Unit4 Information zur Datenverarbeitung mit EU-Standarddatenschutzklauseln („SCCS“)

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	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. 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. Zusätzliche personenbezogene Daten für frühere und aktuelle Bewerber: Daten früherer Hochschulen; Zeugnisse und/oder (zusätzliche) Testergebnisse, körperlicher Gesundheitszustand; Zeugnisse früherer Arbeitgeber sowie Arbeitsplatzinformationen. 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.	• 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; 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 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	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:
	
	• Reiseanträge;
	• Spesenantragsverarbeitung;
	• Stundenzettelverarbeitung;
	• Abwesenheitsmanagement;
	• Prozesse im Zusammenhang mit Personalwesen und Gehaltsabrechnung:
	  ○ Gehaltsabrechnung;
	  ○ Kursanmeldung;
	  ○ Kompetenzmanagement;
	  ○ Beurteilungen;
	  ○ Gehaltsüberprüfung;
	  ○ Bewerberregistrierung;
	• Zahlungsverarbeitung;

	• Abrechnung; • Bestellanforderungen; • Personal-/Projektplanung. Die Verarbeitung umfasst: ***Produkt (Softwarelösung)*** • 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. ***Services*** • 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	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: • ; • Reiseanträge; • ; • Spesenantragsverarbeitung; • Verarbeitung Zeiterfassung; • Prozesse im Zusammenhang mit Personalwesen und Gehaltsabrechnung; • Gehaltsabrechnung; • Kursanmeldung; • Kompetenzmanagement; • Beurteilungen; • Gehaltsüberprüfung; • Bewerberregistrierung; • Verarbeitung Zahlungsvorgänge; • Rechnungsstellung; • Bestellanforderungen; • Personal / Projektplanung. Die Verarbeitung umfasst: **Produkt (Softwarelösung)** • 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. **Services** • 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	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:
	
	• Kunden-/Lieferanten-/Mitarbeiterregistrierung;
	• Zahlungsverarbeitung;
	• Abrechnung;
	• Spesenantragsverarbeitung;
	• Reiseanträge;
	• Bestellanforderungen und Aufträge;
	• Personal-/Projektplanung;
	• Prozesse im Zusammenhang mit Personalwesen und Gehaltsabrechnung:
	  ○ Gehaltsabrechnung;
	  ○ Stundenzettelverarbeitung;
	  ○ Abwesenheitsmanagement
	  ○ Kursanmeldung;
	  ○ Kompetenzmanagement;
	  ○ Beurteilungen;
	  ○ Gehaltsüberprüfung;
	  ○ Bewerberregistrierung;
	
	Die Verarbeitung umfasst:
	
	Produkt (Softwarelösung)

	• 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. **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 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	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: • 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 Die Verarbeitung umfasst: **Produkt (Softwarelösung)** • 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. **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.
Unit4 FP&A	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: • Finanzplan; • Finanz- und sonstige Berichterstattung; • Berichtsverteiler; • Zustimmungsverarbeitung; • Personal-/Projektplanung. Die Verarbeitung umfasst: **Produkt (Softwarelösung)** • 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. **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 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	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: • Humankapital-Management; • Mitarbeiterleistungs-Management; • Talententwicklung; • Kandidatenbewertung; • Weiterbildung; • Feedback und Lob; sowie • Personalanalyse und -motivation. Die Verarbeitung umfasst:

	Produkt (Softwarelösung) • 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. **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.
Unit4 Assistance PSA Suite	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: • 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. Die Verarbeitung umfasst: **Produkt (Softwarelösung)** • 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. **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.
People-Plattform-Services („**PPS**“, Localisations Services) und Apps)	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. 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. Die Aufgaben können Folgendes umfassen: • Stundenzetteleingaben • Speseneingaben • Reiseanträge • Gehaltsabrechnungsanfragen • Abwesenheitseingaben • Saldoabfragen • Bestellanforderungen. Die Verarbeitung umfasst: ***Produkt (Softwarelösung)*** • 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 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	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: • 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-.	<u>Personal</u> 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. <u>Anlagen und Infrastruktur</u> Unit4 nutzt Hosting-Infrastrukturservices von Drittanbietern, um Unit4 SaaS bereitzustellen, und setzt andere Software-Systeme für Betrieb und Verwaltung ein. Siehe Abschnitt 3.
U4 Talent Management	Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Zusammenhang mit den im Vertrag beschriebenen Aktivitäten und insbesondere der geltenden Service-Beschreibung.	<u>Personal</u> 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. <u>Anlagen und Infrastruktur</u> 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.
Supportleistungen	Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Zusammenhang mit den im Vertrag beschriebenen Aktivitäten und insbesondere den Unit4-Supportbedingungen.	<u>Personal</u> 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). <u>Anlagen und Infrastruktur</u> Unit4 nutzt andere Software-Systeme für den Betrieb, die Erbringung und Verwaltung dieser Leistungen.
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.	<u>Personal</u> 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. <u>Anlagen und Infrastruktur</u> Unit4 nutzt andere Software-Systeme für den Betrieb, die Erbringung und Verwaltung dieser Leistungen.

