

1. GEGENSTAND DIESER DATENVERARBEITUNGSBEDINGUNGEN

- 1.1 Der Kunde, nachfolgend als („**Datenverantwortlicher**“) bezeichnet, ist die Partei, die alleine oder zusammen mit anderen Personen bestimmt, zu welchen Zwecken und in welcher Weise personenbezogene Daten einer betroffenen Person verarbeitet werden.
- 1.2 Unit4 und seine verbundenen Unternehmen, nachstehend als der („**Daten-)**Auftragsverarbeiter“) bezeichnet, ist der Partei, die im Namen des Verantwortlichen handelt, ohne diesem direkt unterstellt zu sein.
- 1.3 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten für den Datenverantwortlichen (und der Datenverantwortliche stimmt der Verarbeitung zu) unter Einhaltung des geltenden Rechts und dieser Datenverarbeitungsbedingungen einschließlich ihrer Verzeichnisse.
- 1.4 Verzeichnis 1 beschreibt ohne Einschränkung die Zwecke und Mittel der Verarbeitung, die Kategorien der personenbezogenen Daten, die verarbeitet werden, und die Aufbewahrungsfrist der personenbezogenen Daten sowie das Land/die Länder (oder den Ort/die Orte), wo die personenbezogenen Daten verarbeitet werden.
- 1.5 Verzeichnis 2 beschreibt die durch den Auftragsverarbeiter ergriffenen anwendbaren Sicherheitsmaßnahmen, deren Angemessenheit der Datenverantwortliche bestätigt.
- 1.6 Verzeichnis 3 nennt die Daten der Unterauftragsverarbeiter.
- 1.7 Verzeichnis 4 enthält die EU-Standardvertragsklauseln, die für die Übertragung personenbezogener Daten aus dem EWR durch den Datenverantwortlichen an einen nicht im EWR ansässigen Auftragsverarbeiter (wie unten in Klausel 2.3 beschrieben) gelten.
- 1.8 Die Parteien aktualisieren von Zeit zu Zeit und bei Bedarf die Verzeichnisse während der Laufzeit dieser Datenverarbeitungsbedingungen.

2. VERARBEITUNG

- 2.1 Der Auftragsverarbeiter und der Datenverantwortliche stellen sich gegenseitig unverzüglich alle Informationen zur Verfügung, die für die ordnungsgemäße Einhaltung der einschlägigen Datenschutzbestimmungen nötig sind.
- 2.2 Die Verarbeitung personenbezogener Daten findet in dem in Verzeichnis 1 genannten Land/Ort bzw. den genannten Ländern/Orten statt. Der Datenverantwortliche erlaubt ausdrücklich die Verarbeitung der personenbezogenen Daten in den in Verzeichnis 1 genannten Ländern/Orten. Falls die Verarbeitung in einem anderen Land oder an einem anderen Ort stattfindet, wird der Auftragsverarbeiter den Datenverantwortlichen darüber informieren.
- 2.3 Sofern die Verarbeitung personenbezogener Daten in einem Land außerhalb des Europäischen Wirtschaftsraums (EWR) stattfindet, das nach der Entscheidung der Europäischen Kommission kein ausreichendes Schutzniveau für personenbezogene Daten bietet, werden die Parteien zur Gewährleistung einer angemessenen vertraglichen Absicherung ihre jeweiligen Pflichten in den EU-Standardvertragsklauseln in Verzeichnis 4 zu diesen Datenverarbeitungsbedingungen einhalten oder für eine andere angemessene Absicherung sorgen, die nach Entscheidung der Datenschutzbehörde oder einer zuständigen Regulierungsstelle ein ausreichendes Schutzniveau bietet; der Datenverantwortliche stimmt einem solchen Vorgehen hiermit zu und weist den Auftragsverarbeiter an, die Verarbeitung durchzuführen.

3. VERANTWORTUNG DES DATENAUFTRAGSVERARBEITERS

- 3.1 Der Datenauftragsverarbeiter verarbeitet die personenbezogenen Daten in ordnungsgemäßer und sorgfältiger Weise gemäß diesen Datenverarbeitungsbedingungen und sorgt für die Einhaltung des Datenschutzgesetzes.
- 3.2 Der Datenauftragsverarbeiter verarbeitet personenbezogene Daten nur zum Zweck der Vertragserfüllung und gemäß den schriftlichen Anweisungen des Datenverantwortlichen, es sei denn der Auftragsverarbeiter ist gesetzlich zu einer anderslautenden Verarbeitung der personenbezogenen Daten verpflichtet. Im letzteren Fall setzt der Auftragsverarbeiter den Datenverantwortlichen über die entsprechenden Gesetzesvorschriften und seine daraus entstehenden Pflichten in Kenntnis.
- 3.3 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur für die Zwecke, für die er Anweisungen erhalten hat, und zur Erfüllung der durch diese Datenverarbeitungsbedingungen übertragenen Pflichten. Der Auftragsverarbeiter verwendet die personenbezogenen Daten für keine anderen Zwecke.
- 3.4 Der Auftragsverarbeiter stellt die personenbezogenen Daten keinem Dritten (außer der betroffenen Person oder anderen durch den Datenverantwortlichen oder den Auftragsverarbeiter zur Verarbeitung der personenbezogenen Daten zugelassenen Personen) zur Verfügung, es sei denn, dieser Austausch findet auf Anweisung des Datenverantwortlichen oder im Rahmen der Erfüllung dieser Datenverarbeitungsbedingungen (einschließlich der Anhänge oder Verzeichnisse) statt oder wenn dies zur Einhaltung einer gesetzlichen Pflicht oder einer behördlichen oder gerichtlichen Anordnung nötig ist.
- 3.5 Der Auftragsverarbeiter wird ohne Anweisung des Datenverantwortlichen die personenbezogenen Daten nicht modifizieren, bearbeiten, ergänzen oder in anderer Weise ändern.
- 3.6 Der Auftragsverarbeiter gewährt dem Datenverantwortlichen seine angemessene Unterstützung bei der Erfüllung von Ersuchen einer betroffenen Person im Zusammenhang mit ihren Rechten laut Datenschutzgesetz, wie beispielsweise: (i) Gewährung des Zugriffs betroffener Personen auf ihre personenbezogenen Daten; (ii) Berichtigung oder Löschung personenbezogener Daten auf Verlangen einer betroffenen Person; (iii) Erbringung von Nachweisen über die Berichtigung oder Löschung ihrer personenbezogenen Daten; (iv) Vorlage der personenbezogenen Daten, die die betroffene Person dem Datenverantwortlichen übermittelt hat und die der Datenverantwortliche an den Auftragsverarbeiter weitergeleitet hat, und (v) Übermittlung personenbezogener Daten der betroffenen Person an einen anderen Datenverantwortlichen (Datenübertragbarkeit). Bei einem Ersuchen zur Rückgabe oder Vorlage einer Kopie der personenbezogenen Daten übermittelt der Auftragsverarbeiter die personenbezogenen Daten in einem strukturierten, verbreiteten und maschinenlesbaren Format.
- 3.7 Falls der Auftragsverarbeiter ein Ersuchen oder einen Einspruch einer betroffenen Person erhält (wobei es sich um ein Ersuchen in Bezug auf (ohne Einschränkung) Informationen, Zugriff, Berichtigung, Datenübertragung, Einführung einer Verarbeitungsbeschränkung oder die Übertragung personenbezogener Daten handeln kann), leitet der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Datenverantwortlichen weiter.
- 3.8 Der Auftragsverarbeiter unterhält gemäß dem Datenschutzgesetz Aufzeichnungen über alle Kategorien der Datenverarbeitungstätigkeiten, die er im Namen des Datenverantwortlichen durchführt. Der Auftragsverarbeiter übermittelt dem Datenverantwortlichen alle diesbezüglich erforderlichen Informationen.
- 3.9 Der Auftragsverarbeiter unterstützt den Datenverantwortlichen bei der Erfüllung seiner gesetzlichen Informations- und Auskunftspflichten gegenüber den Aufsichtsbehörden oder den Betroffenen sowie bei der Durchführung der gesetzlich vorgeschriebenen Datenschutz-Folgenabschätzung, sofern die Technologie des Auftragsverarbeiters betroffen ist.
- 3.10 Erhält der Datenverantwortliche ein spezifisches Auskunftersuchen von einer betroffenen Person oder einem Dritten (außer der betroffenen Person oder anderen Personen, die durch den Datenverantwortlichen oder den Auftragsverarbeiter zur Verarbeitung der personenbezogenen Daten zugelassen sind), der zu einem Ersuchen berechtigt ist, unterstützt der Auftragsverarbeiter den Datenverantwortlichen dabei. Der Auftragsverarbeiter darf keine Schritte in Bezug auf eine Anfrage von einer betroffenen Person oder einem Dritten (außer der betroffenen Person oder anderen Personen, die durch den Datenverantwortlichen oder den Auftragsverarbeiter zur Verarbeitung der personenbezogenen Daten zugelassen sind) unternehmen, außer in

Übereinstimmung mit vorherigen Anweisungen des Datenverantwortlichen. Falls eine betroffene Person sich an den Auftragsverarbeiter wendet, um ihre Ansprüche in Bezug auf das Datenschutzgesetz durchzusetzen, muss der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Datenverantwortlichen weiterleiten.

4 VERANTWORTUNG DES DATENVERANTWORTLICHEN

- 4.1 Der Datenverantwortliche ist für die rechtmäßige Verarbeitung der personenbezogenen Daten und die Einhaltung des Datenschutzgesetzes, einschließlich des Schutzes der Rechte der betroffenen Personen, verantwortlich.
- 4.2 Der Datenverantwortliche ist allein dafür verantwortlich, die Zwecke und die Art der Verarbeitung der personenbezogenen Daten festzulegen.
- 4.3 Der Datenverantwortliche ist dafür verantwortlich, die betroffenen Personen zu informieren und die Rechte zu gewährleisten, die diese aufgrund des Datenschutzgesetzes und anderer geltender Datenschutzgesetze und -vorschriften ausüben können, sowie für die Kommunikation mit den betroffenen Personen.
- 4.4 Der Datenverantwortliche garantiert, dass die erhobenen personenbezogenen Daten in Bezug auf die Zwecke, für die sie übertragen und (weiter)verarbeitet werden, angemessen, sachdienlich und nicht übermäßig umfangreich sind.
- 4.5 Der Datenverantwortliche stellt dem Auftragsverarbeiter alle Informationen, die dieser zur Verarbeitung benötigt, zeitnah und in dem vereinbarten Format wie in Verzeichnis 1 aufgeführt zur Verfügung.
- 4.6 Der Datenverantwortliche ist dafür verantwortlich und haftbar (zwischen den Parteien selbst und gegenüber den betroffenen Personen und der Datenschutzbehörde): (i) sicherzustellen, dass betroffene Personen zur Datenverarbeitung durch den Auftragsverarbeiter (oder Unterauftragsverarbeiter) die entsprechende Zustimmung erteilt haben und es dazu eine entsprechende gesetzliche Grundlage gibt; (ii) der Datenverantwortliche ist auch für Ansprüche oder Beschwerden aufgrund von Handlungen des Auftragsverarbeiters verantwortlich und haftbar, soweit diese Handlungen auf Anweisungen beruhen, die der Auftragsverarbeiter vom Datenverantwortlichen erhalten hat.

