juni 2021 gemäß Artikel 47 GDPR gebunden.

13.2. Der Auftragnehmer stellt sicher, dass seine Unterauftragnehmer, die vom Kunden zur Verarbeitung personenbezogener Kundendaten ermächtigt wurden, ein angemessenes Schutzniveau für diese personenbezogenen Kundendaten bieten. Zu diesem Zweck muss der Auftragnehmer: (i) sicherstellen, dass jeder dritte Unterauftragnehmer, der zur Verarbeitung von personenbezogenen Daten des Kunden außerhalb des EWR berechtigt ist, die Verpflichtungen einhält, die in den von der Europäischen Kommission (oder einer anderen zuständigen Behörde) festgelegten Standardvertragsklauseln für die Übermittlung personenbezogener Daten (insbesondere die Standardvertragsklauseln der Europäischen Kommission gemäß der Verordnung (EU) 2016/679) mit dem Kunden oder mit dem Auftragnehmer festgelegt sind; oder (ii) alternative Mittel zu den Standardvertragsklauseln anwenden, um ein angemessenes Schutzniveau für die personenbezogenen Daten des Kunden zu gewährleisten, wenn dies von den zuständigen europäischen oder lokalen Behörden als angemessen anerkannt wird.

14. Sicherheits- und Vertraulichkeitsmaßnahmen

14.1. Der Kunde erkennt an, dass: (i) die vom Auftragnehmer definierten und angewandten technischen und organisatorischen Sicherheitsmaßnahmen auf den Weisungen und Informationen beruhen, die er vom Kunden erhalten hat und die dazu dienen, gemeinsam mit dem Kunden die mit der Verarbeitung der personenbezogenen Daten des Kunden verbundenen Risiken zu beurteilen und zu bewerten, und (ii) er die in Anhang 2 (Anforderungen an die Informationssicherheit) dargelegten technischen und organisatorischen Sicherheitsmaßnahmen überprüft hat und sie unter Berücksichtigung der Risiken der Verarbeitung und des festgelegten Zwecks der Verarbeitung für angemessen hält.

14.2. Der Kunde erklärt sich damit einverstanden, dass für den Fall, dass er seine Verarbeitungsweisungen gemäß den Bestimmungen von Abschnitt 5 dieser AVV ändert, die ursprünglich festgelegten und umgesetzten technischen und organisatorischen Sicherheitsmaßnahmen möglicherweise nicht mehr den Risiken der Verarbeitung und den festgelegten Zwecken der Verarbeitung angemessen sind. In diesem Fall erklärt sich der Kunde damit einverstanden, dass die technischen und organisatorischen Sicherheitsmaßnahmen möglicherweise geändert werden müssen und dass diese Änderungen Auswirkungen auf die Erbringung der Dienstleistungen und die Bedingungen der Vereinbarung, insbesondere die finanziellen Bestimmungen, haben können.

14.3. Der Kunde informiert den Auftragnehmer über alle besonderen Gefahren oder Schwachstellen, von denen er Kenntnis erlangt. Darüber hinaus erkennt der Kunde an, dass von Zeit zu Zeit erhebliche Sicherheitsgefahren und -schwachstellen auftreten und vom Auftragnehmer identifiziert werden können. Wenn solche Gefahren und Schwachstellen aus technischen oder betrieblichen Entscheidungen des Kunden resultieren oder damit zusammenhängen (z.B. beschlossene anfängliche Sicherheitsmaßnahmen, implementierte Systeme usw.), wird der Auftragnehmer den Kunden unverzüglich über diese Gefahr oder Schwachstelle informieren, sobald er davon Kenntnis erlangt. Der Auftragnehmer wird, soweit möglich, Maßnahmen oder Abhilfemaßnahmen empfehlen, um die Auswirkungen der Gefahr oder Schwachstelle zu unterdrücken, abzuschwächen oder zu begrenzen, und die Parteien werden solchen Änderungen im Rahmen der in Abschnitt 15 der Vereinbarung festgelegten Änderungskontrollverfahren zustimmen. Der Kunde trägt alle Kosten im Zusammenhang mit den Aufwänden des Auftragnehmers zur Abschwächung von Gefahren oder Schwachstellen, die sich aus den Handlungen des Kunden ergeben.