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 Dritten festgelegt sind. Für weitere Informationen siehe Abschnitt 3. Der Auftragsverarbeiter schließt mit dem bzw. den Unterauftragsverarbeiter(n) einen schriftlichen Vertrag, der den relevanten Gesetzen und Vorschriften gemäß geltender Vereinbarung entspricht. Der Datenverantwortliche hat durch den Vertragsschluss dem Auftragsverarbeiter außerdem die Zustimmung erteilt, den bzw. die in Abschnitt 3 aufgeführten Unterauftragsverarbeiter zu beauftragen.	Siehe Abschnitt 3 bzw. das einschlägige Angebotsformular.
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 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.

People-Plattform-Services („**PPS**“), Lokalisation Services oder Apps	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.	<u>Personal</u>
		
		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.
		
		<u>Anlagen und Infrastruktur</u>
		
		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:
		
		• Kognitive Leistungen:
		  ○ LUIS Cognitive Service - *Sprachverstehen.*
		  ○ Text Translator API – *Textübersetzung*
		  ○ QnA Maker Cognitive Service – *Frage- und Antwortservice*
		• Bot Framework Connectors – *sorgt für die Verbindung von Wanda zu den unterstützten Social-Media-Kanälen*.
		• Traffic Manager – *verwendet für Disaster Recovery und Ausfallsicherung bei gestörter Primärregion*
		• Web Apps / Web Jobs – *hostet Web-APIs und langlaufende webbasierte Prozesse*
		• Service Bus – *stellt interne Kommunikation im Wanda-Ökosystem bereit*
		• Speicherkonten – *verwendet zur Speicherung des Konversationsstatus und der Nutzereinstellungen*
		• Cosmos DB –*stellt Speicherung bereit*
		• *Functions – stellt logische Algorithmen für Erweiterungen bereit*
		• *Event grid – stellt Kommunikationsmöglichkeiten bereit*
		• API Management – verwaltet APIs
		• Service Plans - Linux und dynamischer Service
		• Storage accounts - Speicherplatz
		• Key Vault – *speichert vertrauliche Daten, die zur Kommunikation mit Microsoft-Services und für interne Services verwendet werden*
		• Redis Cache – *bietet Caching-Funktionen*
		• Application Insights – *Systemüberwachung, einschließlich Telemetrie und Protokollierung*
		• *SQL-Server – bietet Speicherung*
		• Kubernetes – *Open-Source-Container*
		
		Weitere Informationen und nähere Angaben zu diesen Microsoft-Produkten und -Services sind hier zu finden: https://azure.microsoft.com/en-us/services/.
		
		Zusätzlich nutzt PPS, Unit4 Localisation Services bzw. Apps Twilio – sendgrid- um Mails zu verschicken.

4. AUFBEWAHRUNGSFRIST

Der Auftragsverarbeiter bewahrt die personenbezogenen Daten **<u>während der Laufzeit des Vertrags</u>** 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

<table>
<tr><td>Produkt - Vor Ort</td><td colspan="4">Daten sind auf den Servern des Datenverantwortlichen in dessen Hauptniederlassung oder eingetragenem Geschäftssitz, wie Unit4 jeweils mitgeteilt werden kann, gespeichert.</td></tr>
<tr><td>Produkt - Unit4 SaaS</td><td colspan="4">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.
<table>
<tr><th>CLOUD-MODELL</th><th>GEOPOLITISCHE ZONE</th><th>STANDORT DES RECHENZENTRUMS</th><th>ANLAGE ODER PARTNERSCHAFT</th></tr>
<tr><td>SAAS CLOUD</td><td>EU</td><td>DUBLIN / AMSTERDAM</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>USA</td><td>MEHRERE STANDORTE</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>KANADA</td><td>TORONTO / QUEBEC CITY</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>VEREINIGTES KÖNIGREICH</td><td>LONDON / CARDIFF</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>ASIEN</td><td>SINGAPUR / HONGKONG</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>AUSTRALIEN</td><td>VICTORIA / NEW SOUTH WALES</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>NORWAY</td><td>OSLO / STAVANGER</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>SWEDEN (NORDICS)</td><td>SÄTRA AND SOLLENTUNA</td><td>CONPATO</td></tr>
</table></td></tr>
<tr><td>Produkt – Talent Management SaaS</td><td colspan="4">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.</td></tr>
<tr><td>Unit4 Support – Standardsupport und andere Standard-Supportleistungen</td><td colspan="4">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.
<table>
<tr><th>Standort des Kunden</th><th>Support wird vorrangig aus folgenden Standorten (die aber auch andere EU-Länder mit einschließen können) bereitgestellt:</th></tr>
<tr><td>Vereinigtes Königreich und Irland</td><td>Vereinigtes Königreich, Irland, Portugal und Polen.</td></tr>
<tr><td>Schweden, Norwegen, Dänemark, Finnland und Island</td><td>Polen, Portugal, Norwegen und Schweden.</td></tr>
<tr><td>USA & Kanada</td><td>Polen, Portugal, USA und Kanada.</td></tr>
<tr><td>Rest-Europa</td><td>Polen, Portugal und Deutschland.</td></tr>
<tr><td>APAC</td><td>Polen, Portugal und Singapur / Malaysia.</td></tr>
</table></td></tr>
<tr><td>Unit4 Support – Rund-um-die-Uhr-(24/7) Support</td><td colspan="4">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.</td></tr>
<tr><td>Unit4 Support – Nur-EU-Support</td><td colspan="4">Wird der Nur-EU-Support gewählt, erfolgt der Standard-Support nur innerhalb der oben aufgeführten EU-Standorte (während der Geschäftszeiten).</td></tr>
<tr><td>People-Plattform-Services („PPS“) (allgemein), einschließlich IDS und Wanda (sowie alle Supportleistungen); LOKALISATION SERVICES ODER APPS</td><td colspan="4">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.
<table>
<tr><th>Service</th><th>Geopolitische Zone</th><th>Ort, an dem der Service die Daten verarbeitet oder speichert</th><th>Support wird vorrangig aus folgenden Standorten bereitgestellt:</th></tr>
<tr><td>Wanda</td><td>Alle</td><td>Vorwiegend innerhalb der EU, aber unter Umständen auch andernorts, wo es Azure standorte gibt (z.B. USA).</td><td>EU-Länder, einschließlich Irland, Polen, Spanien Vereinigte Staaten und sonstiger globaler Support an anderen Standorten, sofern erforderlich</td></tr>
<tr><td>PPS, Lokalisation Services oder Apps</td><td>Anhängig vom Cloud-Einsatz</td><td>Verarbeitung und Datenspeicherung erfolgt in der ausgewählten</td><td>Wie oben für Unit4 SaaS</td></tr>
</table></td></tr>
</table>

