

ABSCHNITT 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 ERPx | 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 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 nicht 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; Auftragnehmer (jeder Art), Bevollmächtigte oder Geschäftsführer. |
| Unit4 Assistance PSA Suite | Namen; Adressen; Telefonnummern (einschließlich Mobiltelefon); E-Mail-Adresse(n); sonstige Kontaktdaten. Andere personenbezogene Daten müssen nicht gespeichert oder verarbeitet werden, damit die Zielsetzungen des Produkts (wie nachstehend genannt) erreicht werden, andere personenbezogene | Gegenwärtige oder frühere Mitarbeiter; |

| | | |
|--|---|---|
| | 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. | 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): Anmeldedaten, 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), Localisations Services und Unit4 Apps | Da es sich bei den PPS, Localisations Services bzw. Unit4 Apps 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. 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). | Alle Kategorien einzelner Personen, die in dieser Tabelle aufgeführt sind. 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. |
| Unit4 Property Management | 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. |

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 gemäß Vereinbarung, 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 x | <p>Personenbezogene Daten werden in Unit4 ERP 8 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; |

| | |
|------------------|---|
| | <ul style="list-style-type: none"> • Abrechnung; • Bestellanforderungen; • Personal-/Projektplanung. <p>Die Verarbeitung umfasst:</p> <p>Produkt (Softwarelösung)</p> <ul style="list-style-type: none"> • Unit4 ERP 8 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 Services, wie näher in der Services-Beschreibung aufgeführt, oder People-Plattform-Services. • 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 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; • Verarbeitung Zeiterfassung; • Prozesse im Zusammenhang mit Personalwesen und Gehaltsabrechnung; • Gehaltsabrechnung; • Kursanmeldung; • Kompetenzmanagement; • Beurteilungen; • Gehaltsüberprüfung; • Bewerberregistrierung; • Verarbeitung Zahlungsvorgänge; • Rechnungsstellung; • 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 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 Services, wie näher in der Services-Beschreibung oder People-Plattform-Service-Leistungsbeschreibung aufgeführt. • Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 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 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; • 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. <p>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.</p> |
| 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 Services, wie näher in der Services-Beschreibung oder People-Plattform-Services aufgeführt. Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 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 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 Services, wie näher in der Services-Beschreibung oder People-Plattform-Services 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 Services wie näher in der Services-Beschreibung oder People-Plattform-Services aufgeführt. Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 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, und 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 Services, wie näher in der Services-Beschreibung oder People-Plattform-Services aufgeführt. Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 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“, Localisations Services) und Apps | <p>Die Daten werden durch die PPS, Localisations Services bzw. Apps 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, 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 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. <p>Services</p> <ul style="list-style-type: none"> Übertragung und Speicherung von personenbezogenen Daten zur Bereitstellung weiterer Services, wie näher in der Services-Beschreibung oder People-Plattform-Services aufgeführt. Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für Unit4 PPS 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. |
| Unit4 Property Management | <p>Personenbezogene Daten werden in Unit4 Property 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"> Bewerberregistrierung; Lease out Management; |

- Verarbeitung von Mietverträgen
- Vermietungs-/Eigentumsverwaltung;
- Elektronische Unterzeichnung;
- Lastschriften inkl. Rechnungsausdruck;
- Verarbeitung Zahlungsvorgänge;
- Mahnverfahren;
- Mieterwechsel.

Die Verarbeitung umfasst:

Produkt (Softwarelösung)

- Unit4 Property 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.

Services

- Übertragung und Speicherung von personenbezogenen Daten zur Bereitstellung weiterer Services, wie näher in der Services-Beschreibung oder People-Plattform-Services aufgeführt.
- Zugriff auf die personenbezogenen Daten zur Bereitstellung von Support und Wartung für das Unit4 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.

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 (General) | Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Zusammenhang mit den im Vertrag beschriebenen Aktivitäten und insbesondere der Services-. | <p><u>Personal</u></p> <p>Das operative Team der Unit4 Cloud verfügt über Personal in der EU (wie etwa in Polen, Schweden, Norwegen) dem Vereinigten Königreich, den USA, Kanada, Malaysia und Singapur. Diese Mitarbeiter des Auftragsverarbeiters verarbeiten die Unit4 SaaS.</p> <p><u>Anlagen und Infrastruktur</u></p> <p>Unit4 nutzt Hosting-Infrastrukturservices von Drittanbietern, um Unit4 SaaS bereitzustellen, und setzt andere Software-Systeme für Betrieb und Verwaltung ein. Siehe Abschnitt 3.</p> |
| U4 Talent Management | Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Zusammenhang mit den im Vertrag beschriebenen Aktivitäten und insbesondere der geltenden Service-Beschreibung. | <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. Abschnitt 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 in der EU (wie etwa in Polen, Portugal, Spanien, Niederlande., Deutschland, Schweden,) in Norwegen, UK 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> |