15. Verletzungen des Schutzes personenbezogener Daten

15.1. Im Falle einer Verletzung des Schutzes personenbezogener Daten, die während der Erbringung der Dienstleistungen durch den Auftragnehmer auftritt, wird der Auftragnehmer den Kunden unverzüglich, nachdem er davon Kenntnis erlangt hat, über die Verletzung des Schutzes personenbezogener Daten informieren und Folgendes mitteilen

(i) soweit möglich die Kategorien und die ungefähre Zahl der betroffenen Personen, sowie die betroffene Kategorien und die ungefähre Zahl der betroffenen personenbezogenen Datensätze;

(ii) soweit möglich, den Namen und die Kontaktdaten der zuständigen Kontaktstelle, bei der weitere Informationen eingeholt werden können; und

(iii) soweit möglich, eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

15.2. Im Falle einer Verletzung des Schutzes personenbezogener Daten ist der Auftragnehmer verpflichtet:

15.2.1. in Abstimmung mit dem Kunden alle relevanten weiteren Maßnahmen zu ergreifen, die erforderlich sind zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung;

15.2.2. Unterstützung des Kunden bei der Festlegung und Durchführung aller Vorkehrungen, die nach geltendem Recht erforderlich sind (einschließlich etwaiger Meldungen an die zuständigen Aufsichtsbehörden);

15.2.3. eine Aufzeichnung der Informationen über die Verletzung des Schutzes personenbezogener Daten zu führen, einschließlich, soweit möglich, der Ergebnisse ihrer eigenen Untersuchungen und/oder der Untersuchungen der Behörden; und

15.2.4. mit dem Kunden zusammenzuarbeiten und die erforderlichen Maßnahmen zu ergreifen, um zu verhindern, dass sich eine solche Verletzung des Schutzes personenbezogener Daten wiederholt.

15.3. Im Falle einer solchen Verletzung des Schutzes personenbezogener Daten behandeln beide Parteien alle Informationen über die Verletzung des Schutzes personenbezogener Daten mit höchster Vertraulichkeit und arbeiten aktiv an öffentlichen Mitteilungen und/oder offiziellen Meldungen an die zuständigen Behörden mit.

16. Rechtliche Ersuchen um Zugang zu personenbezogenen Kundendaten

16.1. Für den Fall, dass der Auftragnehmer aufgrund anwendbarer Gesetze oder behördlicher Auflagen aufgefordert oder verpflichtet wird, bestimmte Verarbeitungsvorgänge (einschließlich, aber nicht beschränkt auf die Weitergabe an Behörden) in Bezug auf personenbezogene Daten des Kunden in einem Drittland durchzuführen, das kein im Wesentlichen gleichwertiges Schutzniveau für personenbezogene Daten gewährleistet wie der EWR, und im Zusammenhang mit Massenüberwachung oder Überwachungsmaßnahmen, verpflichtet sich der Auftragnehmer hiermit ausdrücklich dazu (i) den Kunden so schnell wie möglich über ein solches Ersuchen oder eine solche Anforderung zu informieren (vorbehaltlich der Einhaltung gesetzlicher Bestimmungen, die ihn daran hindern könnten, den Kunden zu informieren), um die ausdrückliche und schriftliche Zustimmung des Kunden zu einer solchen Verarbeitung einzuholen; (ii) sich, soweit möglich, einem solchen Ersuchen oder einer solchen Anforderung zu widersetzen (insbesondere durch den Hinweis, dass der Auftragnehmer weder Eigentümer der Daten ist, die er im Auftrag des Kunden verarbeitet, noch die Kontrolle über diese Daten hat); oder (iii) den Kunden, soweit möglich und auf dessen Kosten, bei allen Maßnahmen zu unterstützen, die er ergreift, um sich einer solchen Verarbeitung zu widersetzen (sofern er dies beschließt).

17. Prüfungsrechte

17.1. Der Kunde ist berechtigt, einmal jährlich und nach vorheriger schriftlicher Ankündigung mit einer Frist von mindestens vier (4) Wochen ein Audit der Verarbeitungseinrichtungen des Auftragnehmers durchzuführen oder durch einen unabhängigen, ordnungsgemäß beauftragten Dritten

durchführen zu lassen, um die Einhaltung der in dieser AVV festgelegten Pflichten durch den Auftragnehmer sicherzustellen. Jeder Dritte, der ein Audit im Namen des Kunden durchführt, unterliegt einer strengen Geheimhaltungspflicht und darf kein Konkurrent des Auftragnehmers sein. Ein solches Audit darf den Betrieb oder die Geschäftstätigkeiten des Auftragnehmers nicht behindern oder stören und darf sich nur auf den Teil der relevanten informationstechnischen Infrastruktur beziehen, der die personenbezogenen Daten des Kunden verarbeitet.

17.2. Zusätzlich zu dem jährlichen Audit-Recht gemäß 17.1 ist der Kunde berechtigt, zusätzliche Audits im Falle einer Verletzung des Schutzes personenbezogener Daten, auf Anordnung einer zuständigen Datenschutzbehörde oder aufgrund von Änderungen der geltenden Datenschutzgesetze durchzuführen.