			Geo-politischen Zone	
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 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 leergeräumten 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 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 bösartiger Aktivitäten folgt unser Vorfallreaktionsteam 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)	Mail Versand (EU SCCs – siehe Abschnitt 4)

ABSCHNITT 4 – EU-STANDARDVERTRAGSKLAUSELN

DURCHFÜHRUNGSBESCHLUSS (EU) 2021/914 DER KOMMISSION

vom 4. Juni 2021

über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates

---

ANHANG

STANDARDVERTRAGSKLAUSELN (Modul Zwei: Übermittlung von Verantwortlichen an Auftragsverarbeiter)

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) [(1)] bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

b) Die Parteien:

i) die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)“), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur“), und

ii) die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur“),

haben sich mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) einverstanden erklärt.

c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß Anhang I.B.

d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2

Wirkung und Unabänderbarkeit der Klauseln

a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 sowie — in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter — Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, sofern diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

b) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

Klausel 3

Drittbegünstigte

a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:

i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7

ii) Klausel 8 — Modul eins: Klausel 8.5 Buchstabe e und Klausel 8.9 Buchstabe b Modul zwei: Klausel 8.1 Buchstabe b, Klausel 8.9 Buchstaben a, c, d und e Modul drei: Klausel 8.1 Buchstaben a, c und d und Klausel 8.9 Buchstaben a, c, d, e, f und g Modul vier: Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe b

iii) Klausel 9 — Modul zwei: Klausel 9 Buchstaben a, c, d und e Modul drei: Klausel 9 Buchstaben a, c, d und e

iv) Klausel 12 — Modul eins: Klausel 12 Buchstaben a und d Module zwei und drei: Klausel 12 Buchstaben a, d und f

v) Klausel 13

vi) Klausel 15.1 Buchstaben c, d und e

vii) Klausel 16 Buchstabe e

viii) Klausel 18 — Module eins, zwei und drei Klausel 18 Buchstaben a und b Modul vier: Klausel 18

b) Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe a unberührt.

Klausel 4

Auslegung

a) Werden in diesen Klauseln in der Verordnung (EU) 2016/679 definierte Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in dieser Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die mit den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten im Widerspruch steht.

Klausel 5

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen von damit zusammenhängenden Vereinbarungen zwischen den Parteien, die zu dem Zeitpunkt bestehen, zu dem diese Klauseln vereinbart oder eingegangen werden, haben diese Klauseln Vorrang.

Klausel 6

Beschreibung der Datenübermittlung(en)

Die Einzelheiten der Datenübermittlung(en), insbesondere die Kategorien der übermittelten personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in Anhang I.B aufgeführt.

Klausel 7 — fakultativ

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung der Parteien jederzeit entweder als Datenexporteur oder als Datenimporteur beitreten, indem sie die Anlage ausfüllt und Anhang I.A unterzeichnet.

b) Nach Ausfüllen der Anlage und Unterzeichnung von Anhang I.A wird die beitretende Einrichtung Partei dieser Klauseln und hat die Rechte und Pflichten eines Datenexporteurs oder eines Datenimporteurs entsprechend ihrer Bezeichnung in Anhang I.A.

c) Für den Zeitraum vor ihrem Beitritt als Partei erwachsen der beitretenden Einrichtung keine Rechte oder Pflichten aus diesen Klauseln.

ABSCHNITT II — PFLICHTEN DER PARTEIEN

Klausel 8

Datenschutzgarantien

Der Datenexporteur versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Datenimporteur — durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen — in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen.

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

8.1. Weisungen

a) Der Datenimporteur verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs. Der Datenexporteur kann solche Weisungen während der gesamten Vertragslaufzeit erteilen.

b) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er diese Weisungen nicht befolgen kann.