5 UNTERAUFTRAGSVERARBEITER

- 5.1 Der Auftragsverarbeiter beauftragt mit Vertragsschluss die im Verzeichnis 3 oder in einem Angebotsformular aufgeführten Unterauftragsverarbeiter.
- 5.2 Der Datenverantwortliche erklärt sich mit einem Wechsel der Unterauftragsverarbeiter für einverstanden. Der Auftragsverarbeiter informiert den Datenverantwortlichen schriftlich und zeitlich vor einer beabsichtigten Änderung, beispielsweise bei Ersatz eines Unterauftragsverarbeiters. Der Datenverantwortliche kann den Änderungen schriftlich innerhalb 7 Tagen nach einer schriftlichen Mitteilung über eine Änderung bei den Unterauftragsverarbeitern widersprechen.
- 5.3 Die Beauftragung eines Unterauftragsverarbeiters hat keinerlei Auswirkung auf die Pflichten des Auftragsverarbeiters gegenüber dem Datenverantwortlichen. Zugriff auf die entsprechenden personenbezogenen Daten darf nur gewährt werden, wenn der Unterauftragsverarbeiter in allen wesentlichen Belangen die Pflichten dieser Datenverarbeitungsbedingungen einhält (oder die Einhaltung zusichert). Der Auftragsverarbeiter schließt mit den Unterauftragsverarbeitern einen schriftlichen Vertrag in Bezug auf die Unterauftragsverarbeitung von personenbezogenen Daten, der dem Datenschutzgesetz entspricht und, sofern praktikabel, im Wesentlichen auf denselben Bedingungen beruht wie diese Datenverarbeitungsbedingungen.
- 5.4 In Verzeichnis 3 sind die aktuellen Unterauftragsverarbeiter, der Ort der Verarbeitung und die Tätigkeitsbeschreibung genannt. Der Auftragsverarbeiter wird, sofern notwendig und innerhalb einer angemessenen Frist nach einer Änderung, dieses Verzeichnis während der Vertragslaufzeit aktualisieren.
- 5.5 Wenn der Auftragsverarbeiter seine Pflichten an einen Unterauftragsverarbeiter vergibt, dem der Datenverantwortliche (laut Vertrag oder bei Wechsel durch nachfolgende Zustimmung) zugestimmt hat, bleibt der Auftragsverarbeiter gemäß diesen Datenverarbeitungsbedingungen für die Handlungen seiner Unterauftragsverarbeiter haftbar.
- 5.6 Wenn der Auftragsverarbeiter seine Pflichten an einen Unterauftragsverarbeiter vergibt, kann der Datenverantwortliche (unter manchen Umständen) dem Unterauftragsverarbeiter Anweisungen in Bezug auf die Verarbeitung seiner personenbezogenen Daten durch den Unterauftragsverarbeiter erteilen. Unter diesen Umständen ist der Auftragsverarbeiter nicht für einen Verstoß gegen die Datenverarbeitungsbedingungen verantwortlich, der daraus folgt, dass der Unterauftragsverarbeiter auf Anweisungen des Datenverantwortlichen handelt, gleich ob diese dem Auftragsverarbeiter bekannt sind oder nicht.

6 SICHERHEIT UND DATENSCHUTZVERLETZUNGEN

- 6.1 Der Auftragsverarbeiter ergreift die technischen und organisatorischen Sicherheitsmaßnahmen, die dem Datenschutzgesetz und der bewährten Branchenpraxis entsprechen und notwendig sind, um die Verfügbarkeit, Vollständigkeit und Vertraulichkeit der personenbezogenen Daten zu gewährleisten und diese gegen Verlust oder unrechtmäßige Verarbeitung zu schützen. Um dem Auftragsverarbeiter die Einhaltung der hier genannten Bedingungen zu ermöglichen, teilt der Datenverantwortliche diesem alle für die Verarbeitung geltenden Zuverlässigkeitsanforderungen mit und übermittelt ihm im Falle verlangter Änderungen bei den Zuverlässigkeitsanforderungen für die Verarbeitung personenbezogener Daten alle notwendigen Informationen mit ausreichendem Vorlauf.
- 6.2 Die technischen und organisatorischen Sicherheitsmaßnahmen sind in Verzeichnis 2 beschrieben und entsprechen den allgemein anerkannten Sicherheitsstandards. Der Datenverantwortliche bestätigt, dass er die in Verzeichnis 2 dargelegten Vorkehrungen als ausreichend für die angemessene Sicherheit der personenbezogenen Daten entsprechend dem Datenschutzgesetz betrachtet.
- 6.3 Wenn dem Auftragsverarbeiter eine Datenschutzverletzung bekannt wird, meldet er diese dem Datenverantwortlichen unverzüglich.
- 6.4 Die in Klausel 6.3 genannte Meldung umfasst mindestens folgende Angaben:
- 6.4.1 die Art der Datenschutzverletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- 6.4.2 den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Person für weitere Informationen;
- 6.4.3 die wahrscheinlichen Folgen der Datenschutzverletzung;
- 6.4.4 die von dem Datenverantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

6.5 Der Auftragsverarbeiter unterstützt den Datenverantwortlichen, im Falle einer Datenschutzverletzung, bei der Erfüllung seiner gesetzlichen Informationspflichten gegenüber Aufsichtsbehörden und/oder den betroffenen Personen.

6.6 Der Auftragsverarbeiter informiert den Datenverantwortlichen unverzüglich, falls der Auftragsverarbeiter der Auffassung ist, dass eine durch den Datenverantwortlichen erteilte Verarbeitungsanweisung gegen die gesetzlichen Datenschutzbestimmungen verstößt.

7 ZUSÄTZLICHE GEHEIMHALTUNGSBESTIMMUNGEN

7.1 Der Auftragsverarbeiter bewahrt bezüglich der von ihm laut Vertrag verarbeiteten personenbezogenen Daten Verschwiegenheit und ergreift alle notwendigen Maßnahmen, um die Vertraulichkeit der personenbezogenen Daten zu gewährleisten. Der Auftragsverarbeiter verpflichtet auch seine Mitarbeiter und die von ihm beauftragte Person mit Zugriff auf die personenbezogenen Daten zur Verschwiegenheit.

7.2 Die Verschwiegenheit, auf die in diesem Absatz Bezug genommen wird, gilt nicht, sofern der Datenverantwortliche seine schriftliche Zustimmung zur Übermittlung der personenbezogenen Daten an einen Dritten gegeben hat oder eine gesetzliche Pflicht zur Übermittlung der personenbezogenen Daten an einen Dritten besteht.

8 DATENSCHUTZÜBERPRÜFUNGEN

8.1 Der Auftragsverarbeiter ermöglicht dem Datenverantwortlichen die Überprüfung der Einhaltung dieser Datenverarbeitungsbedingungen seitens des Auftragsverarbeiters oder erlaubt eine Überprüfung durch unabhängige Prüfer, auf Kosten des Datenverantwortlichen, ohne Verwendung vertraulicher Unternehmensinformationen des Auftragsverarbeiters und ohne Störung des Geschäftsbetriebs des Auftragsverarbeiters. Falls die Prüfung ergibt, dass der Auftragsverarbeiter seine Verpflichtungen laut diesen Datenverarbeitungsbedingungen nicht einhält, muss der Auftragsverarbeiter die durch die Prüfung identifizierten Versäumnisse so bald wie möglich beheben oder beseitigen. In diesem Fall trägt der Auftragsverarbeiter die vertretbaren und begründet nachweisbaren Kosten des Prüfers (die Zahlung erfolgt nur nach Vorlage einer gültigen Rechnung der Prüfer über die Kosten).

8.2 Eine Prüfung kann höchstens einmal pro Jahr stattfinden, es sei denn, es liegen ausreichende Beweise vor, dass der Auftragsverarbeiter seine Pflichten aus diesen Datenverarbeitungsbedingungen nicht einhält. Der Auftragsverarbeiter übermittelt dem Datenverantwortlichen alle für die Überprüfung vernünftigerweise erforderlichen Informationen.

8.3 Im Fall einer Untersuchung durch eine Datenschutzbehörde oder eine andere zuständige Behörde („Behörde“) arbeitet der Auftragsverarbeiter mit dieser in angemessener Weise zusammen und informiert den Datenverantwortlichen so schnell wie möglich.

8.4 Der Auftragsverarbeiter benennt eine Person als Ansprechpartner, der den Datenverantwortlichen bei der Erfüllung der sich aus der Verarbeitung ergebenden Offenlegungspflichten unterstützt, und teilt dem Datenverantwortlichen die Kontaktdaten des Ansprechpartners mit.

9 ÄNDERUNGEN

9.1 Sofern Änderungen bezüglich der Erfüllung einer Vertragspflicht wesentliche Folgen für die Verarbeitung personenbezogener Daten haben, teilt der Auftragsverarbeiter dem Datenverantwortlichen die beabsichtigten Änderungen der Datenverarbeitungsbedingungen mit Email oder über die Unit4 Communities mit. Der Datenverantwortliche übermittelt Einwände gegen die geänderten Bedingungen innerhalb 7 Werktagen nach Erhalt der Benachrichtigung durch Email oder über die Unit4 Communities und falls er keinen Einwand vorbringt, gelten die Änderungen als durch ihn akzeptiert.

9.2 Änderungen der Verzeichnisse zu diesen Datenverarbeitungsbedingungen können von Zeit zu Zeit durch den Auftragsverarbeiter erfolgen und werden auf der Unit4 Webpage veröffentlicht. Der Datenverantwortliche wird davon durch Email oder über die Unit4 Communities informiert wobei die Versionsnummer und das Datum des Inkrafttretens der aktualisierten Version angegeben werden. Wesentliche Änderungen der Verzeichnisse erfolgen nicht ohne Einwandmöglichkeit des Datenverantwortlichen.

10 GEGENSEITIGE SCHADLOSHALTUNG

10.1 Der Auftragsverarbeiter hält den Datenverantwortlichen schad- und klaglos von allen Geldbußen und / oder Strafzahlungen, die gegen diesen von oder im Namen einer Datenschutzbehörde verhängt werden, sowie von allen Schadensersatzforderungen im Zusammenhang mit Verlusten oder Schäden, die einer betroffenen Person entstanden sind, sofern nachgewiesen ist, dass diese Geldbußen und / oder Strafzahlungen oder Forderungen direkt auf ein Versäumnis des Auftragsverarbeiters bei der Verarbeitung personenbezogener Daten in Übereinstimmung mit dem Datenschutzgesetz oder anderer geltender Datenschutzgesetzgebung zurückzuführen sind.

Um von diesem Absatz 9.1 Gebrauch zu machen, muss der Datenverantwortliche:

- (i) den Auftragsverarbeiter unverzüglich schriftlich über das Vorliegen und den Gegenstand der Forderung einer betroffenen Person oder einer Untersuchung oder anderen Anordnung informieren, die Ursache einer Absicht oder Entscheidung der Datenschutzbehörde über das Verhängen einer Strafzahlung oder eines Strafbefehls sein könnte;
- (ii) gegenüber der Datenschutzbehörde oder der betroffenen Person, in Absprache mit dem Auftragsverarbeiter, tätig werden und mit dieser kommunizieren;
- (iii) Einspruch und / oder Rechtsmittel gegen verhängte Geldbußen einlegen, sofern dies begründet ist, und
- (iv) die Fallbearbeitung, einschließlich des Vergleichsschlusses, vollständig dem Auftragsverarbeiter überlassen. Zu diesem Zweck gewährt der Datenverantwortliche dem Auftragsverarbeiter die Vollmacht, Informationen und die Zusammenarbeit, die erforderlich sind, damit der Auftragsverarbeiter sich, bei Bedarf im Namen des Datenverantwortlichen, gegen diese Klagen verteidigen kann.

10.2 Der Datenverantwortliche hält den Auftragsverarbeiter schad- und klaglos von allen Geldbußen und / oder Strafzahlungen, die gegen diesen von oder im Namen der Datenschutzbehörde verhängt werden, sowie von allen Schadensersatzforderungen für Verluste oder Schäden, die einer betroffenen Person entstanden sind, sofern nachgewiesen ist, dass diese Geldbußen und / oder Strafzahlungen oder Forderungen darauf zurückzuführen sind, dass der Datenverantwortliche das Datenschutzgesetz oder eine andere geltende Datenschutzgesetzgebung nicht eingehalten hat.

Um von diesem Absatz 9.2 Gebrauch zu machen, muss der Auftragsverarbeiter:

- (i) den Datenverantwortlichen unverzüglich schriftlich über das Vorliegen und den Gegenstand einer Forderung einer betroffenen Person oder einer Untersuchung oder anderen Anordnung informieren, die Ursache einer Absicht oder Entscheidung der Datenschutzbehörde über das Verhängen einer Strafzahlung oder eines Strafbefehls sein könnte;
- (ii) gegenüber der Datenschutzbehörde oder der betroffenen Person, in Absprache mit dem Datenverantwortlichen, tätig werden und mit dieser kommunizieren;
- (iii) Einspruch und / oder Rechtsmittel gegen verhängte Geldbußen einlegen, sofern dies begründet ist, und
- (iv) die Fallbearbeitung, einschließlich des Vergleichsschlusses, vollständig dem Datenverantwortlichen überlassen. Zu diesem Zweck gewährt der Auftragsverarbeiter dem Datenverantwortlichen die Vollmacht, Informationen und die Zusammenarbeit, die erforderlich sind, damit der Datenverantwortliche sich, bei Bedarf im Namen des Auftragsverarbeiters, gegen diese Klagen verteidigen kann.