17.3. Die Partei, die das Datenschutzaudit durchführt, trägt ihre eigenen Kosten für Audits.

18. Kein Verkauf von persönlichen Daten

18.1. Der Auftragnehmer erkennt an und bestätigt, dass er keine persönlichen Daten als Gegenleistung für Dienstleistungen oder andere Gegenstände erhält, die der Auftragnehmer dem Kunden zur Verfügung stellt. Der Kunde behält alle Rechte und Interessen an seinen persönlichen Daten. Der Auftragnehmer verpflichtet sich, keine Maßnahmen zu ergreifen, die dazu führen würden, dass die Übermittlung personenbezogener Daten an den Auftragnehmer oder vom Auftragnehmer als Verkauf personenbezogener Daten gemäß den geltenden Gesetzen eingestuft wird.

Anhang 1 Allgemeine Beschreibung Der Verarbeitung Von Personenbezogenen Daten Durch Unify

Kontaktinformationen

Unify-Tochtergesellschaften	
Der Datenschutzbeauftragte von Unify	Name: _____ Post: gdpr@mitel.com Tel: _____

Beschreibung der Dienstleistung

Bitte beschreiben Sie in wenigen Worten die von Unify für den Kunden erbrachten Dienstleistungen oder Produkte	Bitte angeben: Cloud Service Unify Phone

Verarbeitungstätigkeiten

Zweck der Verarbeitung	Bitte beschreiben Sie den Vorgang oder die Reihe von Vorgängen, die mit personenbezogenen Daten durchgeführt werden Leistung des Cloud Services Unify Phone inkl. Support. Weitere Details zur Nutzung: *durch Kunden auszufüllen*			
Kategorien von Verarbeitungstätigkeiten* (siehe Definitionsliste unten)	Sammlung*	☒	Konsultation	☐
	Lagerung	☒	Medienhandling (z. B. Versand von Bändern oder optischen Medien)	☐
	Organisation	☐	Offenlegung	☐
	Strukturierung*	☒	Verfügbar machen*	☒
	Aufnahme	☐	Abgleich/Kombination/Matching	☐
	Anpassung	☐	Einschränkung der Nutzung oder des Zugangs*	☒
	Abruf	☒	Löschung oder Zerstörung	☐
	Fernzugriff	☒	Nutzung	☐
	Profilierung	☐	Big Data-Analytik	☐

	Sonstiges (bitte angeben): *Sammlung – ja – für Metadaten *Strukturierung – nicht der Hauptzweck *Verfügbar machen – nicht der Hauptzweck *Einschränkung der Nutzung oder des Zugangs – ja – von Natur aus, aber nicht der Hauptzweck Offenlegung – nein - weil es nicht für den Eigengebrauch des Empfängers freigegeben ist Löschung oder Zerstörung - nein - nicht über die gesetzlich vorgeschriebene Löschung von Daten hinaus
Standort der betroffenen Personen	Europäische Union ☒ Nicht-Europäische Union ☒ Bitte angeben (Nicht-EU): *Als in der EU ansässiger Cloud-Service-Anbieter macht Unify keine Annahmen über den Standort der betroffenen Personen, da die DSGVO für alle betroffenen Personen unabhängig von ihrem Standort gilt. Falls ausländische Datenschutzgesetze erfüllt werden müssen, ist der Kunde verpflichtet, Unify zu benachrichtigen, um zu bestätigen, dass diese ausländischen Gesetze eingehalten werden.*
Kategorien von verarbeiteten personenbezogenen Daten	Daten zur Identifizierung ☒ Verbindungsdaten ☒ Persönliches Leben ☐ Standortdaten ☐ Das Berufsleben ☒ Kontoprofil ☒ Sonstiges (bitte angeben):
Kategorien von verarbeiteten sensiblen personenbezogenen Daten	Keine sensiblen persönlichen Daten ☒ Sozialversicherungsnummer oder nationale Identifikationsnummer ☐ Gewerkschaftszugehörigkeit ☐ Biometrische Daten ☐ Informationen zur Gesundheit ☐ Genetische Daten ☐ Sexuelle Präferenzen ☐

	Bank- und Finanzdaten ☐ Straftaten und Sanktionen ☐ Philosophische, politische oder religiöse Überzeugungen ☐ Telefonabhörungen ☐ *Der Cloud-Dienst ist nicht für die Verarbeitung sensibler Daten gedacht, es ist die Entscheidung des Kunden, ob er solche Daten als Inhalt in die Cloud einspeist.*
Kategorien von betroffenen Personen	Mitarbeiter des Kunden ☒ Endnutzer ☒ Kunden des Kunden ☒ Mitglieder ☒ Auftragnehmer ☒ Besucher ☒ Sonstiges (bitte angeben): *Bei den betroffenen Personen handelt es sich um Benutzer, die vom Kunden für den Unify Phone Service bereitgestellt werden, sowie um externe Anrufer, die ihre Telefonnummer in Protokollen und Anrufjournalen hinterlassen. Unify macht keine Annahmen über die Zugehörigkeit dieser betroffenen Personen zum Kunden.*
Dauer der Aufbewahrung/Löschung personenbezogener Daten	Bitte angeben: Bis zum Vertragsende
	Datenschutz/Privacy-Politik/verbindliche interne Datenschutzvorschriften Referenz: EU-Standard-Vertragsklauseln vom 4. Juni 2021 ☒
	Zertifizierungen nach Sicherheitsstandards (z. B. ISO 27001) Unify ist zertifiziert nach: - DIN EN ISO 9001: 2015 (Qualitätsmanagement); - ISO / IEC 27001: 2013 (Informationssicherheitsmanagement) ☒