| | | |
|---|---|--|
| <p>Unit4 Professional Services (falls an einen Leistungserbringerpartner als Unterauftrag vergeben)</p> | <p>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 Dritten festgelegt sind. Für weitere Informationen siehe Abschnitt 3.</p> <p>Der Auftragsverarbeiter schließt mit dem bzw. den Unterauftragsverarbeiter(n) einen schriftlichen Vertrag, der den relevanten Gesetzen und Vorschriften gemäß geltender Vereinbarung entspricht.</p> <p>Der Datenverantwortliche hat durch den Vertragsschluss dem Auftragsverarbeiter außerdem die Zustimmung erteilt, den bzw. die in Abschnitt 3 aufgeführten Unterauftragsverarbeiter zu beauftragen.</p> | <p>Siehe Abschnitt 3 bzw. das einschlägige Angebotsformular.</p> |
| <p>Drittanbieter-Produkte und -Leistungen</p> | <p>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.</p> | <p>Siehe Abschnitt 3 bzw. das einschlägige Angebotsformular und alle anderen Bestimmungen, die in weiteren Verzeichnissen oder Anlagen zu diesen Datenverarbeitungsinformationen enthalten sind, sofern dies durch den Drittanbieter oder gesetzlich vorgeschrieben ist.</p> |
| <p>People-Plattform-Services („PPS“), Lokalisation Services oder Apps</p> | <p>Neben Unit4 SaaS verarbeitet mit der / den PPS, Localisation Services bzw. Apps (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> | <p><u>Personal</u></p> <p>Das operative Team der Unit4 Cloud, das die PPS betreibt, verfügt über Personal in der EU (wie etwa Polen, Schweden, Niederlande, Spanien, Portugal), in 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, Localisation Services bzw. Apps anzubieten. Dazu gehören auch Drittanbietersysteme (d. h. Anwendungen zur Zusammenarbeit), über die Unit4 keine Kontrolle hat. Die PPS, Localisation Services bzw. Apps 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> • Functions – <i>stellt logische Algorithmen für Erweiterungen bereit</i> • Event grid – <i>stellt Kommunikationsmöglichkeiten bereit</i> • API Management – <i>verwaltet APIs</i> • Service Plans - <i>Linux und dynamischer Service</i> • Storage accounts - <i>Speicherplatz</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> <p>Zusätzlich nutzt PPS, Unit4 Localisation Services bzw. Apps Twilio – sendgrid-um Mails zu verschicken.</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 | GEPOLITISCHE 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 in Microsoft Azure sowohl für die EU als auch UK in den oben genannten Geo-politischen Zonen, mit der Zone, die dem Kunden zugerechnet wird, betrieben. Alle Kundendaten werden, außer für den Austausch mit ausgewählten Unterauftragsverarbeitern in Abschnitt 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 (die aber auch andere EU-Länder mit einschließen können) 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-(24/7) Support | Nach der „Follow the sun“-Methode kann der Rund-um-die-Uhr-Support für Kundenfälle von jedem der oben aufgeführten Support-Standorte (aber auch von den Niederlanden, Spanien oder von anderen Standorten, sofern dies wegen des operativen Unit4 Geschäfts erforderlich ist) 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); LOKALISATION SERVICES ODER APPS | 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, wo es Azure standorte gibt (z.B. USA). | EU-Länder, einschließlich Irland, Polen, Spanien, Vereinigte Staaten und sonstiger globaler Support an anderen Standorten, sofern erforderlich |
| PPS, Lokalisation Services oder Apps | Anhängig vom Cloud-Einsatz | Verarbeitung und Datenspeicherung erfolgt in der ausgewählten | Wie oben für Unit4 SaaS | |

| | | | | |
|---|---|---|----------------------|--|
| | | | Geo-politischen Zone | |
| Unit4 Professional Services und Unit4-Kundenerfolgsfunktion | Thema | Professionelle Dienstleistungen und Kundenerfolg werden bereitgestellt durch: | | |
| | Implementierung und andere Projekt-services | 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 Datenverarbeitungsinformationen ist der Ansprechpartner der:

Datenverarbeiter: Per Brief (adressiert an Global Data Protection 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.