10.3 Soweit die Parteien die Haftung (gleich ob gesamtschuldnerische oder anderweitige Haftung) gegenüber Dritten, einschließlich betroffenen Personen, teilen oder eine Geldbuße durch die Datenschutzbehörde gesamtschuldnerisch auferlegt wird, sind die Parteien weiterhin verpflichtet, einander laut Absatz 9.1 und 9.2 schad- und klaglos zu halten für den Teil der Haftung gegenüber Dritten und für eine gesamtschuldnerische Geldbuße, der bzw. die anteilig ihrem jeweiligen Grad der Verantwortung für das Ereignis entspricht, wodurch die Haftung oder gesamtschuldnerische Geldbuße entstanden ist, wobei die Entscheidung eines Gerichts oder einer zuständigen Schiedsinstanz, die Datenschutzbehörde und der Beitrag einer Pflichtverletzung einer Partei gemäß diesen Datenverarbeitungsbedingungen zu berücksichtigen sind.

11 LAUFZEIT UND VERTRAGSENDE

11.1 Diese Datenverarbeitungsbedingungen treten mit dem Vertragsdatum in Kraft.

11.2 Bei Vertragsende muss der Auftragsverarbeiter die personenbezogenen Daten in der in Verzeichnis 1 dargelegten Weise zurückgeben oder auf Verlangen des Datenverantwortlichen entweder vernichten oder speichern Falls die personenbezogenen Daten in einem Computersystem oder einem anderen Format, das vernünftigerweise nicht an den Datenverantwortlichen übergeben werden kann, aufbewahrt oder gespeichert sind, vernichtet der Auftragsverarbeiter die personenbezogenen Daten auf seinen Systemen unverzüglich, es sei denn, die Parteien vereinbaren schriftlich etwas anderes.

Verzeichnisse:

Verzeichnis 1: Beschreibung der Verarbeitung personenbezogener Daten

Verzeichnis 2: Sicherheitsmaßnahmen

Verzeichnis 3: Unterauftragsverarbeiter

Verzeichnis 4: EU-Standardvertragsklauseln

VERZEICHNIS 1 - BESCHREIBUNG DER VERARBEITUNG PERSONENBEZOGENER DATEN

1. DIE PERSONENBEZOGENEN DATEN, DIE VERARBEITET WERDEN:

Produkt	Personenbezogene Daten, die unter Umständen verarbeitet werden, können Folgendes umfassen:	Diese können folgenden Personen gehören:
Unit4 ERP 7	Namen; Adressen; Vertragsdaten; Telefonnummern (einschließlich Mobiltelefon); E-Mail-Adresse(n); sonstige Kontaktdaten; Geburtsdatum; Alter; Geburtsort; Nationalität oder Staatsangehörigkeit; Wohnsitz; Geschäftssitz; gesprochene Sprache(n); Passnummer; Sozialversicherungsnummer oder Personalausweisnummer; Familienstand; Daten des Begünstigten von Leistungen; Geschlecht; Beschäftigungsdaten (einschließlich: Gehalt, Position; Tarifeinstufung; Gehaltsstufe; Kompetenzen und persönliche Bemerkungen); Steuerdaten; Leistungsdaten; Gewerkschaftsmitgliedschaft; nächster Angehöriger (Name; Adresse; Geburtsdatum; Telefonnummer; Notfallkontaktdaten); Beginn- und Enddaten der Beschäftigung; Bankkonto- oder Kreditkartendaten; Daten des Personaldienstleistungsunternehmens (Name; Registrierungsnummer und eingetragener Geschäftssitz); Direktorenpositionen; Umsatzsteuernummern; Dokumente (auf Papier oder elektronisch) mit den oben genannten Daten.	Gegenwärtige oder frühere Mitarbeiter; Auftragnehmer oder Unterauftragnehmer (jeder Art), Bevollmächtigte oder Geschäftsführer; und Bewerber oder zukünftige Mitarbeiter.
Unit4 Financials	Namen; Adressen; Vertragsdaten; Telefonnummern (einschließlich Mobiltelefon); E-Mail-Adresse(n); sonstige Kontaktdaten; Geburtsdatum; Alter; Geburtsort; Nationalität oder Staatsangehörigkeit; Wohnsitz; Geschäftssitz; gesprochene Sprache(n); Passnummer; Sozialversicherungsnummer oder Personalausweisnummer; Familienstand; Daten des Begünstigten von Leistungen; Geschlecht; Beschäftigungsdaten (einschließlich: Gehalt, Position; Tarifeinstufung; Gehaltsstufe; Kompetenzen und persönliche Bemerkungen); Steuerdaten; Leistungsdaten; Gewerkschaftsmitgliedschaft; nächster Angehöriger (Name; Adresse; Geburtsdatum; Telefonnummer; Notfallkontaktdaten); Beginn- und Enddaten der Beschäftigung; Bankkonto- oder Kreditkartendaten; Daten des Personaldienstleistungsunternehmens (Name; Registrierungsnummer und eingetragener Geschäftssitz); Direktorenpositionen; Umsatzsteuernummern; Dokumente (auf Papier oder elektronisch) mit den oben genannten Daten.	Gegenwärtige oder frühere Mitarbeiter; Auftragnehmer oder Unterauftragnehmer (jeder Art), Bevollmächtigte oder Geschäftsführer; und Bewerber oder zukünftige Mitarbeiter.
Unit4 Student Management	<p>Namen; Adressen; Vertragsdaten; Telefonnummern (einschließlich Mobiltelefon); E-Mail-Adresse(n); sonstige Kontaktdaten; Geburtsdatum; Alter; Geburtsort; Nationalität oder Staatsangehörigkeit; Wohnsitz; Geschäftssitz; gesprochene Sprache(n); Passnummer; Sozialversicherungsnummer oder Personalausweisnummer; Familienstand; Daten des Begünstigten von Leistungen; Geschlecht; Beschäftigungsdaten (einschließlich: Gehalt, Position; Tarifeinstufung; Gehaltsstufe; Kompetenzen und persönliche Bemerkungen); Steuerdaten; Leistungsdaten; Gewerkschaftsmitgliedschaft; nächster Angehöriger (Name; Adresse; Geburtsdatum; Telefonnummer; Notfallkontaktdaten); Beginn- und Enddaten der Beschäftigung; Bankkonto- oder Kreditkartendaten; Daten des Personaldienstleistungsunternehmens (Name; Registrierungsnummer und eingetragener Geschäftssitz); Direktorenpositionen; Umsatzsteuernummern; Dokumente (auf Papier oder elektronisch) mit den oben genannten Daten.</p> <p>Zusätzliche personenbezogene Daten für frühere und aktuelle Mitarbeiter: Personalart (z. B. Fakultätsangehöriger, Berater, Wohnheimleiter); Fachbereich; Anstellungsstatus; Beschäftigungsstatus; Arbeitspensum; Dienstgrad in der Fakultät; Veröffentlichungen, Arbeitsstatus-Nachverfolgung; Ausbildungsdaten und Qualifikationsdaten.</p> <p>Zusätzliche personenbezogene Daten für frühere und aktuelle Bewerber: Daten früherer Hochschulen; Zeugnisse und/oder (zusätzliche) Testergebnisse, körperlicher Gesundheitszustand; Zeugnisse früherer Arbeitgeber sowie Arbeitsplatzinformationen.</p> <p>Zusätzliche personenbezogene Daten für frühere und aktuelle Studierende: Studienlaufbahn einschließlich Ergebnissen und Zielen; Immatrikulationsangaben; Angaben zu Studienfortschritt (einschließlich Noten); Studienleistungen; Praktika oder Studienaufenthalte; Seminarplanungsdaten; Abrechnungs- und Bezahlhistorie; bevorzugte Unterkunft und Historie; Finanzförderungsdaten; Gesundheitsdaten (einschließlich Impfungen, Allergien, chronische Krankheiten); Versicherungsdaten und Gesundheitsdokumentation.</p>	<ul style="list-style-type: none"> • Gegenwärtige oder frühere Mitarbeiter (einschließlich aller Fakultätsangehörigen oder Personal); • Auftragnehmer oder Unterauftragnehmer (jeder Art), Bevollmächtigte oder Geschäftsführer; • Bewerber oder zukünftige Mitarbeiter und • Gegenwärtige, frühere und zukünftige Studierende.
Unit4 FP&A	Namen; Adressen; Telefonnummern (einschließlich Mobiltelefon); E-Mail-Adresse(n); sonstige Kontaktdaten. Andere personenbezogene Daten müssen <u>nicht</u> gespeichert oder verarbeitet werden, damit die Zielsetzungen des Produkts (wie nachstehend genannt) erreicht werden, andere personenbezogene Daten können durch das Produkt jedoch gespeichert oder verarbeitet werden, wenn dieses entsprechend konfiguriert ist (z. B. Gehaltsdaten) oder die Daten durch den Kunden in das Produkt eingegeben werden.	Gegenwärtige oder frühere Mitarbeiter; Unterauftragnehmer (jeder Art), Bevollmächtigte oder Geschäftsführer.
Unit4 Assistance PSA Suite	Namen; Adressen; Telefonnummern (einschließlich Mobiltelefon); E-Mail-Adresse(n); sonstige Kontaktdaten. Andere personenbezogene Daten müssen <u>nicht</u> gespeichert oder verarbeitet werden, damit die Zielsetzungen des Produkts (wie nachstehend genannt) erreicht werden, andere personenbezogene Daten können durch das Produkt jedoch gespeichert oder verarbeitet werden, wenn dieses entsprechend konfiguriert ist oder die Daten durch den Kunden in das Produkt eingegeben werden.	Gegenwärtige oder frühere Mitarbeiter; Unterauftragnehmer (jeder Art), Bevollmächtigte oder Geschäftsführer; Jedes andere Mitglied des Projektteams (auch wenn dies kein Mitarbeiter ist) Bewerber oder zukünftige Mitarbeiter. Kundenkontakte und Lieferantenkontakte des Kunden

Unit4 Talent Management	Namen; Adressen; Vertragsdaten; Telefonnummern (einschließlich Mobiltelefon); E-Mail-Adresse(n); sonstige Kontaktdaten (postalische Anschrift und Land); Geburtsdatum; Alter; Geburtsort; Stellenbezeichnung; Abteilung. Durch Nutzung des Lernmoduls (Learn): Kursanmeldungen; Sitzungsanmeldungen, Quizergebnisse und -prüfungen; Videoaktivitätsdaten, Folienaktivitätsdaten, Textaktivitätsdaten; Abzeichen; Zertifizierungen. Durch Nutzung des Leistungsmoduls (Perform): Anmeldezeiten, OKR-Daten, Feedback und Lob. Durch Nutzung des Aktivitätsmoduls (Engage): Antworten und Feedback zu Aktivitätsfragen.	Gegenwärtige oder frühere Mitarbeiter; Gegenwärtige oder frühere Bewerber; Auftragnehmer oder Unterauftragnehmer (jeder Art), Bevollmächtigte oder Geschäftsführer; und Bewerber oder zukünftige Mitarbeiter.
People-Plattform-Services („PPS“) (allgemein), einschließlich IDS und Wanda (sowie alle Supportleistungen)	<p>Da es sich bei den PPS um Services handelt, die mit den anderen Produkten oder Services von Unit4 zusammenarbeiten und Schnittstellen dazu bilden, können mit den PPS sämtliche Arten von personenbezogenen Daten verarbeitet werden, die in dieser Tabelle im Zusammenhang mit den genannten Produkten und Services aufgeführt sind.</p> <p>Zusätzlich verarbeitet Wanda gegebenenfalls: Unit4Id (womit die Nutzer von IDS identifiziert werden); alle personenbezogenen Daten oder Informationen, die von dem Nutzer in eine Anwendung eingegeben werden, mit der Wanda gegebenenfalls verbunden ist (diese Daten werden verarbeitet oder gespeichert, wenn der Nutzer diese nicht löschen lässt); sämtliche weiteren Konversations- und Dialogdaten; einer einzelnen Person zuzuordnende Metadaten; sowie Application Insights Logs (ein Microsoft-Service, der zur Leistungsdiagnose verwendet wird).</p>	<p>Alle Kategorien einzelner Personen, die in dieser Tabelle aufgeführt sind.</p> <p>Je nach Anwendung oder Service, mit dem Wanda verbunden ist, können die PPS unter Umständen personenbezogene Daten aller lebenden Personen verarbeiten, die der Nutzer eingibt.</p>