	- ISO / IEC 20000-1: 2011 (IT-Service-Management); - ISO / IEC 14001:2015 (Umweltmanagement)	
	Regelmäßige Schulung der Mitarbeiter zum Thema Datenschutz	☒
	Der Kunde als für die Datenverarbeitung Verantwortlicher kann während des Anpassungsprozesses eine andere Länge festlegen.	

Datenschutzpraktiken von Unify

Die Garantien von Unify hinsichtlich der Verarbeitung personenbezogener Daten	
Standort von Unify Verarbeitungs-tätigkeiten	

Name	Adresse	Land	Beschreibung der Dienstleistung
Mitel Networks (Bulgaria) EOOD	2 Maria Luiza Boulevard, TZUM-Business Center, 1000, Sofia, Bulgarien	Bulgarien	Technische Support-leistungen
Mitel Networks Romania S.R.L.	21st Mihail Kogalniceanu str. Bdg. C6/AP11, 500090 Brasov, Rumänien	Rumänien	Technische Support-leistungen
Unify Communications Spain S.A.U.	25 Calle de Albarracin, 28307 Madrid Spanien	Spanien	Technische Support-leistungen
Unify Communications and Collaboration GmbH & Co. KG	Otto-Hahn-Ring 6 81739 München	Deutschland	Technische Support-leistungen

	Mitel Networks Greece AE	455 Irakleiou Ave, Irakleio, 14122 Athen, Griechenland	Griechen-land	Technische Support-leistungen
	Unify – Soluções em Tecnologia da Informação Ltda	Rua do Semeador, 702, Cidade Industrial - Curitiba City, Paraná State, Adressen Code (CEP 81.270-050), Brasilien	Brasilien	Technische Support-leistungen
	Mitel Communications Private Limited	MIDC Plot B1 & B2 Software Technology Park 411062 Talwade, Pune, Maharashtra, Indien	Indien	Technische Support-leistungen (Ressourcen Pool)

Arbeitet Unify mit einem oder mehreren externen Unterauftragnehmern?	YES ☒ NO ☐

Liste der an dem Projekt beteiligten externen Unterauftragnehmer von Unify

Wenn ja, geben Sie bitte die nachstehenden Informationen zu den externen Unterauftragnehmern von Unify an

Name	Adresse	Land	Beschreibung der Dienstleistung
Google Irland Limited	Google-Gebäude Gordon House, 4 Barrow St, Dublin, D04 E5W5, Irland	Irland	Dienstleistungen für Rechenzentren
MongoDB, Inc.	1633 Broadway 38. Stockwerk New York, NY 10019, Vereinigte Staaten	USA	Verwalteter Datenbankservice

	Der Cloud Service wird in Datenzentren in den folgenden Ländern gehostet: Google Cloud Plattform (GCP) Region Frankfurt a.M. (Europe-west3), Deutschland. *Die MongoDB-Datenbanken sind in der Google Cloud Plattform (GCP) Region Frankfurt (Europe-west3) installiert. Encryption at rest wird für die Verschlüsselung der Daten durch Unify mit Schlüsseln verwendet, die Unify gehören und von Unify verwaltet werden. MongoDB ist ein verwalteter Dienst. Unify erstellt die Datenbank auf Knoten, die von MongoDB installiert und verwaltet werden.*

Sicherheitsvorkehrungen für den Fall, dass verbundene Unternehmen oder Unterauftragnehmer von Unify außerhalb der EU ansässig sind oder wenn personenbezogene Daten von außerhalb der EU verfügbar sind	Unify gibt an, welche Maßnahmen es für die Übermittlung personenbezogener Daten an seine Unterauftragnehmer ergreift

Land, das von der EU-Kommission als Land mit einem angemessenen Schutzniveau anerkannt wurde	☒
Die Standardvertragsklauseln der Europäischen Kommission	☒
Spezifische (Ad-hoc-)Vereinbarung zur Datenübermittlung, die ein hohes Schutzniveau erfordert und von den zuständigen Behörden ordnungsgemäß validiert wurde	☐
Die für gültig erklärten verbindliche interne Datenschutzvorschriften von Unify	☒
Die Einhaltung validierten Verhaltensregeln durch Unify	☐

Bitte angeben:

