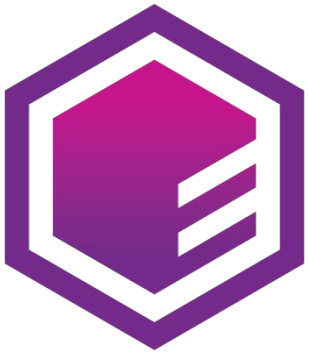

ENTRUST

GLOBALE POLITIK ZUM SCHUTZ PERSONENBEZOGENER DATEN

Dokumentenversion	1.4
Datum	10. Dezember 2021

Inhalt

1. Einführung

Als Unternehmen und Arbeitgeber ist es für die Entrust Corporation und ihre Tochtergesellschaften und verbundenen Unternehmen (zusammen "Entrust" oder das "Unternehmen") erforderlich, personenbezogene Daten über unsere Mitarbeiter, Zeitarbeitskräfte, Kunden, Lieferanten und andere Dritte, die wir mit der Bereitstellung von Produkten oder Dienstleistungen in unserem Namen beauftragen, zu erfassen, zu speichern und zu verarbeiten.

Mit der Einführung der Europäischen Datenschutzgrundverordnung ("GDPR") am 25. Mai 2018 und anderen geltenden Gesetzen zum Datenschutz unterliegen wir erhöhten Anforderungen hinsichtlich der Erhebung, Verwendung und Speicherung personenbezogener Daten.

2. Zweck

Der Zweck dieser Richtlinie ist es, uns allen zu helfen, unsere rechtlichen Verpflichtungen zu erfüllen und es den Personen, über die wir persönliche Daten besitzen, zu ermöglichen, Vertrauen in uns zu haben. Diese Richtlinie gilt für alle Mitarbeiter von Entrust, externe Mitarbeiter und Dritte, die Daten im Auftrag von Entrust verarbeiten. Sofern nicht anders angegeben, gilt diese Richtlinie in allen Ländern, in denen Entrust tätig ist und/oder Geschäfte tätigt.

3. Anforderungen der Richtlinie

3.1 Definitionen

"Data Controller" oder **"Personally Identifiable Information Controller (PII Controller)"** bezeichnet die Stelle, die den Zweck und die Mittel der Verarbeitung personenbezogener Daten bestimmt.

"Datenverarbeiter" oder **"Verarbeiter personenbezogener Daten (PII-Verarbeiter)"** bezeichnet die Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.

"Datenschutzgesetze" bezeichnet alle anwendbaren Datenschutzgesetze und -vorschriften, einschließlich, aber nicht beschränkt auf die Allgemeine Datenschutzverordnung der EU (GDPR), die Allgemeine Datenschutzverordnung des Vereinigten Königreichs (UK GDPR), den kanadischen Personal Information Protection and Electronic Documents Act (PIPEDA) und den California Consumer Privacy Act (CCPA)

"Betroffene Person" oder **"Principal of Personally Identifiable Information (PII Principal)"** bezeichnet die identifizierte oder identifizierbare Person oder den Haushalt, auf den sich die personenbezogenen Daten beziehen.

"Datennutzer" ist ein Begriff, der verwendet wird, um jeden Angestellten, Berater, unabhängigen Auftragnehmer, Praktikanten, Zeitarbeiter oder Dritten zu beschreiben, der im

Namen von Entrust handelt (einschließlich Datenverarbeiter) und dessen Arbeit die Verarbeitung personenbezogener Daten für Entrust beinhaltet

"Personenbezogene Daten" hat die Bedeutung von "persönlich identifizierbaren Informationen", "persönlichen Informationen", "persönlichen Daten" oder gleichwertigen Begriffen, wie sie in den Datenschutzgesetzen definiert sind

"Vorfall mit personenbezogenen Daten" hat die Bedeutung, die die Datenschutzgesetze den Begriffen "Sicherheitsvorfall", "Sicherheitsverletzung" oder "Verletzung des Schutzes personenbezogener Daten" zuweisen, und umfasst jede Situation, in der der Verkäufer Kenntnis davon erlangt, dass personenbezogene Daten von unbefugten Personen in unbefugter Weise eingesehen, offengelegt, verändert, verloren, zerstört oder verwendet wurden oder werden könnten

"Verarbeitung" ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die organisatorische Strukturierung, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung Die Verarbeitung umfasst auch die Übermittlung oder Weitergabe personenbezogener Daten an Dritte.