8.2. Zweckbindung

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang I.B genannten spezifischen Zweck(e), sofern keine weiteren Weisungen des Datenexporteurs bestehen.

8.3. Transparenz

Auf Anfrage stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich der in Anhang II beschriebenen Maßnahmen und personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage zu diesen Klauseln vor der Weitergabe einer Kopie unkenntlich machen; er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen. Diese Klausel gilt unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

8.4. Richtigkeit

Stellt der Datenimporteur fest, dass die erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet er unverzüglich den Datenexporteur. In diesem Fall arbeitet der Datenimporteur mit dem Datenexporteur zusammen, um die Daten zu löschen oder zu berichtigen.

8.5. Dauer der Verarbeitung und Löschung oder Rückgabe der Daten

Die Daten werden vom Datenimporteur nur für die in Anhang I.B angegebene Dauer verarbeitet. Nach Wahl des Datenexporteurs löscht der Datenimporteur nach Beendigung der Erbringung der Datenverarbeitungsdienste alle im Auftrag des Datenexporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenexporteur, dass dies erfolgt ist, oder gibt dem Datenexporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist. Dies gilt unbeschadet von Klausel 14, insbesondere der Pflicht des Datenimporteurs gemäß Klausel 14 Buchstabe e, den Datenexporteur während der Vertragslaufzeit zu benachrichtigen, wenn er Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten oder gelten werden, die nicht mit den Anforderungen in Klausel 14 Buchstabe a im Einklang stehen.

8.6. Sicherheit der Verarbeitung

a) Der Datenimporteur und, während der Datenübermittlung, auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu diesen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann. Im Falle einer Pseudonymisierung verbleiben die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, soweit möglich, unter der ausschließlichen Kontrolle des Datenexporteurs. Zur Erfüllung seinen Pflichten gemäß diesem Absatz setzt der Datenimporteur mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen um. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

b) Der Datenimporteur gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Er gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

c) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung, darunter auch Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen. Zudem meldet der Datenimporteur dem Datenexporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde. Diese Meldung enthält die Kontaktdaten einer Anlaufstelle für weitere Informationen, eine Beschreibung der Art der Verletzung (soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), die wahrscheinlichen Folgen der Verletzung und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung etwaiger nachteiliger Auswirkungen. Wenn und soweit nicht alle Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

d) Unter Berücksichtigung der Art der Verarbeitung und der dem Datenimporteur zur Verfügung stehenden Informationen arbeitet der Datenimporteur mit dem Datenexporteur zusammen und unterstützt ihn dabei, seinen Pflichten gemäß der Verordnung (EU) 2016/679 nachzukommen, insbesondere die zuständige Aufsichtsbehörde und die betroffenen Personen zu benachrichtigen.

8.7. Sensible Daten

Soweit die Übermittlung personenbezogene Daten umfasst, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Datenimporteur die in Anhang I.B beschriebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

8.8. Weiterübermittlungen

Der Datenimporteur gibt die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs an Dritte weiter. Die Daten dürfen zudem nur an Dritte weitergegeben werden, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union [(4)] ansässig sind (im Folgenden „Weiterübermittlung"), sofern der Dritte im Rahmen des betreffenden Moduls an diese Klauseln gebunden ist oder sich mit der Bindung daran einverstanden erklärt oder falls

i) die Weiterübermittlung an ein Land erfolgt, für das ein Angemessenheitsbeschluss nach Artikel 45 der Verordnung (EU) 2016/679 gilt, der die Weiterübermittlung abdeckt,

ii) der Dritte auf andere Weise geeignete Garantien gemäß Artikel 46 oder Artikel 47 der Verordnung (EU) 2016/679 im Hinblick auf die betreffende Verarbeitung gewährleistet,

iii) die Weiterübermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich ist oder

iv) die Weiterübermittlung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Jede Weiterübermittlung erfolgt unter der Bedingung, dass der Datenimporteur alle anderen Garantien gemäß diesen Klauseln, insbesondere die Zweckbindung, einhält.

8.9. Dokumentation und Einhaltung der Klauseln

a) Der Datenimporteur bearbeitet Anfragen des Datenexporteurs, die sich auf die Verarbeitung gemäß diesen Klauseln beziehen, umgehend und in angemessener Weise.

b) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können. Insbesondere führt der Datenimporteur geeignete Aufzeichnungen über die im Auftrag des Datenexporteurs durchgeführten Verarbeitungstätigkeiten.

c) Der Datenimporteur stellt dem Datenexporteur alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesen Klauseln festgelegten Pflichten nachzuweisen; auf Verlangen des Datenexporteurs ermöglicht er diesem, die unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung zu prüfen, und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Datenexporteur einschlägige Zertifizierungen des Datenimporteurs berücksichtigen.

d) Der Datenexporteur kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Datenimporteurs umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der zuständigen Aufsichtsbehörde die unter den Buchstaben b und c genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