_____

_____

_____

* KATEGORIEN VON VERARBEITUNGSTÄTIGKEITEN	
Begriff	Definition
Anpassung	Bereitstellung von Dienstleistungen, die vorhandene Daten in eine Form umwandeln, die für einen

	bestimmten Zweck besser geeignet ist, indem beispielsweise Daten entfernt werden, die für diesen Zweck nicht erforderlich sind, oder indem sie auf anderem Wege zugänglich gemacht werden.
Ausrichten / Kombinieren / Abgleichen	Bereitstellung von Dienstleistungen, die zwei oder mehr Kundendatensätze verarbeiten, um entweder (a) einen oder mehrere von ihnen zu validieren oder zu aktualisieren oder (b) einen weiteren Datensatz zu erstellen.
Big Data-Analytics	Bereitstellung von Mitteln für die Analyse von Big Data (Big Data ist eine riesige Menge von Datensätzen, die mit herkömmlichen Tools nicht gespeichert, verarbeitet oder analysiert werden können). Big-Data-Analytics ermöglicht die Akkumulation und/oder Abfrage großer Datensätze mit dem Ziel, neue Erkenntnisse oder neue Datensätze zu gewinnen. Zum Beispiel ein Verfahren zur Gewinnung aussagekräftiger Erkenntnisse wie verborgene Muster, unbekannte Korrelationen, Markttrends und Kundenpräferenzen.
Sammlung	Bereitstellung von Dienstleistungen, mit denen direkt Daten erhoben werden können, wie z. B. die Bereitstellung einer Website, die Bewerbungen entgegennimmt, die Verarbeitung schriftlicher Daten oder die Kontaktaufnahme mit Einzelpersonen, um Daten zu erhalten.
Konsultation	Bereitstellung von Dienstleistungen, die einen Verweis auf bestehende Kundendatensätze erfordern, um Anfragen im Namen des Kunden zu beantworten.
Offenlegung	Erbringung von Dienstleistungen, bei denen Kundendaten kopiert oder an einen befugten Dritten für dessen eigene Zwecke übermittelt werden (z. B. an eine Steuerbehörde oder eine Aufsichtsbehörde).
Löschung oder Zerstörung	Bereitstellung von Dienstleistungen, die Daten dauerhaft löschen, so dass sie nicht wiederhergestellt werden können - entweder durch sicheres Löschen/Überschreiben oder durch physische Zerstörung der Medien, auf denen sie gespeichert sind.
Zur Verfügung stellen	Bereitstellung von Dienstleistungen, die den Zugang zu personenbezogenen Daten erleichtern, wie z. B. ein Internet- oder Intranetdienst, der dem Nutzer Zugang zu zulässigen Daten bietet.
Umgang mit Medien	Erbringung von Dienstleistungen zur Organisation, Speicherung oder zum Transport von Datenträgern, die Daten des Kunden enthalten.

Organisation	Bereitstellung von Dienstleistungen zur Verbesserung der Datenqualität oder -zugänglichkeit, z. B. durch Zusammenführung von Daten an einem Ort oder Beseitigung von Vervielfältigung.
Profiling von Einzelpersonen	Bereitstellung von Dienstleistungen, die personenbezogene Daten aus einer oder mehreren Quellen analysieren, um bestimmte persönliche Aspekte in Bezug auf eine natürliche Person zu bewerten, insbesondere um Aspekte in Bezug auf die Arbeitsleistung, die wirtschaftliche Situation, die Gesundheit, die persönlichen Vorlieben, die Interessen, die Zuverlässigkeit, das Verhalten, den Standort oder die Bewegungen dieser natürlichen Person zu analysieren oder vorherzusagen. Mit anderen Worten, es werden Merkmale identifizierbarer Personen ermittelt und/oder Entscheidungen getroffen, wie z. B. Marketingentscheidungen, die sich in der Folge auf bestimmte Personen auswirken können (z. B. die Art von Werbung, die ihnen zugesandt wird, oder die Art von Dienstleistungen, die ihnen angeboten werden).
Aufnahme	Erbringung von Dienstleistungen, die zur Speicherung von Audio- oder Videoaufzeichnungen oder zur Erstellung von Daten auf der Grundlage manueller oder automatisierter Beobachtung zur Reproduktion einer Szene führen. (z. B. elektronische Aufzeichnung von Sprache oder genaue Aufzeichnung eines Gesprächs)
Fernzugriff	Die Möglichkeit für eine autorisierte Person, über eine Netzwerkverbindung aus einer geografischen Entfernung auf einen Computer oder ein Netzwerk zuzugreifen. Sie ermöglicht es den Nutzern, eine Verbindung zu den von ihnen benötigten Systemen herzustellen, auch wenn sie physisch weit entfernt sind.
Einschränkung der Nutzung oder des Zugangs	Bereitstellung von Dienstleistungen, die es ermöglichen, bestimmte Daten unter Quarantäne zu stellen, z. B. zur Erfüllung gesetzlicher Verpflichtungen zur Einschränkung der Verarbeitung oder zur Wahrung der Beweiskraft von Daten für rechtliche/behördliche Zwecke.
Abruf	Bereitstellung von Dienstleistungen, die Anfragen zum Auffinden personenbezogener Daten, z. B. aus Archiven oder Datenbanken, bearbeiten. Abruf ist der Vorgang des Zugriffs auf Daten, entweder aus dem Speicher oder aus einem Speichergerät.
Nutzung	"Nutzung" ist unspezifisch und umfasst eine Vielzahl anderer Verarbeitungskategorien, die hier aufgeführt