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

ABSCHNITT 2 – SICHERHEITSMASSNAHMEN

Wie in Absatz 6 der Datenverarbeitungsbedingungen dargelegt, sind die technischen und organisatorischen Sicherheitsmaßnahmen in diesem Abschnitt 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/oder 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. Es 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 Chief Information Security Officer und Global Data Protection 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 SaaS 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.
- Database Backups werden mit einer die gesamte Datenbank umfassenden Verschlüsselungstechnologie wie Transparent Database Encryption verschlüsselt.
- Nicht-transaktionsbezogene Daten und Ordner werden standardgemäß systematisch verschlüsselt (AES).

- 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 unserer 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 für alle unserer Kunden zum Einsatz kommen.

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. 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.

Unit4 und die Betreiber der Rechenzentren besitzen verschiedene Sicherheitszertifizierungen. Einzelheiten entnehmen Sie bitte der einschlägigen 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 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.

ABSCHNITT 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 in weiteren Abschnitten 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 Abschnitt 2, Absatz 5 angegeben | Anbieter von Cloud-Infrastruktur und -Services |
| | Microsoft Dynamics | Wie oben in Abschnitt 2, Absatz 5 angegeben | Anbieter von Softwareleistungen, insbesondere Microsoft Dynamics (einschließlich bestimmter Cloud-Infrastruktur). |
| | Microsoft | Wie oben in Abschnitt 2, Absatz 5 angegeben | Anbieter von Software-Tools und Office |
| | | | |
| | Conapto | Wie oben in Abschnitt 2, Absatz 5 angegeben | Anbieter von Cloud-Infrastruktur und -Services |
| | Twilio - Sengrid | Vereinigte Staaten von Amerika (Privacy policy) | Mail Versand (EU SCCs – siehe Abschnitt 4) |
| | | | |
| Unit4 SaaS-Talent Management | Microsoft Azure | Dublin, Irland | Lösungsanbieter – Suite |
| | | | |
| | LogDNA | Vereinigte Staaten von Amerika (Datenschutzrichtlinie) | Lösungsanbieter – Suite (EU SCCs – siehe Abschnitt 4) |
| | Mandrill | Vereinigte Staaten von Amerika (Datenschutzrichtlinie) | Lösungsanbieter – Suite (EU SCCs – siehe Abschnitt 4) |
| | Mixpanel | Vereinigte Staaten von Amerika (Datenschutzrichtlinie) | Lösungsanbieter – Suite (EU SCCs – siehe Abschnitt 4) |
| | | | |
| | Rustici Software | AWS US-East-1 (Datenschutzrichtlinie) | Lösungsanbieter – Learn (nur SCORM) (EU SCCs – siehe Abschnitt 4) |
| | Sentry | Vereinigte Staaten von Amerika (Datenschutzrichtlinie) | Lösungsanbieter – Suite (EU SCCs – siehe Abschnitt 4) |
| | Slack | Vereinigte Staaten von Amerika (Datenschutzrichtlinie) | Lösungsanbieter – Perform (EU SCCs – siehe Abschnitt 4) |
| | | | |
| | Wistia | Vereinigte Staaten von Amerika (Datenschutzrichtlinie) | Lösungsanbieter – Learn (EU SCCs – siehe Abschnitt 4) |
| People-Plattform-Services („PPS“) (allgemein), einschließlich IDS und Wanda (sowie alle Supportleistungen) | Microsoft Azure | Wie oben in Abschnitt 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 1. |
| | | Twilio - Sengrid | Vereinigte Staaten von Amerika (Privacy policy) |

ABSCHNITT 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 Abschnitt 1 und Abschnitt 3 dieser Datenverarbeitungsinformationen aufgeführt |
| Anlage 2 | Die zum Ausfüllen dieser Anlage benötigten Daten sind in Abschnitt 2 dieser Datenverarbeitungsinformationen 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 Auftrags 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 Abschnitt 1 der Datenverarbeitungsinformationen.

Datenimporteur

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

Siehe dazu oben Abschnitt 1 der Datenverarbeitungsinformationen.

Betroffene Personen

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

Siehe dazu oben Abschnitt 1 der Datenverarbeitungsinformationen.

Kategorien von Daten

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

Siehe dazu oben Abschnitt 1 der Datenverarbeitungsinformationen.

Besondere Datenkategorien (falls zutreffend)

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

Siehe dazu oben Abschnitt 1 der Datenverarbeitungsinformationen.

Verarbeitung

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

Siehe dazu oben Abschnitt 1 der Datenverarbeitungsinformationen.

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 Abschnitt 2 der Datenverarbeitungsinformationen)