2. ART UND ZIELSETZUNG(EN) DER VERARBEITUNG:

Grundsätzlich orientiert sich die Art der Verarbeitung durch den Auftragsverarbeiter nur daran, was für dessen Einhaltung seiner Pflichten und Ausübung seiner Rechte laut Vertrag notwendig ist, einschließlich (im Zusammenhang mit personenbezogenen Daten) Erhebung, Erfassung, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übertragung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung. Ziel oder Zweck der Verarbeitung ist die Erfüllung der Pflichten des Auftragsverarbeiters und die Ausübung seiner Rechte laut diesen Datenverarbeitungsbedingungen, einschließlich der Erfüllung von Funktionen, die seitens des Datenverantwortlichen vorausgesetzt oder verlangt werden, damit dieser seine gesetzlichen und/oder vertraglichen Pflichten erfüllen kann. In Bezug auf und in Abhängigkeit von dem Produkt oder Service umfasst die Verarbeitung Folgendes:

Produkt	Art und Zielsetzung der Verarbeitung
Unit4 ERP 7	<p>Personenbezogene Daten werden in Unit4 ERP 7 eingegeben, um dem Kunden die Organisation und Steuerung von Prozessen im Zusammenhang mit der operativen Funktionsweise und dem Betriebsmanagement und/oder interne Geschäftsverwaltungsprozesse zu ermöglichen. Die Prozesse können Folgendes umfassen:</p> <ul style="list-style-type: none"> • Reiseanträge; • Spesenantragsverarbeitung; • Stundenzettelverarbeitung; • Abwesenheitsmanagement; • Prozesse im Zusammenhang mit Personalwesen und Gehaltsabrechnung: <ul style="list-style-type: none"> ○ Gehaltsabrechnung; ○ Kursanmeldung; ○ Kompetenzmanagement; ○ Beurteilungen; ○ Gehaltsüberprüfung; ○ Bewerberregistrierung; • Zahlungsverarbeitung; • Abrechnung; • Bestellanforderungen; • Personal-/Projektplanung. <p>Die Verarbeitung umfasst:</p> <p>Produkt (Softwarelösung)</p> <ul style="list-style-type: none"> • Unit4 ERP 7 ausführender programmierbarer Softwarecode, damit die (oben) genannten Aktivitäten stattfinden können. Dazu kann auch die Datenübertragung an oder von Drittanbieterlösungen, die nicht von dem Auftragsverarbeiter kontrolliert werden, durch Integrationen gehören. <p>Services</p> <ul style="list-style-type: none"> • Übertragung und Speicherung von personenbezogenen Daten zur Bereitstellung weiterer Unit4 Cloud Services, wie näher in der Unit4 Cloud Services-Beschreibung aufgeführt, oder People-Plattform-Services (wie in der entsprechenden People-Plattform-Service-Leistungsbeschreibung aufgeführt). • Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 ERP 7 und zur Unterstützung des Kunden beim Betrieb der Lösung, wie in den Unit4-Supportbedingungen näher geregelt. • Zugriff auf die personenbezogenen Daten zur Bereitstellung der Konfiguration und/oder Anpassung und/oder Datenmigration (z. B. von vorhandenen Systemen) und/oder anderer professioneller Dienstleistungen, wie vom Kunden erworben.
Unit4 Financials	<p>Personenbezogene Daten werden in Unit4 Financials eingegeben, um dem Kunden die Organisation und Steuerung von Prozessen im Zusammenhang mit der operativen Funktionsweise und dem Betriebsmanagement und/oder interne Geschäftsverwaltungsprozesse zu ermöglichen. Die Prozesse können Folgendes umfassen:</p> <ul style="list-style-type: none"> • Kunden-/Lieferanten-/Mitarbeiterregistrierung;

	<ul style="list-style-type: none"> • Zahlungsverarbeitung; • Abrechnung; • Spesenantragsverarbeitung; • Reiseanträge; • Bestellanforderungen und Aufträge; • Personal-/Projektplanung; • Prozesse im Zusammenhang mit Personalwesen und Gehaltsabrechnung: <ul style="list-style-type: none"> ○ Gehaltsabrechnung; ○ Stundenzettelverarbeitung; ○ Abwesenheitsmanagement ○ Kursanmeldung; ○ Kompetenzmanagement; ○ Beurteilungen; ○ Gehaltsüberprüfung; ○ Bewerberregistrierung; <p>Die Verarbeitung umfasst:</p> <p>Produkt (Softwarelösung)</p> <ul style="list-style-type: none"> • Unit4 Financials ausführender programmierbarer Softwarecode, damit die (oben näher) genannten Aktivitäten stattfinden können. Dazu kann auch die Datenübertragung an oder von Drittanbieterlösungen, die nicht von dem Auftragsverarbeiter kontrolliert werden, durch Integrationen gehören. <p>Services</p> <ul style="list-style-type: none"> • Übertragung und Speicherung von personenbezogenen Daten zur Bereitstellung weiterer Unit4 Global Services, wie näher in der Unit4 Cloud Services-Beschreibung aufgeführt, oder People-Plattform-Services (wie in der entsprechenden People-Plattform-Service-Leistungsbeschreibung aufgeführt). • Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 Financials-Produkt und zur Unterstützung des Kunden beim Betrieb der Lösung, wie in den Unit4-Supportbedingungen näher geregelt. • Zugriff auf die personenbezogenen Daten zur Bereitstellung der Konfiguration und/oder Anpassung und/oder Datenmigration (z. B. von vorhandenen Systemen) und/oder anderer professioneller Dienstleistungen, wie vom Kunden erworben.
Unit4 Student Management	<p>Personenbezogene Daten werden in Unit4 Student Management eingegeben, um dem Kunden die Organisation und Steuerung von Prozessen im Zusammenhang mit der operativen Funktionsweise und dem Betriebsmanagement und/oder interne Geschäftsverwaltungsprozesse zu ermöglichen. Die Prozesse können Folgendes umfassen:</p> <ul style="list-style-type: none"> • Anwerbung zukünftiger Studierender, • Beantwortung von Informationsanfragen • Antragsverarbeitung • Bearbeitung des Studienverlaufs eines Studierenden, einschließlich Immatrikulation, Kursplanung, Studienfortschritt, Beratung, Studentenwohnheime und andere Einrichtungen, Abschluss • Planung und Einteilung der Fakultätsmitarbeiter <p>Die Verarbeitung umfasst:</p> <p>Produkt (Softwarelösung)</p> <ul style="list-style-type: none"> • Unit4 Student Management ausführender programmierbarer Softwarecode, damit die (oben) genannten Aktivitäten stattfinden können. Dazu kann auch die Datenübertragung an oder von Drittanbieterlösungen, die nicht von dem Auftragsverarbeiter kontrolliert werden, durch Integrationen gehören. <p>Services</p> <ul style="list-style-type: none"> • Übertragung und Speicherung von personenbezogenen Daten zur Bereitstellung weiterer Unit4 Global Services, wie näher in der Unit4 Cloud Services-Beschreibung aufgeführt, oder People-Plattform-Services (wie in der entsprechenden People-Plattform-Service-Leistungsbeschreibung aufgeführt). • Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 Student Management-Produkt und zur Unterstützung des Kunden beim Betrieb der Lösung, wie in den Unit4-Supportbedingungen näher geregelt. • Zugriff auf die personenbezogenen Daten zur Bereitstellung der Konfiguration und/oder Anpassung und/oder Datenmigration (z. B. von vorhandenen Systemen) und/oder anderer professioneller Dienstleistungen, wie vom Kunden erworben.
Unit4 FP&A	<p>Personenbezogene Daten werden in Unit4 FP&A eingegeben, um dem Kunden die Organisation und Steuerung von Prozessen im Zusammenhang mit der operativen Funktionsweise und dem Betriebsmanagement und/oder interne Geschäftsverwaltungsprozesse zu ermöglichen. Die Prozesse können Folgendes umfassen:</p> <ul style="list-style-type: none"> • Finanzplan; • Finanz- und sonstige Berichterstattung; • Berichtsverteiler; • Zustimmungsverarbeitung; • Personal-/Projektplanung. <p>Die Verarbeitung umfasst:</p> <p>Produkt (Softwarelösung)</p> <ul style="list-style-type: none"> • Unit4 prevero ausführender programmierbarer Softwarecode, damit die (oben) genannten Aktivitäten stattfinden können. Dazu kann auch die Datenübertragung an oder von Drittanbieterlösungen, die nicht von dem Auftragsverarbeiter kontrolliert werden, durch Integrationen gehören. <p>Services</p>

	<ul style="list-style-type: none"> • Übertragung und Speicherung von personenbezogenen Daten zur Bereitstellung weiterer Unit4 Cloud Services, wie näher in der Unit4 Cloud Services-Beschreibung aufgeführt, oder People-Plattform-Services (wie in der entsprechenden People-Plattform-Service-Leistungsbeschreibung aufgeführt). • Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 FP&A Produkt und zur Unterstützung des Kunden beim Betrieb der Lösung, wie in den Unit4-Supportbedingungen näher geregelt. • Zugriff auf die personenbezogenen Daten zur Bereitstellung der Konfiguration und/oder Anpassung und/oder Datenmigration (z. B. von vorhandenen Systemen) und/oder anderer professioneller Dienstleistungen, wie vom Kunden erworben.
Unit4 Talent Management	<p>Personenbezogene Daten werden in Unit4 Talent Management eingegeben, um dem Kunden die Organisation und Steuerung von Prozessen im Zusammenhang mit der operativen Funktionsweise und dem Betriebsmanagement und/oder interne Geschäftsverwaltungsprozesse zu ermöglichen. Die Prozesse können Folgendes umfassen:</p> <ul style="list-style-type: none"> • Humankapital-Management; • Mitarbeiterleistungs-Management; • Talententwicklung; • Kandidatenbewertung; • Weiterbildung; • Feedback und Lob; sowie • Personalanalyse und -motivation. <p>Die Verarbeitung umfasst:</p> <p>Produkt (Softwarelösung)</p> <ul style="list-style-type: none"> • Unit4 Talent Management ausführender programmierbarer Softwarecode, damit die (oben näher) genannten Aktivitäten stattfinden können. Dazu kann auch die Datenübertragung an oder von Drittanbieterlösungen, die nicht von dem Auftragsverarbeiter kontrolliert werden, durch Integrationen gehören. <p>Services</p> <ul style="list-style-type: none"> • Übertragung und Speicherung von personenbezogenen Daten zur Bereitstellung weiterer Unit4 Talent Management Cloud Services, wie näher in der Unit4 Talent Management Cloud Services-Beschreibung aufgeführt. • Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 Talent Management -Produkt und zur Unterstützung des Kunden beim Betrieb der Lösung, wie in den Unit4-Supportbedingungen näher geregelt • Zugriff auf die personenbezogenen Daten zur Bereitstellung der Konfiguration und/oder Anpassung und/oder Datenmigration (z. B. von vorhandenen Systemen) und/oder anderer professioneller Dienstleistungen, wie vom Kunden erworben.
Unit4 Assistance PSA Suite	<p>Personenbezogene Daten werden in Unit4 Assistance PSA Suite eingegeben, um dem Kunden die Organisation und Steuerung von Prozessen im Zusammenhang mit der operativen Funktionsweise und dem Betriebsmanagement und/oder interne Geschäftsverwaltungsprozesse zu ermöglichen. Die Prozesse können Folgendes umfassen:</p> <ul style="list-style-type: none"> • Automatisierung eines professionellen Dienstleistungsunternehmens, einschließlich Finanz- und Personalressourcenmanagement; • tägliches Zeit- und Projektmanagement; • Zeit- und Spesenbuchung mit Belegen; • Überleitung von Gelegenheiten in Projekte, Budget und Stundenprognose sowie Projekt- und Ressourcenplanung; • Zeit- und Aufwendungsverfolgung und Rechnungsstellung; • Integration von Projekten in andere Anwendungen • Buchhaltung zur Unterstützung der Integration von Finanzdaten in andere Lösungen. <p>Die Verarbeitung umfasst:</p> <p>Produkt (Softwarelösung)</p> <ul style="list-style-type: none"> • Unit4 Assistance PSA Suite ausführender programmierbarer Softwarecode, damit die (oben näher) genannten Aktivitäten stattfinden können. Dazu kann auch die Datenübertragung an oder von Drittanbieterlösungen, die nicht von dem Auftragsverarbeiter kontrolliert werden, durch Integrationen gehören. <p>Services</p> <ul style="list-style-type: none"> • Übertragung und Speicherung von personenbezogenen Daten zur Bereitstellung weiterer Unit4 Global Cloud Services, wie näher in der Unit4 Cloud Services-Beschreibung aufgeführt, oder People-Plattform-Services (wie in der entsprechenden People-Plattform-Service-Leistungsbeschreibung aufgeführt). • Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 Assistance PSA Suite-Produkt und zur Unterstützung des Kunden beim Betrieb der Lösung, wie in den Unit4-Supportbedingungen näher geregelt. • Zugriff auf die personenbezogenen Daten zur Bereitstellung der Konfiguration und/oder Anpassung und/oder Datenmigration (z. B. von vorhandenen Systemen) und/oder anderer professioneller Dienstleistungen, wie vom Kunden erworben.
People-Plattform-Services („PPS“) (allgemein), einschließlich IDS und Wanda (sowie alle Supportleistungen)	<p>Die Daten werden durch die PPS verarbeitet, um die genannten Zwecke der Leistungen zu ermöglichen, wie in der entsprechenden PPS - Leistungsbeschreibung unter www.unit4.com/terms dargelegt.</p> <p>Außerdem werden personenbezogene Daten mit einer Drittanbieter-Software nach Wahl (z. B. Slack Integration, Facebook Messenger oder andere Microsoft-Anwendungen (u. a. Microsoft Teams)) in Wanda eingegeben. Je nach dem vom Kunden verwendeten Unit4-Produkt oder -Service kann Wanda bei der Erledigung administrativer Aufgaben durch die Kundenmitarbeiter helfen.</p> <p>Die Aufgaben können Folgendes umfassen:</p> <ul style="list-style-type: none"> • Stundenzetteleingaben • Speseneingaben • Reiseanträge • Gehaltsabrechnungsanfragen • Abwesenheitseingaben • Saldoabfragen