	sind. Bitte greifen Sie nur dann auf diesen Begriff zurück, wenn die Verarbeitung alle anderen Kategorien außer Profiling, Kombination und Big Data Analytics umfasst. Verwendete Daten sind Daten, die gerade von einem System aktualisiert, verarbeitet, gelöscht, abgerufen oder gelesen werden. Diese Art von Daten wird nicht passiv gespeichert, sondern bewegt sich aktiv durch Teile einer IT-Infrastruktur
Lagerung	Bereitstellung von Dienstleistungen, die die Möglichkeit bieten, Kundendaten zu speichern (d. h. für die tatsächliche oder mögliche weitere Verwendung aufzubewahren), wie z. B. Cloud-Speicher, Backup oder Archivierung.
Strukturierung	Bereitstellung von Dienstleistungen, die dazu beitragen, Daten so zu ordnen, dass sie leichter zugänglich und für den beabsichtigten Zweck besser nutzbar sind.

Anhang 2 ANFORDERUNGEN AN DIE INFORMATIONSSICHERHEIT

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

Technische und organisatorische Maßnahmen werden gemäß der Technischen und Organisatorischen Maßnahmen Unify umgesetzt.

Anmerkungen:

1. Diese TOM gelten für die Verarbeitung personenbezogener Daten durch Unify für die technische Unterstützung der im Rahmen dieser Vereinbarung weiterverkauften Cloud Services..
2. Maßnahmen, die mit K.A. gekennzeichnet sind, fallen nicht in den Anwendungsbereich der von Unify erbrachten technischen Unterstützungsdienste.
3. Maßnahmen, die mit NEIN gekennzeichnet sind, sind für Cloud Services technisch nicht möglich.

Vertraulichkeit

Physische Zugangskontrolle Ziel der physischen Zugangskontrolle ist es, Unbefugten den Zugang zu den Datenverarbeitungssystemen zu verwehren, auf denen personenbezogene Daten verarbeitet oder verwendet werden.	JA/NEIN
Unify implementiert Kontrollen, die den Zugang von Unbefugten zu Datenverarbeitungssystemen verhindern sollen	JA
Unify teilt die Räumlichkeiten des Rechenzentrums auf	K.A.
Unify setzt ein Videoüberwachungs- und Einbruchserkennungssystem ein, um den Zugang zu Datenverarbeitungssystemen zu überwachen	K.A.
Unify verfügt über Richtlinien zur physischen Zugangskontrolle	JA

Logische Zugangskontrolle Ziel der logischen Zugriffskontrolle ist es, zu verhindern, dass Unbefugte Datenverarbeitungssysteme nutzen, auf denen personenbezogene Daten verarbeitet oder verwendet werden.	JA/NEIN
Unify stellt sicher, dass der Zugriff auf die Datenverarbeitungssysteme mittels Autorisierung und Authentifizierung in allen Systemen erfolgt	JA
Unify vergibt Passwörter an autorisierte Personen	JA
Unify weist autorisierten Personen eine Unternehmens-ID zu	JA
Unify stellt sicher, dass rollenbasierte Rechte an die Zugangskennung gebunden sind	JA
Unify verwendet Verschlüsselung von Datenspeichern während der Übertragung	JA
Unify sorgt für den Einsatz von Firewalls und Antiviren-Software, einschließlich regelmäßiger Sicherheitsupdates und Patches	JA

Logische Zugangskontrolle Ziel der logischen Zugriffskontrolle ist es, zu verhindern, dass Unbefugte Datenverarbeitungssysteme nutzen, auf denen personenbezogene Daten verarbeitet oder verwendet werden.	JA/NEIN
Unify verfügt über Richtlinien, die eine logische Zugriffskontrolle gewährleisten	JA

Zugriffskontrolle für Anwendungen Maßnahmen zur Zugriffskontrolle verhindern die unbefugte Verarbeitung und Aktivitäten (z.B. unbefugtes Lesen, Kopieren, Ändern oder Entfernen) in Datenverarbeitungssystemen durch Personen ohne die erforderliche Berechtigung.	JA/NEIN
Unify sorgt für die systemweite Authentifizierung aller Nutzer und Datenterminals inklusive Zugangsregelungen und Nutzerberechtigungen	JA
Unify implementiert ein rollenbasiertes Autorisierungskonzept	JA
Unify stellt sicher, dass die Zugriffsberechtigung immer auf dem Prinzip der restriktiven Rechtevergabe basiert	JA
Unify setzt ein programmbezogenes Berechtigungskonzept um	JA
Unify stellt sicher, dass gemeinsam genutzte Systeme über eine Mandantentrennung/ einen separaten Datenpool verfügen	JA
Unify hat klare Regeln für die Informationssicherheit am Arbeitsplatz	JA
Unify stellt sicher, dass die Datenspeicher aller mobilen Systeme während der Übertragung verschlüsselt sind	JA
Unify verwendet Firewalls und Antiviren-Software einschließlich regelmäßiger Sicherheitsupdates und Patches	JA
Unify führt eine regelmäßige Überprüfung aller bestehenden privilegierten Konten durch	JA