Klausel 9

Einsatz von Unterauftragsverarbeitern

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

a) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG. Der Datenimporteur besitzt die allgemeine Genehmigung des Datenexporteurs für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Datenimporteur unterrichtet den Datenexporteur mindestens [Zeitraum angeben] im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Datenexporteur damit ausreichend Zeit ein, um vor der Beauftragung des/der Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Datenimporteur stellt dem Datenexporteur die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b)Beauftragt der Datenimporteur einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Datenexporteurs), so muss diese Beauftragung im Wege eines schriftlichen Vertrags erfolgen, der im Wesentlichen dieselben Datenschutzpflichten vorsieht wie diejenigen, die den Datenimporteur gemäß diesen Klauseln binden, einschließlich im Hinblick auf Rechte als Drittbegünstigte für betroffene Personen. ([8]) Die Parteien erklären sich damit einverstanden, dass der Datenimporteur durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß Klausel 8.8 nachkommt. Der Datenimporteur stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Datenimporteur gemäß diesen Klauseln unterliegt.

c)Der Datenimporteur stellt dem Datenexporteur auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d)Der Datenimporteur haftet gegenüber dem Datenexporteur in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Datenimporteur geschlossenen Vertrag nachkommt. Der Datenimporteur benachrichtigt den Datenexporteur, wenn der Unterauftragsverarbeiter seinen Pflichten gemäß diesem Vertrag nicht nachkommt.

e)Der Datenimporteur vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Datenexporteur — sollte der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sein — das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

Klausel 10

Rechte betroffener Personen

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

a)Der Datenimporteur unterrichtet den Datenexporteur unverzüglich über jeden Antrag, den er von einer betroffenen Person erhalten hat. Er beantwortet diesen Antrag nicht selbst, es sei denn, er wurde vom Datenexporteur dazu ermächtigt.

b)Der Datenimporteur unterstützt den Datenexporteur bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 zu beantworten. Zu diesem Zweck legen die Parteien in Anhang II unter Berücksichtigung der Art der Verarbeitung die geeigneten technischen und organisatorischen Maßnahmen, durch die Unterstützung geleistet wird, sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

c) Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Datenimporteur die Weisungen des Datenexporteurs.

Klausel 11

Rechtsbehelf

a)Der Datenimporteur informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält.

[OPTION: Der Datenimporteur erklärt sich damit einverstanden, dass betroffene Personen eine Beschwerde auch bei einer unabhängigen Streitbeilegungsstelle ([11]) einreichen können, ohne dass für die betroffene Person Kosten entstehen. Er unterrichtet die betroffenen Personen in der unter Buchstabe a beschriebenen Weise über einen solchen Rechtsbehelfsmechanismus sowie darüber, dass sie nicht verpflichtet sind, davon Gebrauch zu machen oder bei der Einlegung eines Rechtsbehelfs eine bestimmte Reihenfolge einzuhalten.]

b)Im Falle einer Streitigkeit zwischen einer betroffenen Person und einer der Parteien bezüglich der Einhaltung dieser Klauseln bemüht sich die betreffende Partei nach besten Kräften um eine zügige gütliche Beilegung. Die Parteien halten einander über derartige Streitigkeiten auf dem Laufenden und bemühen sich gegebenenfalls gemeinsam um deren Beilegung.

c)Macht die betroffene Person ein Recht als Drittbegünstigte gemäß Klausel 3 geltend, erkennt der Datenimporteur die Entscheidung der betroffenen Person an,

i)eine Beschwerde bei der Aufsichtsbehörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts oder ihres Arbeitsorts oder bei der zuständigen Aufsichtsbehörde gemäß Klausel 13 einzureichen,

ii) den Streitfall an die zuständigen Gerichte im Sinne der Klausel 18 zu verweisen.

d)Die Parteien erkennen an, dass die betroffene Person von einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht gemäß Artikel 80 Absatz 1 der Verordnung (EU) 2016/679 vertreten werden kann.

e) Der Datenimporteur unterwirft sich einem nach geltendem Unionsrecht oder dem geltenden Recht eines Mitgliedstaats verbindlichen Beschluss.

f)Der Datenimporteur erklärt sich damit einverstanden, dass die Entscheidung der betroffenen Person nicht ihre materiellen Rechte oder Verfahrensrechte berührt, Rechtsbehelfe im Einklang mit geltenden Rechtsvorschriften einzulegen.

Klausel 12

Haftung

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

a) Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.

b) Der Datenimporteur haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenimporteur oder sein Unterauftragsverarbeiter der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt.

c) Ungeachtet von Buchstabe b haftet der Datenimporteur gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenexporteur oder der Datenimporteur (oder dessen Unterauftragsverarbeiter) der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs und, sofern der Datenexporteur ein im Auftrag eines Verantwortlichen handelnder Auftragsverarbeiter ist, unbeschadet der Haftung des Verantwortlichen gemäß der Verordnung (EU) 2016/679 oder gegebenenfalls der Verordnung (EU) 2018/1725.

d) Die Parteien erklären sich damit einverstanden, dass der Datenexporteur, der nach Buchstabe c für durch den Datenimporteur (oder dessen Unterauftragsverarbeiter) verursachte Schäden haftet, berechtigt ist, vom Datenimporteur den Teil des Schadenersatzes zurückzufordern, der der Verantwortung des Datenimporteurs für den Schaden entspricht.

e) Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.

f) Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Buchstabe e haftbar gemacht wird, berechtigt ist, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.

g) Der Datenimporteur kann sich nicht auf das Verhalten eines Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung entziehen.