	<ul style="list-style-type: none"> • Bestellanforderungen. <p>Die Verarbeitung umfasst:</p> <p>Produkt (Softwarelösung)</p> <ul style="list-style-type: none"> • Wanda ausführender programmierbarer Softwarecode, damit die (oben) genannten Aktivitäten stattfinden können. Dazu kann auch die Datenübertragung an oder von Drittanbieterlösungen, die nicht von dem Auftragsverarbeiter kontrolliert werden, durch Integrationen gehören. • Services • Übertragung und Speicherung von personenbezogenen Daten zur Bereitstellung weiterer Unit4 Global Services, wie näher in der Unit4 Cloud Services-Beschreibung aufgeführt, oder People-Plattform-Services (wie in der entsprechenden People-Plattform-Service-Leistungsbeschreibung aufgeführt). • Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 PPS-Produkt und zur Unterstützung des Kunden beim Betrieb der Lösung, wie in den Unit4-Supportbedingungen näher geregelt. • Zugriff auf die personenbezogenen Daten zur Bereitstellung der Konfiguration und/oder Anpassung und/oder Datenmigration (z. B. von vorhandenen Systemen) und/oder anderer professioneller Dienstleistungen, wie vom Kunden erworben. • Zugriff auf personenbezogene Daten zur Produktverbesserung über KI-Maschinenlernen oder Datenanalyse.
--	--

3. BESCHREIBUNG DER VERARBEITUNG UND MITTEL:

Der Auftragsverarbeiter verarbeitet die vorgenannten personenbezogenen Daten im Zusammenhang mit den folgenden Aktivitäten (die nachstehend genannten Aktivitäten dienen lediglich als Beispiel):

Art der Verarbeitung	Beschreibung	Mittel und Ressourcen
Unit4 SaaS	Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Zusammenhang mit den im Vertrag beschriebenen Aktivitäten und insbesondere der Unit4 Global Services-.	<p><u>Personal</u></p> <p>Das operative Team der Unit4 Cloud Services verfügt über Personal in Polen, Schweden, Norwegen, dem Vereinigten Königreich, den USA, Kanada, Malaysia und Singapur. Diese Mitarbeiter des Auftragsverarbeiters verarbeiten die Unit4 Global Services.</p> <p><u>Anlagen und Infrastruktur</u></p> <p>Unit4 nutzt Hosting-Infrastrukturservices von Drittanbietern, um die Unit4 SaaS bereitzustellen, und setzt andere Software-Systeme für Betrieb und Verwaltung ein. Siehe Verzeichnis 3.</p>
U4 Talent Management	Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Zusammenhang mit den im Vertrag beschriebenen Aktivitäten und insbesondere der Unit4 Talent Management Cloud Service-Beschreibung und den lösungsspezifischen Leistungsbeschreibungen.	<p><u>Personal</u></p> <p>Das operative Team der Unit4 Talent Management Cloud Services verfügt über Personal vorwiegend in Belgien und einigen anderen EWR-Ländern. Diese Mitarbeiter des Auftragsverarbeiters verarbeiten die Unit4 Talent Management SaaS Services.</p> <p><u>Anlagen und Infrastruktur</u></p> <p>Unit4 nutzt Hosting-Infrastrukturservices von Drittanbietern, um den Unit4 Talent Management SaaS Service bereitzustellen, und setzt andere Software-Systeme für Betrieb und Verwaltung ein. Siehe Verzeichnis 3.</p>
Supportleistungen	Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Zusammenhang mit den im Vertrag beschriebenen Aktivitäten und insbesondere den Unit4-Supportbedingungen.	<p><u>Personal</u></p> <p>Das Unit4-Supportteam verfügt über Personal an diesen Standorten: Vereinigtes Königreich, Polen, Portugal, Norwegen, Deutschland, Schweden, Deutschland, USA, Kanada (und anderen Standorten, wie zur Unterstützung der geschäftlichen Anforderungen von Unit4 erforderlich). Diese Mitarbeiter des Auftragsverarbeiters stellen die Unit4-Supportleistungen bereit (aufgeführt in den Unit4-Supportbedingungen in Abschnitt B der SLA).</p> <p><u>Anlagen und Infrastruktur</u></p> <p>Unit4 nutzt andere Software-Systeme für den Betrieb, die Erbringung und Verwaltung dieser Leistungen.</p>
Professionelle Dienstleistungen und/oder Beratung	Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Zusammenhang mit den Aktivitäten, die im Vertrag und insbesondere in detaillierteren Projektdokumentationen oder den nach Projektbeginn zwischen den Parteien vereinbarten Leistungsbeschreibungen festgehalten sind.	<p><u>Personal</u></p> <p>Das Unit4 Professional Services-Team verfügt über Personal an allen Standorten, an denen sich eine Konzerngesellschaft von Unit4 befindet, einschließlich dem Vereinigten Königreich, Irland, Polen, Portugal, Norwegen, Spanien, Frankreich, Deutschland, Schweden, den USA, Kanada, Singapur/Malaysia (und anderen Standorten, wie zur Unterstützung der geschäftlichen Anforderungen von Unit4 erforderlich). Diese Mitarbeiter des Auftragsverarbeiters stellen die Unit4 Professional Services bereit.</p> <p><u>Anlagen und Infrastruktur</u></p> <p>Unit4 nutzt andere Software-Systeme für den Betrieb, die Erbringung und Verwaltung dieser Leistungen.</p>
Unit4 Professional Services (falls an einen Leistungserbringerpartner als Unterauftrag vergeben)	Der Auftragsverarbeiter und seine Unterauftragsverarbeiter verarbeiten die genannten personenbezogenen Daten im Zusammenhang mit den Aktivitäten, die im Vertrag und (gegebenenfalls) in der als Bestandteil des Vertrags bereitgestellten Vertrags- und Servicedokumentation des	Siehe Verzeichnis 3 bzw. das einschlägige Angebotsformular.

	<p>Dritten festgelegt sind. Für weitere Informationen siehe Verzeichnis 3.</p> <p>Der Auftragsverarbeiter schließt mit dem bzw. den Unterauftragsverarbeiter(n) einen schriftlichen Vertrag, der den relevanten Gesetzen und Vorschriften sowie diesen Datenverarbeitungsbedingungen entspricht.</p> <p>Der Datenverantwortliche hat durch den Vertragsschluss dem Auftragsverarbeiter außerdem die Zustimmung erteilt, den bzw. die in Verzeichnis 3 aufgeführten Unterauftragsverarbeiter zu beauftragen.</p>	
Drittanbieter-Produkte und -Leistungen	Der Auftragsverarbeiter und seine Unterauftragsverarbeiter verarbeiten die genannten personenbezogenen Daten im Zusammenhang mit den Aktivitäten, die im Vertrag und (gegebenenfalls) in der als Bestandteil des Vertrags bereitgestellten Vertrags- und Servicedokumentation des Drittanbieters festgelegt sind.	Siehe Verzeichnis 3 bzw. das einschlägige Angebotsformular und alle anderen Bestimmungen, die in weiteren Verzeichnissen oder Anlagen zu diesen Datenverarbeitungsbedingungen enthalten sind, sofern dies durch den Drittanbieter oder gesetzlich vorgeschrieben ist.
People-Plattform-Services („PPS“) (allgemein), einschließlich IDS und Wanda (sowie alle Supportleistungen)	Neben Unit4 SaaS verarbeitet die PPS (gegebenenfalls) personenbezogene Daten in Verbindung mit einer Datenschutzerklärung, die dem Endnutzer vorgelegt wird, um, im Falle der Verarbeitung personenbezogener Daten, sein Einverständnis zu erbitten.	<p><u>Personal</u></p> <p>Das operative Team der Unit4 Cloud Services, das die PPS betreibt, verfügt über Personal in Polen, Schweden, Norwegen, dem Vereinigten Königreich, den USA, Kanada, Malaysia und Singapur. Diese Mitarbeiter des Auftragsverarbeiters verarbeiten Unit4 SaaS.</p> <p><u>Anlagen und Infrastruktur</u></p> <p>Unit4 nutzt eigene und (geteilte) Infrastrukturservices von Drittanbietern, um die Unit4 People-Plattform-Services anzubieten. Dazu gehören auch Drittanbietersysteme (d. h. Anwendungen zur Zusammenarbeit), über die Unit4 keine Kontrolle hat. Die PPS einschließlich Wanda nutzen eine Reihe von Microsoft-Produkten und -Services, und zwar wie folgt:</p> <ul style="list-style-type: none"> • Kognitive Leistungen: <ul style="list-style-type: none"> ○ LUIS Cognitive Service - <i>Sprachverstehen</i>. ○ Text Translator API – <i>Textübersetzung</i> ○ QnA Maker Cognitive Service – <i>Frage- und Antwortservice</i> • Bot Framework Connectors – <i>sorgt für die Verbindung von Wanda zu den unterstützten Social-Media-Kanälen.</i> • Traffic Manager – <i>verwendet für Disaster Recovery und Ausfallsicherung bei gestörter Primärregion</i> • Web Apps / Web Jobs – <i>hostet Web-APIs und langlaufende webbasierte Prozesse</i> • Service Bus – <i>stellt interne Kommunikation im Wanda-Ökosystem bereit</i> • Speicherkonten – <i>verwendet zur Speicherung des Konversationsstatus und der Nutzereinstellungen</i> • Cosmos DB – <i>stellt Speicherung bereit</i> • Key Vault – <i>speichert vertrauliche Daten, die zur Kommunikation mit Microsoft-Services und für interne Services verwendet werden</i> • Redis Cache – <i>bietet Caching-Funktionen</i> • Application Insights – <i>Systemüberwachung, einschließlich Telemetrie und Protokollierung</i> • SQL-Server – <i>bietet Speicherung</i> • Kubernetes – <i>Open-Source-Container</i> <p>Weitere Informationen und nähere Angaben zu diesen Microsoft-Produkten und -Services sind hier zu finden: https://azure.microsoft.com/en-us/services/.</p>

4. AUFBEWAHRUNGSFRIST

Der Auftragsverarbeiter bewahrt die personenbezogenen Daten während der Laufzeit des Vertrags auf.

Nach der vereinbarten Aufbewahrungsfrist gibt der Auftragsverarbeiter die personenbezogenen Daten in einem durch den Auftragsverarbeiter bestimmten migrationsfähigen Format an den Datenverantwortlichen zurück **oder** vernichtet die personenbezogenen Daten nach der erstmaligen Aufforderung durch den Datenverantwortlichen ohne Zurückbehaltung einer Kopie.