Trennungskontrolle Ziel der Trennungskontrolle ist es, sicherzustellen, dass Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden können.	JA/NEIN
Soweit keine dedizierten Systeme für genau einen Kunden im Einsatz sind, stellt Unify sicher, dass die eingesetzten Systeme mandantenfähig sind	JA
Die Entwicklungs- und Qualitätssicherungssysteme sind vollständig von den Produktivsystemen getrennt, um einen produktiven Betrieb zu gewährleisten	JA
Unify stellt sicher, dass nur autorisierte Personen über ein gesichertes Administratornetz auf die Kundensysteme zugreifen können	JA

Pseudonymisierung Ziel der Pseudonymisierungsregelung und -kontrolle ist, dass die Verarbeitung personenbezogener Daten so erfolgt, dass die Daten ohne zusätzliche Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und unter entsprechende technische und organisatorische Maßnahmen fallen.	JA/NEIN
Unify verwendet anonymisierte Identifikatoren, die nur über eine separate Datenbank aufgelöst werden können	NEIN
Unify verwendet Server-Kennungen, die keine Rückschlüsse auf die Funktion zulassen	NEIN
Zu den Anforderungen an die Systemhärtung gehört ein striktes Verbot von Login-Bannern mit Informationen über den Typ und die Version der auf den von Unify betriebenen Systemen verwendeten Software	NEIN

Verschlüsselungsmaßnahmen Ziel der Maßnahmen zur Verschlüsselung personenbezogener Daten ist es, den Inhalt der Datenbanken vor unberechtigtem Zugriff und Veränderung zu schützen.	JA/NEIN
Unify kann die Verschlüsselung personenbezogener Daten auf Anweisung des für die Verarbeitung Verantwortlichen sicherstellen	NEIN
Unify verwendet point-to-point- oder end-to-end-SSL-verschlüsselte Datenübertragungen zwischen Systemen	JA
Unify sorgt für die anwendungsbezogene Verschlüsselung der Daten vor der Übertragung an Datenbanken	JA
Unify gewährleistet Verschlüsselung von DB-Backups	JA
Unify führt E-Mail-Verschlüsselung ein	K.A.

Schrems II Sicherheitsmaßnahmen für personenbezogene Daten, die der EU-DSGVO unterliegen Ziel der Maßnahmen zur Verschlüsselung personenbezogener Daten ist es, den Inhalt von Datenbanken vor unbefugtem Zugriff und Veränderung in Ländern zu schützen, die kein angemessenes Schutzniveau in Bezug auf Gesetze zur Massenüberwachung und Überwachungsmaßnahmen gewährleisten.	JA/NEIN
Unify stellt sicher, dass der Grad der Verschlüsselung und/oder Pseudonymisierung im Vergleich zum Risikoniveau im Importland gemäß der vor der Übermittlung durchgeführten Bewertung angemessen ist	JA
Unify stellt nach der Verschlüsselung sicher, dass die kryptografischen Schlüssel entweder im Ausfuhrland, in der Europäischen Union oder in einem solchen Drittland verbleiben, das anerkanntermaßen ein Schutzniveau bietet, das im Wesentlichen dem entspricht, was in der EU in Bezug auf Gesetze zur Massenüberwachung und Überwachungsmaßnahmen vorgeschrieben ist	JA

Schrems II Sicherheitsmaßnahmen für personenbezogene Daten, die der EU-DSGVO unterliegen Ziel der Maßnahmen zur Verschlüsselung personenbezogener Daten ist es, den Inhalt von Datenbanken vor unbefugtem Zugriff und Veränderung in Ländern zu schützen, die kein angemessenes Schutzniveau in Bezug auf Gesetze zur Massenüberwachung und Überwachungsmaßnahmen gewährleisten.	JA/NEIN
Unify stellt sicher, dass bei der Übermittlung personenbezogener Daten in die oben genannten Drittländer der Importeur keinen unverschlüsselten Zugang zu den personenbezogenen Daten haben darf	JA
Unify stellt sicher, dass es auf Anfrage von Unify den dokumentierten Nachweis erbringt, dass sich die kryptografischen Schlüssel gemäß den Anforderungen von Unify befinden	JA