"Daten der besonderen Kategorie" oder **"Special Category Personal Information"** ist eine Untergruppe der personenbezogenen Daten und bezieht sich auf Informationen über die Rasse oder ethnische Herkunft, das Sexualleben oder die sexuelle Ausrichtung, politische Meinungen, religiöse oder philosophische Überzeugungen, die Mitgliedschaft in einer Gewerkschaft, genetische Daten, biometrische Daten (Augenfarbe, Haarfarbe, Größe, Gewicht), die medizinische Vorgeschichte oder strafrechtliche Verurteilungen und Straftaten oder damit verbundene Sicherheitsmaßnahmen.

3.2 Unsere Verantwortung

Je nach den Umständen kann Entrust als für die Datenverarbeitung Verantwortlicher oder als Datenverarbeiter handeln. Als für die Datenverarbeitung Verantwortlicher ist Entrust für die Einführung von Praktiken und Richtlinien im Einklang mit den Datenschutzgesetzen verantwortlich. Ebenso wichtig ist es, dass Entrust die Einhaltung dieser Gesetze nachweisen kann. Das Unternehmen tut dies durch:

- Umsetzung von Richtlinien, die es dem Unternehmen ermöglichen, die Datenschutzgesetze einzuhalten, wie z.B. diese Richtlinie, Richtlinien zur Aufbewahrung von Dokumenten und zur Datensicherheit sowie die Datenschutzerklärungen von Entrust;
- Unterrichtung und Schulung von Mitarbeitern, Zeitarbeitskräften und Dritten, die im Namen von Entrust handeln, über die Datenschutzanforderungen;
- Untersuchung von Fällen der Nichteinhaltung der Datenschutzrichtlinien von Entrust und Einleitung geeigneter Abhilfemaßnahmen und/oder Disziplinarmaßnahmen;

- Untersuchung, Behebung und, in einigen Fällen, Benachrichtigung über einen Vorfall mit personenbezogenen Daten;
- Durchführung von Folgenabschätzungen für die Datenverarbeitung, wenn dies für neue Arten von Verarbeitungstätigkeiten erforderlich ist;
- Durchführung regelmäßiger interner Audits der Datenschutzpolitik und -verfahren von Entrust; und
- Berücksichtigung des Datenschutzes bereits zu Beginn der Entwicklung neuer Produkte.

3.3 Verarbeitung personenbezogener Daten

Alle personenbezogenen Daten, die das Unternehmen verarbeitet oder die im Auftrag von Entrust verarbeitet werden, müssen:

- Auf faire, rechtmäßige und transparente Weise verarbeitet werden;
- Sie dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet werden;
- Sie müssen sachdienlich sein und sich auf das beschränken, was für den/die rechtmäßigen Zweck(e), für den/die die Daten verarbeitet werden, erforderlich ist;
- Sie müssen sachlich richtig sein und auf dem neuesten Stand gehalten werden, wobei sicherzustellen ist, dass unzutreffende personenbezogene Daten unverzüglich gelöscht oder berichtigt werden, soweit dies nach vernünftigem Ermessen möglich ist;
- Nicht länger aufbewahrt werden, als es für die Erfüllung des Zwecks/der Zwecke, für den/die die Daten erhoben wurden, erforderlich ist; und
- In einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung, versehentlichem Verlust, Zerstörung oder Beschädigung.

3.4 Verarbeitung sensibler Daten und besonderer Kategorien

Entrust verarbeitet im Auftrag von Kollegen sensible Informationen in verschiedenen Geschäftssystemen und begrenzte Daten besonderer Kategorien in Workday. Angemessene Kontrollen sind vorhanden und in den DPIAs für Daten der Sonderkategorie, Leistungen und Gehaltsabrechnung sowie im Zugriffskontrollstandard für sensible Daten und Daten der Sonderkategorie beschrieben, die auf der Entrust Compliance-Website verfügbar sind.

3.5 Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

Das Unternehmen darf personenbezogene Daten nur verarbeiten, wenn dies nach den Datenschutzgesetzen zulässig ist. Nachstehend sind die Gründe aufgeführt, auf die sich Entrust bei der Verarbeitung personenbezogener Daten stützt:

Wo die Verarbeitung notwendig ist:

- Zur Erfüllung eines Vertrags, an dem die betroffene Person beteiligt ist, oder um auf Antrag der betroffenen Person vor Abschluss eines Vertrags Maßnahmen zu ergreifen;

- Zur Erfüllung einer gesetzlichen Verpflichtung, der Entrust unterliegt, insbesondere rechtliche Anfragen von Strafverfolgungsbehörden; und/oder
- Zur Verfolgung der berechtigten Interessen von Entrust, es sei denn, diese Interessen überwiegen die Interessen oder Grundrechte und -freiheiten der betroffenen Person.