5. INFORMATIONEN BEZÜGLICH LAND (ODER ORT) DER VERARBEITUNG PERSONENBEZOGENER DATEN

Produkt - Vor Ort	Daten sind auf den Servern des Datenverantwortlichen in dessen Hauptniederlassung oder eingetragenem Geschäftssitz, wie Unit4 jeweils mitgeteilt werden kann, gespeichert.			
Produkt - Unit4 SaaS	Unit4 Cloud wird in mehreren Rechenzentren betrieben, darunter eine weltweite Präsenz in Microsoft Azure. Unit4 verwendet für die Bereitstellung des Kunden den logischerweise sinnvollsten Standort in Abhängigkeit von dem (im Auftragsformular genannten) Standort des Kunden. Alle Kundendaten werden nur in der ausgewählten geopolitischen Zone gespeichert und ohne ausdrückliche Zustimmung des Kunden nicht nach außerhalb bewegt.			
	CLOUD-MODELL	GEOPOLITISCHE ZONE	STANDORT DES RECHENZENTRUMS	ANLAGE ODER PARTNERSCHAFT

	SAAS CLOUD	EU	DUBLIN / AMSTERDAM	MICROSOFT AZURE
	SAAS CLOUD	USA	MEHRERE STANDORTE	MICROSOFT AZURE
	SAAS CLOUD	KANADA	TORONTO / QUEBEC CITY	MICROSOFT AZURE
	SAAS CLOUD	VEREINIGTES KÖNIGREICH	LONDON / CARDIFF	MICROSOFT AZURE
	SAAS CLOUD	ASIEN	SINGAPUR / HONGKONG	MICROSOFT AZURE
	SAAS CLOUD	AUSTRALIEN	VICTORIA / NEW SOUTH WALES	MICROSOFT AZURE
	SAAS CLOUD	NORWAY	OSLO / STAVANGER	MICROSOFT AZURE
	SAAS CLOUD	SWEDEN (NORDICS)	SÄTRA AND SOLLENTUNA	CONPATO
Produkt – Talent Management SaaS	Talent Manager wird im Amazon Web Services (AWS)-Rechenzentrum in Frankfurt betrieben. Alle Kundendaten werden, außer für den Austausch mit ausgewählten Unterauftragsverarbeitern in Verzeichnis 3, nur in der ausgewählten geopolitischen Zone gespeichert und ohne ausdrückliche Zustimmung des Kunden nicht nach außerhalb bewegt.			
Unit4 Support – Standardsupport und andere Standard-Supportleistungen	Unit4 Support nutzt Drittsoftware (z.B. Salesforce / Service Now) zur Registrierung und Verarbeitung von Fällen. Auf diese Fälle können alle Unit4-Mitarbeiter mit Zugang zur Drittsoftware zugreifen, wie Support-Techniker, Cloud-Techniker, Berater für professionelle Dienstleistungen und das Service-Management. Der Zugriff wird durch interne Verwaltungs- und Betriebsprozesse kontrolliert, damit sichergestellt ist, dass keine Berater oder Techniker an Standorten, die keinen Zugang zu bestimmten Kundendaten haben dürfen, auf personenbezogene Daten zugreifen.			
	Standort des Kunden		Support wird vorrangig aus folgenden Standorten bereitgestellt:	
	Vereinigtes Königreich und Irland		Vereinigtes Königreich, Irland, Portugal und Polen.	
	Schweden, Norwegen, Dänemark, Finnland und Island		Polen, Portugal, Norwegen und Schweden.	
	USA & Kanada		Polen, Portugal, USA und Kanada.	
	Rest-Europa		Polen, Portugal und Deutschland.	
	APAC		Polen, Portugal und Singapur / Malaysia.	
Unit4 Support – Rund-um-die-Uhr-Support (Kunden mit erweitertem und Premium-Support)	Nach der „Follow the sun“-Methode kann der Rund-um-die-Uhr-Support für Kundenfälle von jedem der oben aufgeführten Support-Standorte aus erfolgen.			
Unit4 Support – Nur-EU-Support	Wird der Nur-EU-Support gewählt, erfolgt der Standard-Support nur innerhalb der oben aufgeführten EU-Standorte (während der Geschäftszeiten).			
People-Plattform-Services („PPS“) (allgemein), einschließlich IDS und Wanda (sowie alle Supportleistungen)	PPS sind Cloud-Services, die geteilte Infrastruktur- und Drittanbieter-Services nutzen, die unter Umständen keine geopolitische Trennung nach Zonen bieten. Im nachstehenden Überblick sind die PPS und das Land (oder der Ort) der Verarbeitung personenbezogener Daten, in dem dieser Service verwendet wird, aufgeführt.			
	Service	Geopolitische Zone	Ort, an dem der Service die Daten verarbeitet oder speichert	Support wird vorrangig aus folgenden Standorten bereitgestellt:
	Wanda	Alle	Vorwiegend innerhalb der EU, aber unter Umständen auch andernorts.	Irland, Vereinigte Staaten und sonstiger globaler Support, sofern erforderlich
	IDS	Anhängig vom Cloud-Einsatz	Wie oben für Unit4 SaaS	Wie oben für Unit4 SaaS
Unit4 Professional Services und Unit4-Kundenerfolgsfunktion	Thema	Professionelle Dienstleistungen und Kundenerfolg werden bereitgestellt durch:		
	Implementierung und andere Projektservices	In dem Gebiet oder an dem Kundenstandort des eingetragenen Geschäftssitzes/der Hauptniederlassung (wie zutreffend) und/oder in Portugal, je nachdem, was zwischen den Parteien in der Projektdokumentation bzw. einer Leistungsbeschreibung vereinbart ist.		
	Datenmigration	In dem Gebiet oder an dem Kundenstandort des eingetragenen Geschäftssitzes/der Hauptniederlassung (wie zutreffend) und/oder in Portugal, je nachdem, was zwischen den Parteien in der Projektdokumentation bzw. einer Leistungsbeschreibung vereinbart ist.		
	Fehlerbehebung	In dem entsprechenden Standort des Unit4-Support-Service und Portugal.		
	Kundenerfolg	In dem entsprechenden Standort des Unit4-Support-Service und Portugal.		

6. KONTAKTDATEN

Für Fragen oder Anmerkungen zu diesen Datenverarbeitungsbedingungen ist der Ansprechpartner der:

Datenverantwortliche: Per Brief (adressiert an Global Data Privacy Officer mit Kopie an Corporate Legal Department) P.O. Box 5005, 3528 BJ Utrecht, Niederlande oder per E-Mail an privacy@unit4.com oder an die für Mitteilungen im Vertrag angegebene Unit4-Adresse.

Auftragsverarbeiter: Die für Mitteilungen des Datenverantwortlichen im Vertrag angegebene Adresse.

VERZEICHNIS 2 – SICHERHEITSMASSNAHMEN

Wie in Absatz 6 der Datenverarbeitungsbedingungen dargelegt, sind die technischen und organisatorischen Sicherheitsmaßnahmen in diesem Verzeichnis aufgeführt und werden bei Bedarf ergänzt oder geändert. Der Datenverantwortliche betrachtet diese Maßnahmen als geeignet für die Verarbeitung personenbezogener Daten.

Unit4-Unternehmenssicherheitsmaßnahmen (Zusammenfassung interner Geschäftsbetrieb)

Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die der Auftragsverarbeiter in seinem Unternehmen (allgemein) implementiert hat:

Physische Sicherheit:

- Die physische Zugangskontrolle wird durch die Unit4-Einrichtungen gesteuert.
- Alle Büros verfügen über Sicherheitssysteme für die Zugangskontrolle durch Barrieren, z. B. Eingangstore, mit Personal besetzte Empfangstresen, Brandschutztüren mit Alarmfunktion, Einbruchmeldeanlagen und abschließbare Büros.
- Unit4 betreibt Zugangskontrollen mithilfe dessen, was Menschen wissen, wie Passwörter oder persönliche Zugangscodes, oder dessen, was Menschen bei sich tragen, wie Sicherheitsausweise;
- Serverräume vor Ort verfügen (gegebenenfalls) über zusätzliche physische Kontrollen.
- Eingeschränkter Zugang zu Sicherheitsbereichen oder sensiblen Daten, um nichtgenehmigten Zugang durch Besucher / nichtautorisierte Mitarbeiter zu verhindern (durch abschließbare Büros oder Schränke), sowie bei Bedarf der Grundsatz des leergeäumten Schreibtisches.
- Besucher bei Unit4 werden am Empfang kontrolliert (durch einen speziellen Empfangsmitarbeiter oder andere Mitarbeiter).
- Es werden Aktenvernichter oder andere geeignete sichere Entsorgungsmethoden für sensible Dokumente verwendet.

Virtuelle und Computer-Sicherheit:

- Der zuständige Vorgesetzte sorgt dafür, dass Mitarbeiter und Auftragnehmer alle Unit4 gehörenden Anlagen in ihrem Besitz am Ende ihrer Beschäftigung oder Vertragslaufzeit zurückgeben. Im Ticketing-System werden Aufzeichnungen über die Rückgabe von Anlagen gepflegt.
- Unit4 verfolgt das Ziel, Daten als öffentlich, vertraulich, geschützt oder sensibel zu klassifizieren. Daten werden dann entsprechend ihrer Klassifizierung geschützt.
- Medien (einschließlich Festplatten) werden sicher entsorgt, wenn sie nicht mehr benötigt werden. Alle sensiblen Materialien (Festplatten, Disketten usw.) werden vor der Entsorgung oder physischen Vernichtung mit garantierter Deinstallations-Software (nicht durch Neuformatierung oder Löschung) entfernt.
- Anti-Malware - wir verwenden die aktuellste Version von Branchenstandardlösungen zum Schutz vor Viren und Malware.
- Außerdem nutzt Unit4:
 - Kontrollen übertragener Rechte;
 - Protokollierung und Kontrolle des Systemzugriffs;
 - Recovery-Maßnahmen;
 - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste auf Dauer sicherzustellen, und
 - Systeme und Prozesse, um die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- Es bestehen Business Continuity- und Disaster Recovery-Pläne unter Berücksichtigung der Informationssicherheit.

Sicherheitsrichtlinien und Dokumentation:

- Das Global Leadership Team für Unit4 und/oder dessen jeweilige Management-Teams vor Ort haben die Kontrolle über globale wie lokale Pläne für das Informationsmanagement und die Informationssicherheit, einschließlich aller Informationssicherheitsrichtlinien, mit denen identifizierten Informationssicherheitsrisiken begegnet wird und die Unternehmensziele unterstützt werden.
- Informationssicherheit und -management obliegen global dem Global Information Security Manager und Global Data Privacy Officer, die Ressourcen verwalten, mit denen die Informationssicherheitsrichtlinie und der Informationssicherheitsprozess strategisch und insgesamt eingehalten werden.
- Unit4 verfügt über Sicherheitsrichtlinien, die entsprechend der bewährten Branchenpraxis regelmäßig aktualisiert und angepasst werden.
- Unit4 verfügt über eine Datenschutzrichtlinie und ein Weißbuch über die DSGVO, veröffentlicht unter www.unit4.com/terms.
- Sofern vertrauliche Geschäftsinformationen ausgetauscht werden, schließt Unit4 mit Drittanbietern Geheimhaltungs- und Vertraulichkeitsvereinbarungen.
- Unit4 sorgt dafür, dass alle Mitarbeiter und Auftragnehmer in ihren Verträgen Standardverschwiegenheitsklauseln unterschreiben.
- Unit4 ermöglicht allen Mitarbeitern Schulungen zu Datenschutz, Sicherheit und seinen zentralen Geschäftsprinzipien, wie oben dargelegt.

Zusätzliche Elemente für Unit4 SaaS auf Microsoft Azure (Zusammenfassung)

Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die der Auftragsverarbeiter in Bezug auf die Bereitstellung der Unit4 Cloud Services implementiert hat:

Datenschutz

Unit4 Cloud nutzt verschiedene Verfahren zum Schutz personenbezogener Daten in der Cloud. Nachstehend finden Sie einen umfassenden Überblick über die angewandten Kontrollen.

Sicherheitsfunktionen, -prozesse und -protokolle auf Netzwerkebene

- Sichere Datenübertragung über öffentliche Netzwerke – sämtlicher Datenverkehr wird über Branchenstandardprotokolle wie SSL/TLS und HTTPS gesichert.
- Systemsicherheit – Logische Authentifizierungs- und Autorisierungsmechanismen
- Firewalls – Firewall-Technologie der nächsten Generation, mit der die Kontrolle des ein- und ausgehenden Datenverkehrs gewährleistet ist.