Integrität

Kontrolle der Übertragung Ziel der Übertragungskontrolle ist es, sicherzustellen, dass personenbezogene Daten während der Übertragung, des Transports oder der Speicherung auf einem Datenträger nicht gelesen, kopiert, modifiziert, verändert oder entfernt werden können, und dass dies überprüft und festgestellt werden kann, wenn die Übermittlung personenbezogener Daten durch Übertragungssysteme beabsichtigt ist	JA/NEIN
Unify unterstützt sichere Standardübertragungsarten wie netzbasierte Verschlüsselung (Server zu Server oder Server zu Client und/oder zu Lieferanten) und verschlüsselte Verbindungstunnel	JA
Unify verwendet SSL-Zertifikate für Websites (https://) zur Übertragung von Daten in Formularen	JA
Unify hat Richtlinien für mobile Geräte	JA
Unify führt die Entsorgung von Datenspeichern in einer Weise durch, die mit den Datenschutzbestimmungen vereinbar ist	K.A.
Unify hat klare Regeln für die Informationssicherheit am Arbeitsplatz	JA
Unify verwendet die Verschlüsselung von Datenspeichermedien während der Übertragung (einschließlich Notebook-Festplatten)	JA

Eingabekontrolle Maßnahmen, die geeignet sind, die nachträgliche Prüfung und Feststellung zu erleichtern, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht worden sind	JA/NEIN
Unify hat Zugangsregelungen und Benutzerberechtigungen implementiert, die die Identifizierung aller Benutzer und Datenterminals im System ermöglichen	JA
Alle Überwachungs- und Protokollierungsmaßnahmen werden dem Stand der Technik und der Kritikalität der zu schützenden Daten	JA

Eingabekontrolle Maßnahmen, die geeignet sind, die nachträgliche Prüfung und Feststellung zu erleichtern, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht worden sind	JA/NEIN
angepasst und in dem damit verbundenen wirtschaftlichen Rahmen durchgeführt	

Verfügbarkeit und Widerstandsfähigkeit

Verfügbarkeitskontrolle Das Ziel der Verfügbarkeitskontrolle ist es, sicherzustellen, dass personenbezogene Daten vor versehentlicher Zerstörung, Beschädigung oder Verlust geschützt werden.	JA/NEIN
Unify stellt sicher, dass personenbezogene Daten in Systemen gespeichert werden, die zumindest gegen hardwarebedingten Datenverlust geschützt sind	JA
Unify stellt sicher, dass personenbezogene Daten in sicheren und redundanten Systemen bis hin zu einem räumlich getrennten Bereich gespeichert werden, um eine kurze Wiederherstellungszeit und eine hohe Gesamtverfügbarkeit zu gewährleisten	JA
Unify implementiert Speichersysteme in Kombination mit entsprechenden Softwarekomponenten, die mit einer Technologie ausgestattet sind, die es ermöglicht, definierte Daten zu bestimmten Zeitpunkten wiederherzustellen	JA
Unify führt die Datensicherungen regelmäßig gemäß den bestehenden Servicevereinbarungen durch	JA
Unify sorgt für eine unterbrechungsfreie Stromversorgung der Systeme	JA

Widerstandsfähigkeit / schnelle Wiederherstellung Diese Maßnahme stellt sicher, dass personenbezogene Daten im Falle eines physischen oder technischen Zwischenfalls durch einen Notfallplan und regelmäßige Wiederherstellungstests (mindestens jährlich) schnell wiederhergestellt werden können.	JA/NEIN
Unify stellt sicher, dass eine Notfallplanung / Krisenplanung in Verbindung mit Notfall- und Wiederanlaufplänen für die Rechenzentren vorliegt	JA
Die Notfallpläne unterliegen einem regelmäßigen und kontinuierlichen Prüfungs- und Verbesserungsprozess	JA

Andere Maßnahmen

„Privacy by design and default“ - Datenschutz durch Technikgestaltung und Voreinstellungen	JA/NEIN
Unify stellt durch datenschutzfreundliche Voreinstellungen sicher, dass der Datenschutz zum frühestmöglichen Zeitpunkt berücksichtigt wird,	JA

„Privacy by design and default“ - Datenschutz durch Technikgestaltung und Voreinstellungen	JA/NEIN
um eine unrechtmäßige Verarbeitung oder den Missbrauch von Daten zu verhindern	
Unify minimiert die Menge an personenbezogenen Daten und sorgt für eine Beschränkung der Nutzung	JA
Unify pseudonymisiert oder verschlüsselt Daten so früh wie möglich	JA
Unify schafft Transparenz in Bezug auf Verfahren und Datenverarbeitung	JA
Unify anonymisiert Daten so früh wie möglich	JA
Unify minimiert den Zugang zu Daten	JA
Unify stellt die vorhandenen Konfigurationsoptionen auf die datenschutzfreundlichsten Werte ein	JA
Unify dokumentiert die Bewertung der Risiken für die betroffenen Personen.	JA