Klausel 13

Aufsicht

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

a) [Wenn der Datenexporteur in einem EU-Mitgliedstaat niedergelassen ist:] Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt und einen Vertreter gemäß Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt hat:] Die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 niedergelassen ist, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt, ohne jedoch einen Vertreter gemäß Artikel 27 Absatz 2 der Verordnung (EU) 2016/679 benennen zu müssen:] Die Aufsichtsbehörde eines der Mitgliedstaaten, in denen die betroffenen Personen niedergelassen sind, deren personenbezogene Daten gemäß diesen Klauseln im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen übermittelt werden oder deren Verhalten beobachtet wird, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

b) Der Datenimporteur erklärt sich damit einverstanden, sich der Zuständigkeit der zuständigen Aufsichtsbehörde zu unterwerfen und bei allen Verfahren, mit denen die Einhaltung dieser Klauseln sichergestellt werden soll, mit ihr zusammenzuarbeiten. Insbesondere erklärt sich der Datenimporteur damit einverstanden, Anfragen zu beantworten, sich Prüfungen zu unterziehen und den von der Aufsichtsbehörde getroffenen Maßnahmen, darunter auch Abhilfemaßnahmen und Ausgleichsmaßnahmen, nachzukommen. Er bestätigt der Aufsichtsbehörde in schriftlicher Form, dass die erforderlichen Maßnahmen ergriffen wurden.

ABSCHNITT III — LOKALE RECHTSVORSCHRIFTEN UND PFLICHTEN IM FALLE DES ZUGANGS VON BEHÖRDEN ZU DEN DATEN

Klausel 14

Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe a insbesondere die folgenden Aspekte gebührend berücksichtigt haben:

i) die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,

ii) die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien, [(12)]

iii) alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

c)Der Datenimporteur versichert, dass er sich im Rahmen der Beurteilung nach Buchstabe b nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass er mit dem Datenexporteur weiterhin zusammenarbeiten wird, um die Einhaltung dieser Klauseln zu gewährleisten.

d)Die Parteien erklären sich damit einverstanden, die Beurteilung nach Buchstabe b zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

e)Der Datenimporteur erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Buchstabe a im Einklang stehen; hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen), die sich auf eine nicht mit den Anforderungen in Buchstabe a im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht. [In Bezug auf Modul drei: Der Datenexporteur leitet die Benachrichtigung an den Verantwortlichen weiter.]

f)Nach einer Benachrichtigung gemäß Buchstabe e oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur seinen Pflichten gemäß diesen Klauseln nicht mehr nachkommen kann, ermittelt der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit), die der Datenexporteur und/oder der Datenimporteur ergreifen müssen, um Abhilfe zu schaffen, [in Bezug auf Modul drei: gegebenenfalls in Absprache mit dem Verantwortlichen]. Der Datenexporteur setzt die Datenübermittlung aus, wenn er der Auffassung ist, dass keine geeigneten Garantien für eine derartige Übermittlung gewährleistet werden können, oder wenn er [in Bezug Modul drei: vom Verantwortlichen oder] von der dafür zuständigen Aufsichtsbehörde dazu angewiesen wird. In diesem Fall ist der Datenexporteur berechtigt, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß diesen Klauseln geht. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben. Wird der Vertrag gemäß dieser Klausel gekündigt, finden Klausel 16 Buchstaben d und e Anwendung.

Klausel 15

Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

15.1. Benachrichtigung

a)Der Datenimporteur erklärt sich damit einverstanden, den Datenexporteur und, soweit möglich, die betroffene Person (gegebenenfalls mit Unterstützung des Datenexporteurs) unverzüglich zu benachrichtigen,

i)wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß diesen Klauseln übermittelt werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder

ii)wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die gemäß diesen Klauseln übermittelt wurden; diese Benachrichtigung muss alle dem Datenimporteur verfügbaren Informationen enthalten.

[In Bezug auf Modul drei: Der Datenexporteur leitet die Benachrichtigung an den Verantwortlichen weiter.]

b)Ist es dem Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des Datenexporteurs nachweisen zu können.

c)Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Datenimporteur bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.). [In Bezug auf Modul drei: Der Datenexporteur leitet die Informationen an den Verantwortlichen weiter.]

d)Der Datenimporteur erklärt sich damit einverstanden, die Informationen gemäß den Buchstaben a bis c während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

e)Die Buchstaben a bis c gelten unbeschadet der Pflicht des Datenimporteurs gemäß Klausel 14 Buchstabe e und Klausel 16, den Datenexporteur unverzüglich zu informieren, wenn er diese Klauseln nicht einhalten kann.

15.2. Überprüfung der Rechtmäßigkeit und Datenminimierung

a)Der Datenimporteur erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der Pflichten des Datenimporteurs gemäß Klausel 14 Buchstabe e.

b)Der Datenimporteur erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung. [In Bezug auf Modul drei: Der Datenexporteur stellt die Beurteilung dem Verantwortlichen zur Verfügung.]

c)Der Datenimporteur erklärt sich damit einverstanden, bei der Beantwortung eines Offenlegungsersuchens auf der Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereitzustellen.

ABSCHNITT IV — SCHLUSSBESTIMMUNGEN

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 14 Buchstabe f.

c) Der Datenexporteur ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

i) der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Buchstabe b ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,

ii) der Datenimporteur in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder

iii) der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt.