Sicherheitsfunktionen, -prozesse und -protokolle auf Datenbankebene

- Datensicherheit – Logische Authentifizierungs- und Autorisierungsmechanismen
- Datenbanksicherheit – Jeder Kunde verfügt über seine eigene sichere Datenbank, so dass die Partitionierung von Datenbanken nicht erforderlich ist und die Kundendaten nicht mit anderen Daten vermischt werden. Im Ergebnis werden Kundendaten niemals unbeabsichtigt mit anderen ausgetauscht.
- Backups werden mit einer die gesamte Datenbank umfassenden Verschlüsselungstechnologie wie Transparent Database Encryption verschlüsselt. Azure Storage Service Encryption zur Verschlüsselung aller Daten im Speicherkonto eines Kunden.
- Unit4 verwendet Azure Key Vault für die Kontrolle über Schlüssel, die von Cloud-Anwendungen und -Services zur Datenverschlüsselung genutzt werden.

Fortwährend getestete und weiterentwickelte Sicherheit

Um unvorhergesehene Schwachstellen zu entdecken und unsere Erkennungs- und Reaktionsfunktionen zu verfeinern, untersuchen wir fortwährend, wie wir unseren Sicherheitsstatus verbessern und damit potentielle Datenschutzverletzungen abwehren können. Das operative Team der Unit4 Cloud, das den Betrieb der Unit4 Cloud (Cloud-Infrastruktur, Cloud-Services, Produkte, Geräte und interne Ressourcen) genau überwacht und absichert – Penetrationstest und Verbesserung unser Schutz-, Entdeckungs- und Wiederherstellungsfähigkeit in Bezug auf Cyberbedrohungen.

Entdeckung, Minderung und Reaktion bei Bedrohungen

In dem Maße, wie die Anzahl, Unterschiedlichkeit und Schwere von Cyberbedrohungen zugenommen haben, so ist auch unsere Sorgfalt bei der Entdeckung von Bedrohungen und die Reaktion darauf gewachsen. Zentralisierte Überwachungssysteme sorgen für ständige Sichtbarkeit und zeitnahe Alarme. Die regelmäßige Anwendung von Sicherheitspatches und -updates trägt dazu bei, Systeme vor bekannten Schwachstellen zu schützen. Systeme zur Entdeckung von Eindringversuchen und Malware sind darauf ausgerichtet, die Risiken durch Angriffe von außen zu entdecken und abzumildern. Im Falle bössartiger Aktivitäten folgt unser Vorfalreaktionsteam bewährten Verfahren für die Behandlung von Vorfällen sowie die Kommunikation und Wiederherstellung. Das Team wendet bewährte Branchenverfahren an, um sowohl interne Teams als auch Kunden zu warnen. Außerdem werden mit Sicherheitsberichten Zugriffsmuster überwacht, damit potentielle Bedrohungen proaktiv identifiziert und eingedämmt werden können.

Datentrennung

Daten sind die Währung der digitalen Wirtschaft und wir nehmen unsere Verantwortung für den Schutz der Kundendaten sehr ernst. Sowohl technologische Sicherheitsvorkehrungen wie verschlüsselte Kommunikation als auch betriebliche Prozesse tragen dazu bei, dass Kundendaten sicher sind. In der Cloud können die Daten mehrerer Kunden auf denselben IT-Ressourcen gespeichert sein. Unit4 verwendet die logische Trennung, um die Daten der einzelnen Kunden von denen anderer Kunden zu trennen. Unit4 SaaS ist darauf ausgelegt, den in einer Multitenant-Umgebung auftretenden Risiken entgegenzuwirken. Die Datenspeicherung und -verarbeitung wird zwischen den Verbrauchern logisch getrennt, indem beispielsweise dedizierte Konten und separate Datenbankinstanzen für alle unserer Kunden zum Einsatz kommen.

Netzwerkisolierung an mehreren Stellen:

- Jede Einzelimplementierung ist von anderen Implementierungen getrennt und kommuniziert durch eine private IP-Adresse.
- Die Kommunikation der VMs des Kunden ist nur möglich mit anderen VMs, die dem Kunden gehören oder von diesem kontrolliert werden, und mit Infrastrukturserviceendpunkten für die öffentliche Kommunikation.
- Der Datenverkehr zwischen VMs verläuft stets durch vertrauenswürdige Paketfilter.

Weitere Informationen zur Sicherheitsrichtlinie und dem Sicherheitsprogramm erhalten Sie unter www.unit4.com/terms.

Datenverschlüsselung

Unit4 bietet standardmäßig sicheren Zugriff auf alle seine Services, indem sämtliche Daten bei der Übertragung über öffentliche Netzwerke verschlüsselt werden. Dies geschieht ausschließlich über sichere Protokolle wie HTTPS über TLS mit der aktuellsten Sicherheitsverschlüsselung. Die Verschlüsselung von Daten während der Speicherung kann von Kunden optional bestellt werden. Das verwendete Verfahren ist eine transparente die gesamte Datenbank umfassende Verschlüsselung: TDE. Microsoft Azure-Kunden im Rahmen eines öffentlichen SaaS-Angebots erhalten die TDE-Verschlüsselung während der Speicherung standardmäßig.

Zugriffskontrolle

Kunden, die Unit4-Produkte in der Cloud verwenden, verfügen über die vollständige Front-End-Zugriffskontrolle auf ihre Anwendung. Die Verantwortung für die Erstellung neuer Konten, die Kontenschließung und -prüfung für die Unit4-Anwendung liegt demnach beim Kunden.

Unit4 verfügt weiterhin über einen eingeschränkten Back-End-Zugriff auf Kundendaten (durch eine direkte Datenbank-Verbindung). Der Zugriff durch Unit4 auf personenbezogene Daten ist streng auf die Aktivitäten begrenzt, die zur Installation, Implementierung, Wartung, Reparatur, Problembehebung oder Aktualisierung der Lösung notwendig sind. Alle Zugriffe werden protokolliert und sind auf eine kleine Gruppe von Cloud-Technikern und Support-Beratern beschränkt. Zugriffsprotokolle werden in der zentralen Überwachungslösung 365 Tage lang gespeichert. Bei Datenschutzverletzungen kann Unit4 auf Verlangen das Zugriffsprotokoll vorlegen.

Meldung von Datenschutzverletzungen

Wenn Unit4 eine Datenschutzverletzung bekannt wird, meldet es diese dem Kunden unverzüglich. Kunden müssen dafür sorgen, dass die im Unit4 Supportportal aufgeführten Kontakte stets aktuell sind, da diese für sämtliche Kommunikation genutzt werden.

Eingebauter Datenschutz und eingebaute Datensicherheit

Die Unit4 Cloud-Plattform wurde von Grund auf unter dem Gesichtspunkt der Datensicherheit und des Datenschutzes gestaltet. Unit4 sorgt für die fortwährende Verbesserung der Sicherheit der Lösung, indem Ergebnisse der jährlichen Penetrationstests und Prüfungen umgesetzt werden.

Zum Nachweis des sicheren Designs und Betriebs verfügt Unit4 Cloud Services SaaS Ops über die ISO 27001:2013-Zertifizierung und den ISAE3402 (SOC1)-Bericht. Unit4 und die Betreiber der Rechenzentren besitzen verschiedene Sicherheitszertifizierungen. Einzelheiten entnehmen Sie bitte der Cloud Service-Beschreibung.

Zusätzliche Elemente für Unit4 People-Plattform-Services (Zusammenfassung)

Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die der Auftragsverarbeiter in Bezug auf die Bereitstellung der Unit4 People-Plattform-Services (nur Cloud) implementiert hat:

Datenschutz

Die Unit4 People-Plattform nutzt verschiedene Verfahren zum Schutz personenbezogener Daten in der Cloud. Nachstehend finden Sie einen umfassenden Überblick über die angewandten Kontrollen.

Sicherheitsfunktionen, -prozesse und -protokolle auf Netzwerkebene

- Sichere Datenübertragung über öffentliche Netzwerke – sämtlicher Datenverkehr wird über Branchenstandardprotokolle wie SSL/TLS (1.2) und HTTPS gesichert.

Authentifizierung

- Alle Services folgen dem Prinzip der geringsten Rechte und die Authentifizierung gegenüber den Services und ihren APIs sind über Branchenstandardverfahren gesichert. Für die sichere Authentifizierung von Nutzern und/oder Client Services bei vertrauenswürdigen Parteien werden OpenID Connect und das zugrunde liegende OAuth 2.0-Protokoll verwendet, wobei sie die Identität und den Zugriff mithilfe Claims-basierter Token validieren.
- HMAC (Hash-based Message Authentication) wird als alternative Methode für die sichere Kommunikation zwischen Services verwendet.

Sicherheitsfunktionen, -prozesse und -protokolle auf Datenbankebene.

- Sämtliche in Speicherkonten gespeicherten Daten werden während der Speicherung verschlüsselt.
- Bei allen Speicherkonten ist eine sichere Übertragung erforderlich – sämtlicher Datenverkehr wird über Branchenstandardprotokolle wie SSL/TLS und HTTPS gesichert.
- Alle in Azure Cosmos DB gespeicherten Daten werden während der Speicherung und der Übertragung verschlüsselt.
- Bei allen Azure SQL-Servern ist die transparente Datenverschlüsselung (Transparent Data Encryption, TDE) aktiviert.
- Bei allen Azure SQL Servern ist die Entdeckung und Prüfung von Bedrohungen aktiviert.
- Azure KeyVault wird zur Sicherung besonders sensibler Daten wie Service Principle-Anmeldedaten verwendet.

Sicherheitsfunktionen, -prozesse und -protokolle auf Übermittlungsebene.

- Alle durch Azure Service Bus-Instanzen gespeicherten Daten werden während der Speicherung verschlüsselt.
- Sämtlicher Datenverkehr auf dem Azure Service Bus wird über Branchenstandardprotokolle wie SSL gesichert.

Weitere Informationen zur Sicherheitsrichtlinie und dem Sicherheitsprogramm erhalten Sie unter www.unit4.com/terms.

Datenverschlüsselung

Die Unit4 People-Plattform-Services bieten standardmäßig sicheren Zugriff auf alle ihre Services, indem sämtliche Daten bei der Übertragung über öffentliche Netzwerke verschlüsselt werden. Dies geschieht ausschließlich über sichere Protokolle wie HTTPS über TLS (1.2) mit der aktuellsten Sicherheitsverschlüsselung. Alle gespeicherten Daten sind verschlüsselt.

Meldung von Datenschutzverletzungen

Wenn Unit4 eine Datenschutzverletzung bekannt wird, meldet es diese dem Kunden unverzüglich. Kunden müssen dafür sorgen, dass die im Unit4 Supportportal aufgeführten Kontakte stets aktuell sind, da diese für sämtliche Kommunikation genutzt werden.

Eingebauter Datenschutz und eingebaute Datensicherheit

Die Unit4 People-Plattform-Services wurden von Grund auf unter dem Gesichtspunkt der Datensicherheit und des Datenschutzes gestaltet. Unit4 sorgt für die fortwährende Verbesserung der Sicherheit der Lösung, indem Ergebnisse der jährlichen Penetrationstests und Prüfungen umgesetzt werden.

Zusätzliche Elemente für Unit4 Cloud Service – Talent Management SaaS (Zusammenfassung)

Talent Management SaaS ist nach ISO27001 zertifiziert und hat eine ISO27001 (Phase 1 & 2)- und DSGVO-Prüfung durchlaufen. Die wichtigsten Informationen sind in der Tabelle aufgeführt und zusätzliche Dokumentationen oder Informationen sind auf Anfrage erhältlich.