Zusätzlich zu diesen Gründen kann Entrust personenbezogene Daten auch dann verarbeiten, wenn die betroffene Person in die Verarbeitung für einen oder mehrere bestimmte Zwecke eingewilligt hat, sofern die Einwilligung ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unter unmissverständlicher Angabe des Willens der betroffenen Person erteilt wurde. Wenn Entrust die Verarbeitung mit einer Einwilligung begründet, hat die betroffene Person das Recht, ihre Einwilligung jederzeit und aus beliebigen Gründen zu widerrufen.

Gelegentlich kann es erforderlich sein, dass Entrust besondere Kategorien personenbezogener Daten von Kunden, Angestellten oder befristet Beschäftigten verarbeitet (z. B. wenn dies aufgrund sicherer Beschäftigungspraktiken erforderlich ist). Wenn Entrust besondere Kategorien personenbezogener Daten verarbeitet oder einen Dritten mit der Verarbeitung in seinem Namen beauftragt, stellt Entrust gegebenenfalls sicher, dass die folgenden Bedingungen erfüllt sind:

- Die betroffene Person hat ihre ausdrückliche Einwilligung zur Verarbeitung der besonderen Kategorie personenbezogener Daten für einen oder mehrere bestimmte Zwecke gegeben;
- Die Verarbeitung ist zur Erfüllung arbeitsrechtlicher, sozialversicherungsrechtlicher oder tarifvertraglicher Verpflichtungen erforderlich;
- Die Verarbeitung ist für die Zwecke der Präventiv- oder Arbeitsmedizin oder für die Beurteilung der Arbeitsfähigkeit eines Arbeitnehmers erforderlich;
- Die Verarbeitung ist zur Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich, wenn die betroffene Person aus physischen oder rechtlichen Gründen nicht in der Lage ist, ihre Einwilligung zu geben;
- Die Verarbeitung bezieht sich auf personenbezogene Daten, die von der betroffenen Person öffentlich gemacht wurden; und/oder
- Die Verarbeitung ist für die Begründung oder Verteidigung von Rechtsansprüchen erforderlich.

3.6 Verwaltung von Datensätzen

Entrust führt ein zentrales Verzeichnis der Arten von personenbezogenen Daten, die das Unternehmen erhebt, und der Gründe, warum diese Daten erhoben werden. Entrust verarbeitet personenbezogene Daten nur für den/die im zentralen Datensatz angegebenen Zweck(e) oder für andere Zwecke, die nach den Datenschutzgesetzen ausdrücklich zulässig sind. Entrust unterrichtet die betroffenen Personen über diese Zwecke, wenn die Daten erstmals erhoben werden oder, falls dies nicht möglich ist, so bald wie möglich danach.

Entrust wird personenbezogene Daten nur in dem Umfang verarbeiten, der für die der betroffenen Person mitgeteilten Zwecke erforderlich ist. Dies bedeutet, dass Entrust nicht mehr personenbezogene Daten erfragen oder in seinen Systemen speichern darf, als erforderlich sind. Das Unternehmen verfügt über geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass personenbezogene Daten, die nicht mehr benötigt werden, gelöscht oder vernichtet werden.

Das Unternehmen ergreift außerdem angemessene Maßnahmen, um sicherzustellen, dass alle gespeicherten personenbezogenen Daten korrekt und auf dem neuesten Stand sind. Entrust ist bestrebt, die Richtigkeit aller personenbezogenen Daten zum Zeitpunkt der Erhebung und danach in regelmäßigen Abständen zu überprüfen. Das Unternehmen ergreift alle angemessenen Maßnahmen, um unrichtige oder veraltete Daten unverzüglich und in jedem Fall innerhalb eines Monats nach dem Antrag der betroffenen Person zu löschen, zu vernichten oder zu berichtigen (bzw. bis zu drei Monate, wenn es besondere Gründe gibt, warum ein Monat nicht möglich ist).

Weitere Informationen zur Verwaltung und Aufbewahrung von Aufzeichnungen finden Sie in der Richtlinie zur globalen Verwaltung von Aufzeichnungen und dem dazugehörigen Anhang zur Aufbewahrung von Aufzeichnungen.

3.7 Löschung oder Vernichtung von personenbezogenen Daten

Papierunterlagen, die personenbezogene Daten enthalten, müssen geschreddert und sicher entsorgt werden, wenn sie nicht mehr aufbewahrt werden müssen. *Papierunterlagen, die personenbezogene Daten enthalten, dürfen nicht auf andere Weise entsorgt werden.*

Bei der Löschung elektronischer personenbezogener Daten sollten alle möglichen Schritte unternommen werden, um die fraglichen Daten unbrauchbar zu machen. Ist es nicht möglich, personenbezogene Daten vollständig zu löschen, müssen angemessene Schritte unternommen werden, um sicherzustellen, dass die Daten so vollständig wie möglich gelöscht werden.