In diesen Fällen unterrichtet der Datenexporteur die zuständige Aufsichtsbehörde [in Bezug auf Modul drei: und den Verantwortlichen] über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.

d) [In Bezug auf die Module eins, zwei und drei: Personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen nach Wahl des Datenexporteurs unverzüglich an diesen zurückgegeben oder vollständig gelöscht werden. Dies gilt gleichermaßen für alle Kopien der Daten.] [In Bezug auf Modul vier: Von dem in der EU ansässigen Datenexporteur erhobene personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen unverzüglich vollständig gelöscht werden, einschließlich aller Kopien.] Der Datenimporteur bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.

e) Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn i) die Europäische Kommission einen Beschluss nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird, an das die personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/679 gelten.

Klausel 17

Anwendbares Recht

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

Diese Klauseln unterliegen dem Recht eines der EU-Mitgliedstaaten, sofern dieses Recht Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht ist, das auf den Hauptvertrag Anwendung findet.

Klausel 18

Gerichtsstand und Zuständigkeit

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

a) Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.

b) Die Parteien vereinbaren, dass die die gemäß dem Hauptvertrag zuständigen Gerichte auch für Streitigkeiten, die sich aus diesen Klauseln ergeben, zuständig sind.

c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur auch vor den Gerichten des Mitgliedstaats erheben, in dem sie ihren gewöhnlichen Aufenthaltsort hat.

d) Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

---

(1) Handelt es sich bei dem Datenexporteur um einen Auftragsverarbeiter, der der Verordnung (EU) 2016/679 unterliegt und der im Auftrag eines Organs oder einer Einrichtung der Union als Verantwortlicher handelt, so gewährleistet der Rückgriff auf diese Klauseln bei der Beauftragung eines anderen Auftragsverarbeiters (Unterauftragsverarbeitung), der nicht unter die Verordnung (EU) 2016/679 fällt, ebenfalls die Einhaltung von Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39), insofern als diese Klauseln und die gemäß Artikel 29 Absatz 3 der Verordnung (EU) 2018/1725 im Vertrag oder in einem anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegten Datenschutzpflichten angeglichen sind. Dies ist insbesondere dann der Fall, wenn sich der Verantwortliche und der Auftragsverarbeiter auf die im Beschluss 2021/915 enthaltenen Standardvertragsklauseln stützen.

(2) Die Daten müssen in einer Weise anonymisiert werden, dass eine Person im Einklang mit Erwägungsgrund 26 der Verordnung (EU) 2016/679 nicht mehr identifizierbar ist; außerdem muss dieser Vorgang unumkehrbar sein.

(3) Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Das Datenschutzrecht der Union, darunter die Verordnung (EU) 2016/679, ist in das EWR-Abkommen einbezogen und wurde in Anhang XI aufgenommen. Daher gilt eine Weitergabe durch den Datenimporteur an einen im EWR ansässigen Dritten nicht als Weiterübermittlung im Sinne dieser Klauseln.

(4) Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Das Datenschutzrecht der Union, darunter die Verordnung (EU) 2016/679, ist in das EWR-Abkommen

einbezogen und wurde in Anhang XI aufgenommen. Daher gilt eine Weitergabe durch den Datenimporteur an einen im EWR ansässigen Dritten nicht als Weiterübermittlung im Sinne dieser Klauseln.

([5]) Siehe Artikel 28 Absatz 4 der Verordnung (EU) 2016/679 und, wenn es sich bei dem Verantwortlichen um ein Organ oder eine Einrichtung der Union handelt, Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725.

([6]) Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Das Datenschutzrecht der Union, darunter die Verordnung (EU) 2016/679, ist in das EWR-Abkommen einbezogen und wurde in Anhang XI aufgenommen. Daher gilt eine Weitergabe durch den Datenimporteur an einen im EWR ansässigen Dritten nicht als Weiterübermittlung im Sinne dieser Klauseln.

([7]) Hierzu zählt, ob die Übermittlung und Weiterverarbeitung personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen oder Straftaten enthalten.

([8]) Diese Anforderung ist gegebenenfalls vom Unterauftragsverarbeiter zu erfüllen, der diesen Klauseln gemäß Klausel 7 im Rahmen des betreffenden Moduls beitritt.

([9]) Diese Anforderung ist gegebenenfalls vom Unterauftragsverarbeiter zu erfüllen, der diesen Klauseln gemäß Klausel 7 im Rahmen des betreffenden Moduls beitritt.

([10]) Diese Frist kann um höchstens zwei weitere Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Datenimporteur unterrichtet die betroffene Person ordnungsgemäß und unverzüglich über eine solche Verlängerung.

([11]) Der Datenimporteur darf eine unabhängige Streitbeilegung über eine Schiedsstelle nur dann anbieten, wenn er in einem Land niedergelassen ist, das das New Yorker Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche ratifiziert hat.