Domain	Verfahren
Informationssicherheit und Governance	Der Intuo SaaS Service hat ein Informationssicherheits-Managementsystem (ISMS) nach ISO27001 etabliert. Teil dessen ist unter anderem eine Informationssicherheitsrichtlinie für alle Mitarbeiter, die auf Anfrage erhältlich ist. Im Sinne der Informationssicherheit wurden ebenfalls Managementmaßnahmen zur Risikoreduktion umgesetzt. Diese Risiken und die Wahrscheinlichkeit ihres Eintretens sind Bestandteil des ISO27001 ISMS.
Personalsicherheit	Die Bereitstellung des Talent Management SaaS Service sieht vor, dass alle vertraulichen Daten in einem Personalinformationssystem (HRIS) gespeichert werden und ISO27001 entsprechen, wofür die Informationssicherheitsabteilung zuständig ist.
Anlagenverwaltung	Anlagen (sowohl digitale wie nicht-digitale) werden entsprechend einer Datenklassifizierungsrichtlinie gepflegt
Datenzugriffskontrolle	Es bestehen mehrere Richtlinien, die dem Prinzip der geringsten Rechte folgen, sowohl für bereitgestellte Anwendungen, allgemeine Informationen als auch eigene Daten. Der Zugriff auf eigene Systeme, die bei Amazon (AWS) gehostet werden, ist auf bestimmte ausgewiesene Personen beschränkt und die Verwendung von Passwörtern ist ausdrücklich verboten. Zur Authentifizierung gegenüber Servern werden nur öffentliche/private Schlüsselpaare verwendet. Die Zugriffsrechte des jeweiligen Nutzers werden in Übereinstimmung mit der etablierten Zugriffsrichtlinie festgelegt. Spezielle Fragen zum Datenzugriff und den entsprechenden Richtlinien können an die Informationssicherheit gerichtet werden.
Betriebssicherheit	Diese fällt in den Geltungsbereich unserer ISMS (ISO27001).
Kommunikationssicherheit	Für sämtliche Kommunikation gilt eine Datenklassifizierungsrichtlinie. Der gesamte Netzwerk-Datenverkehr läuft über SSL/HTTPS, das am meisten verwendete und vertrauenswürdigste Kommunikationsprotokoll im Internet. Die interne Infrastruktur wird durch strikte Firewalls und Netzwerkzugriffslisten getrennt. Jedes System ist durch seine Funktion einer Firewall-Sicherheitsgruppe zugewiesen. Standardmäßig wird der gesamte Zugriff verweigert und nur ausdrücklich erlaubte Ports sind zugänglich. Persistenz- und Speicherschichten sind verschlüsselt (auch während der Speicherung) und durch VPN- und VPC-Firewalls geschützt. Das Netzwerk der Büros ist durch eine redundante Fortinet 200D-Firewall geschützt, die sich im Rechenzentrum in Merelbeke befindet, das über Dark Fiber mit der Ghelamco Arena verbunden ist. Weitere Informationen über diese Verbindung findet sich im Dokument „Continuity and Security measures“, das ebenfalls Bestandteil des ISMS der ISO27001-Zertifizierung ist.

VERZEICHNIS 3 – UNIT 4 UNTERAUFTRAGSVERARBEITER

Service	Unterauftragsverarbeiter (Unternehmensname, Standort usw.)	Ort der Verarbeitung	Art der Leistung nach Unterauftragsverarbeiter / damit verwendetem Modul
Unit4 Professional Services (falls an einen Leistungserbringerpartner als Unterauftrag vergeben)	Wie im Vertrag festgelegt.	Wie im Vertrag festgelegt.	Wie im Auftragsformular festgelegt oder schriftlich mit dem Kunden vereinbart.
Drittanbieter-Produkte und -Leistungen nur zutreffend, wenn durch den Kunden erworben	Wie im Vertrag festgelegt.	Wie im Vertrag oder weiteren Verzeichnissen oder Anlagen zum Vertrag im Zusammenhang mit der Verarbeitung durch den Drittanbieter festgelegt.	Software- und//oder Supportleistungen und/oder Cloud-Services.
Unit4 SaaS	Microsoft Azure	Wie oben in Verzeichnis 2, Absatz 5 angegeben	Anbieter von Cloud-Infrastruktur und -Services
	Microsoft Dynamics	Wie oben in Verzeichnis 2, Absatz 5 angegeben	Anbieter von Softwareleistungen, insbesondere Microsoft Dynamics (einschließlich bestimmter Cloud-Infrastruktur).
	Microsoft	Wie oben in Verzeichnis 2, Absatz 5 angegeben	Anbieter von Software-Tools und Office
	Conapto	Wie oben in Verzeichnis 2, Absatz 5 angegeben	Anbieter von Cloud-Infrastruktur und -Services
Unit4 SaaS-Talent Management	Amazon Web Services	Frankfurt, Deutschland	Lösungsanbieter – Suite
	Freshdesk	Vereinigte Staaten von Amerika (Datenschutzrichtlinie)	Lösungsanbieter – Suite (Privacy-Shield-Link: Link)
	LogDNA	Vereinigte Staaten von Amerika (Datenschutzrichtlinie)	Lösungsanbieter – Suite (Privacy-Shield-Link: Link)
	Mandrill	Vereinigte Staaten von Amerika (Datenschutzrichtlinie)	Lösungsanbieter – Suite (Privacy-Shield-Link: Link)
	Mixpanel	Vereinigte Staaten von Amerika (Datenschutzrichtlinie)	Lösungsanbieter – Suite (Privacy-Shield-Link: Link)
	Pingdom	Vereinigte Staaten von Amerika (Datenschutzrichtlinie)	Lösungsanbieter – Suite (Privacy-Shield-Link: Link)
	Productboard	Europäischer Wirtschaftsraum und Vereinigte Staaten von Amerika (Datenschutzrichtlinie)	Lösungsanbieter – Suite (Privacy-Shield-Link: Link)
	Rustici Software	AWS US-East-1 (Datenschutzrichtlinie)	Lösungsanbieter – Learn (nur SCORM) (Privacy-Shield-Link: Link)
	Sentry	Vereinigte Staaten von Amerika (Datenschutzrichtlinie)	Lösungsanbieter – Suite (Privacy-Shield-Link: Link)
	Slack	Vereinigte Staaten von Amerika (Datenschutzrichtlinie)	Lösungsanbieter – Perform (Privacy-Shield-Link: Link)
	Stripe	Länder, in denen Stripe tätig ist (Datenschutzrichtlinie)	Lösungsanbieter – Learn (Privacy-Shield-Link: Link)
	Wistia	Vereinigte Staaten von Amerika (Datenschutzrichtlinie)	Lösungsanbieter – Learn (Privacy-Shield-Link: Link)
People-Plattform-Services („PPS“) (allgemein), einschließlich IDS und Wanda (sowie alle Supportleistungen)	Microsoft Azure	Wie oben in Verzeichnis 1, Absatz 5 und unter folgendem Link durch Microsoft angegeben: https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located .	Anbieter von Cloud-Infrastruktur und Plattform-Services (wie oben angegeben) in Abschnitt 2.

VERZEICHNIS 4 – EU-STANDARDVERTRAGSKLAUSELN

Die Tabelle enthält die Daten, die in die unterhalb der Tabelle aufgeführten EU-Standardvertragsklauseln eingefügt werden müssen:

Parteien	Der Datenexporteur ist der Datenverantwortliche, dessen Angaben in einem Auftragsformular (als Kunde) im Vertrag zwischen dem Datenverantwortlichen und Auftragsverarbeiter erscheinen. Der Datenimporteur ist der Auftragsverarbeiter, dessen Angaben in einem Auftragsformular (von Unit4) im Vertrag zwischen dem Datenverantwortlichen und Auftragsverarbeiter erscheinen.
Klausel 9 und 11(3)	Der Datenexporteur ist in dem im Vertrag genannten Gebiet ansässig.
Anlage 1	Die zum Ausfüllen dieser Anlage benötigten Daten sind in Verzeichnis 1 und Verzeichnis 3 dieser Datenverarbeitungsbedingungen aufgeführt
Anlage 2	Die zum Ausfüllen dieser Anlage benötigten Daten sind in Verzeichnis 2 dieser Datenverarbeitungsbedingungen aufgeführt

STANDARDVERTRAGSKLAUSELN (AUFTRAGSVERARBEITER)

gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

Bezeichnung der Organisation (Datenexporteur): ...

Anschrift: ...

Tel.: ... Fax ... E-Mail: ...

Weitere Angaben zur Identifizierung der Organisation

...

(„Datenexporteur“)

und

Bezeichnung der Organisation (Datenimporteur): ...

Anschrift: ...

Tel.: ... Fax ... E-Mail: ...

Weitere Angaben zur Identifizierung der Organisation:

...

(„Datenimporteur“)

(die „Partei“, wenn eine dieser Organisationen gemeint ist, die „Parteien“, wenn beide gemeint sind)

VEREINBAREN folgende Vertragsklauseln („Klauseln“), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1

Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

- die Ausdrücke „personenbezogene Daten“, „besondere Kategorien personenbezogener Daten“, „Verarbeitung“, „für die Verarbeitung Verantwortlicher“, „Auftragsverarbeiter“, „betroffene Person“ und „Kontrollstelle“ entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (1);
- der „Datenexporteur“ ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;
- der „Datenimporteur“ ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;
- der „Unterauftragsverarbeiter“ ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;
- der Begriff „anwendbares Datenschutzrecht“ bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;
- die „technischen und organisatorischen Sicherheitsmaßnahmen“ sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

Klausel 2

Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3

Drittbegünstigtenklausel

- (1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.
- (2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.
- (3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.
- (4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4

Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

- a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;
- b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;
- c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;
- d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;
- e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;
- f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;
- g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;
- h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;
- i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und
- j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5

Pflichten des Datenimporteurs (2)

Der Datenimporteur erklärt sich bereit und garantiert, dass:

- a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;
- b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;
- c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;
- d) er den Datenexporteur unverzüglich informiert über
 - i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;
 - ii) jeden zufälligen oder unberechtigten Zugang und

- iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;
- e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;
- f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfungsgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;
- g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;
- h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;
- i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;
- j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6

Haftung

- (1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.
- (2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.
- (3) Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7

Schlichtungsverfahren und Gerichtsstand

- (1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:
 - a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder
 - b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.
- (2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8

Zusammenarbeit mit Kontrollstellen

- (1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.
- (2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.
- (3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9

Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: ...

Klausel 10

Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11

Vergabe eines Unterauftrags

- (1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss ⁽³⁾. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.
- (2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.
- (3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: ...
- (4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klausel 12

Pflichten nach Beendigung der Datenverarbeitungsdienste

- (1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.
- (2) Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.

Die Parteien vereinbaren, dass diese Standardvertrags-Klauseln mit Vertragsschluss gemäß dem vorgesehenen Bestellformular zwischen den Parteien verbindlich gelten und Vertragsbestandteil werden.

⁽¹⁾ Die Parteien können die Begriffsbestimmungen der Richtlinie 95/46/EG in diese Klausel aufnehmen, wenn nach ihrem Dafürhalten der Vertrag für sich allein stehen sollte.

⁽²⁾ Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

⁽³⁾ Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.

Anhang 1

zu den Standardvertragsklauseln

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden

Die Mitgliedstaaten können entsprechend den nationalen Verfahren Zusatzangaben, die in diesem Anhang enthalten sein müssen, ergänzen

Datenexporteur

Der Datenexporteur ist (bitte erläutern Sie kurz Ihre Tätigkeiten, die für die Übermittlung von Belang sind):

Siehe dazu oben Verzeichnis 1 der Datenverarbeitungsbedingungen.

Datenimporteur

Der Datenimporteur ist (bitte erläutern Sie kurz die Tätigkeiten, die für die Übermittlung von Belang sind):

Siehe dazu oben Verzeichnis 1 der Datenverarbeitungsbedingungen.

Betroffene Personen

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen (bitte genau angeben):

Siehe dazu oben Verzeichnis 1 der Datenverarbeitungsbedingungen.

Kategorien von Daten

Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben):

Siehe dazu oben Verzeichnis 1 der Datenverarbeitungsbedingungen.

Besondere Datenkategorien (falls zutreffend)

Die übermittelten personenbezogenen Daten umfassen folgende besondere Datenkategorien (bitte genau angeben):

Siehe dazu oben Verzeichnis 1 der Datenverarbeitungsbedingungen.

Verarbeitung

Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen (bitte genau angeben):

Siehe dazu oben Verzeichnis 1 der Datenverarbeitungsbedingungen.

DATENEXPORTEUR

Name: ...

Unterschrift des/der Bevollmächtigten: ...

DATENIMPORTEUR

Name: ...

Unterschrift des/der Bevollmächtigten: ...

Anhang 2

zu den Standardvertragsklauseln

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden

Beschreibung der technischen oder organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gemäß Klausel 4 Buchstabe d und Klausel 5 Buchstabe c eingeführt hat (oder Dokument/Rechtsvorschrift beigefügt):

(Siehe dazu oben Verzeichnis 2 der Datenverarbeitungsbedingungen)