([12]) Zur Ermittlung der Auswirkungen derartiger Rechtsvorschriften und Gepflogenheiten auf die Einhaltung dieser Klauseln können in die Gesamtbeurteilung verschiedene Elemente einfließen. Diese Elemente können einschlägige und dokumentierte praktische Erfahrungen im Hinblick darauf umfassen, ob es bereits früher Ersuchen um Offenlegung seitens Behörden gab, die einen hinreichend repräsentativen Zeitrahmen abdecken, oder ob es solche Ersuchen nicht gab. Dies betrifft insbesondere interne Aufzeichnungen oder sonstige Belege, die fortlaufend mit gebührender Sorgfalt erstellt und von leitender Ebene bestätigt wurden, sofern diese Informationen rechtmäßig an Dritte weitergegeben werden können. Sofern anhand dieser praktischen Erfahrungen der Schluss gezogen wird, dass dem Datenimporteur die Einhaltung dieser Klauseln nicht unmöglich ist, muss dies durch weitere relevante objektive Elemente untermauert werden; den Parteien obliegt die sorgfältige Prüfung, ob alle diese Elemente ausreichend zuverlässig und repräsentativ sind, um die getroffene Schlussfolgerung zu bekräftigen. Insbesondere müssen die Parteien berücksichtigen, ob ihre praktische Erfahrung durch öffentlich verfügbare oder anderweitig zugängliche zuverlässige Informationen über das Vorhandensein oder Nicht-Vorhandensein von Ersuchen innerhalb desselben Wirtschaftszweigs und/oder über die Anwendung der Rechtsvorschriften in der Praxis, wie Rechtsprechung und Berichte unabhängiger Aufsichtsgremien, erhärtet und nicht widerlegt wird.

ANLAGE

ERLÄUTERUNG:

Es muss möglich sein, die für jede Datenübermittlung oder jede Kategorie von Datenübermittlungen geltenden Informationen klar voneinander zu unterscheiden und in diesem Zusammenhang die jeweilige(n) Rolle(n) der Parteien als Datenexporteur(e) und/oder Datenimporteur(e) zu bestimmen. Dies erfordert nicht zwingend, dass für jede Datenübermittlung bzw. jede Kategorie von Datenübermittlungen und/oder für jedes Vertragsverhältnis getrennte Anlagen ausgefüllt und unterzeichnet werden müssen, sofern die geforderte Transparenz bei Verwendung einer einzigen Anlage erzielt werden kann. Erforderlichenfalls sollten getrennte Anlagen verwendet werden, um ausreichende Klarheit zu gewährleisten.

ANHANG I

A. LISTE DER PARTEIEN

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

Datenexporteur(e): [*Name und Kontaktdaten des Datenexporteurs/der Datenexporteure und gegebenenfalls seines/ihres Datenschutzbeauftragten und/oder Vertreters in der Europäischen Union*]

Wie in der Vereinbarung beschrieben.

Verarbeitungstätigkeit betreffend die Datenübermittlung gemäß dieser Klauseln:

Wie in der Vereinbarung beschrieben.

Rolle (Verantwortlicher/Auftragsverarbeiter):

Wie in der Vereinbarung beschrieben.

Datenimporteur(e): [*Name und Kontaktdaten des Datenexporteurs/der Datenimporteure, einschließlich jeder für den Datenschutz zuständigen Kontaktperson*]

Wie in der Vereinbarung beschrieben.

Verarbeitungstätigkeit betreffend die Datenübermittlung gemäß dieser Klauseln:

Wie in der Vereinbarung beschrieben.

Rolle (Verantwortlicher/Auftragsverarbeiter):

Wie in der Vereinbarung beschrieben.

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden

Wie in Klausel 1 und 3 der Datenverarbeitungsinformation beschrieben.

Kategorien der übermittelten personenbezogenen Daten

Wie in Klausel 1 und 3 der Datenverarbeitungsinformation beschrieben

Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

Wie in Klausel 1 und 3 der Datenverarbeitungsinformation beschrieben

Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden)

Wie in Klausel 1 und 3 der Datenverarbeitungsinformation beschrieben

Art der Verarbeitung

Wie in Klausel 1 und 3 der Datenverarbeitungsinformation beschrieben

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Wie in Klausel 1 und 3 der Datenverarbeitungsinformation beschrieben

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

Wie in Klausel 1 und 3 der Datenverarbeitungsinformation beschrieben

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

Wie in Klausel 1 und 3 der Datenverarbeitungsinformation beschrieben

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

Die zuständige Aufsichtsbehörde ist die niederländische Behörde:

"De Autoriteit Persoonsgegevens".

(Sofern unter Klausel 13 nicht anders erforderlich).

ANHANG II

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret (nicht allgemein) beschrieben werden. Beachten Sie hierzu bitte auch die allgemeine Erläuterung auf der ersten Seite der Anlage; insbesondere ist klar anzugeben, welche Maßnahmen für jede Datenübermittlung bzw. jede Kategorie von Datenübermittlungen gelten.

Beschreibung der von dem/den Datenimporteur(en) ergriffenen technischen und organisatorischen Maßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter zur Unterstützung des Verantwortlichen und (bei Datenübermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter) zur Unterstützung des Datenexporteurs ergreifen muss.

Wie in Klausel 2 der Datenverarbeitungsinformation beschrieben

---

ANHANG III

LISTE DER UNTERAUFTRAGSVERARBEITER

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

ERLÄUTERUNG:

Dieser Anhang muss für die Module zwei und drei im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 9 Buchstabe a, **Option 1**).

N/A