Die IT-Abteilung ist für die Vernichtung oder Löschung von elektronischen Geräten verantwortlich, die personenbezogene Daten enthalten (z. B. Laptops, Desktops, firmeneigene mobile Geräte und Arbeitsdaten auf BYOD-Geräten).

3.8 Informationssicherheit

Wenn das Unternehmen personenbezogene Daten verarbeitet, ergreift es angemessene Maßnahmen, um sicherzustellen, dass die Daten sicher bleiben und gegen unbefugte oder unrechtmäßige Verarbeitung, versehentlichen Verlust, Zerstörung oder Beschädigung geschützt sind. Entrust tut dies durch:

- Verschlüsselung personenbezogener Daten, soweit möglich und angemessen;
- Gewährleistung der ständigen Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit der Systeme und Dienste, die zur Verarbeitung personenbezogener Daten verwendet werden;

- Sicherstellung der rechtzeitigen Wiederherstellung des Zugangs zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls; und
- Erleichterung der Prüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit.

Bei der Bewertung des angemessenen Sicherheitsniveaus berücksichtigt Entrust die mit der Verarbeitung verbundenen Risiken, insbesondere die Risiken der versehentlichen oder unrechtmäßigen Zerstörung, des Verlusts, der Veränderung, der unbefugten Weitergabe oder des Zugriffs auf die verarbeiteten personenbezogenen Daten.

Soweit Entrust Dritte mit der Verarbeitung personenbezogener Daten in seinem Auftrag beauftragt, tun diese dies auf der Grundlage schriftlicher Weisungen, sind zur Vertraulichkeit verpflichtet und haben angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Personenbezogene Daten dürfen nicht an Personen außerhalb von Entrust oder an autorisierte Dritte weitergegeben werden.

Schreibtische und Schränke werden verschlossen, wenn sie persönliche Daten oder vertrauliche Informationen jeglicher Art enthalten. Die Datennutzer stellen sicher, dass auf den einzelnen Monitoren/Bildschirmen keine persönlichen Daten oder vertraulichen Informationen für Passanten sichtbar sind und dass sie sich von ihren Computern/Tablets abmelden oder diese abschließen, wenn sie unbeaufsichtigt sind.

3.9 Meldung eines Vorfalls mit personenbezogenen Daten

Ein Vorfall mit personenbezogenen Daten kann auf verschiedene Weise eintreten, unter anderem:

- Verlust eines mobilen Geräts oder einer ausgedruckten Datei, die personenbezogene Daten enthält (z. B. wenn ein Gerät versehentlich in einem öffentlichen Verkehrsmittel zurückgelassen wird);
- Diebstahl eines mobilen Geräts oder einer ausgedruckten Datei, die personenbezogene Daten enthält (z. B. aus einem Fahrzeug oder einer Wohnung gestohlen);
- Menschliches Versagen (z. B. wenn ein Mitarbeiter versehentlich eine E-Mail mit personenbezogenen Daten an einen unbeabsichtigten Empfänger sendet oder versehentlich personenbezogene Daten ändert oder löscht);
- Cyberangriff (z. B. Öffnen eines E-Mail-Anhangs von einem unbekannten Dritten, der Ransomware oder andere Malware enthält);
- Erlauben von unbefugter Nutzung/Zugang (z.B. Erlauben des Zugangs unbefugter Dritter zu sicheren Bereichen der Büros oder Systeme von Entrust);
- Unvorhergesehene Umstände wie ein Brand oder eine Überschwemmung; oder
- Wenn ein Dritter durch Täuschung Informationen von Entrust erhalten hat.

Zu den Anzeichen, die auf einen Vorfall mit personenbezogenen Daten hindeuten, gehören die folgenden:

- Ungewöhnliche Anmeldung und/oder übermäßige Systemaktivität, insbesondere in Bezug auf aktive Benutzerkonten;
- Ungewöhnliche Fernzugriffsaktivitäten;
- Das Vorhandensein von gefälschten drahtlosen (Wi-Fi-)Netzen, die von der Arbeitsumgebung von Entrust aus sichtbar oder zugänglich sind;
- Ausfall der Ausrüstung; und
- Hardware- oder Software-Schlüssellogger, die an Entrust-Systeme angeschlossen oder darauf installiert sind.

Kollegen, die Kenntnis von einem Vorfall mit personenbezogenen Daten erhalten oder Grund zu der Annahme haben, dass ein solcher Vorfall eingetreten ist oder bevorsteht, müssen unverzüglich das Entrust Security Operation Center per E-Mail unter SOC@entrust.com und den Compliance Director unter privacy@entrust.comkontaktieren.

3.10 Reaktionsplan bei Vorfällen mit personenbezogenen Daten

Im Falle eines tatsächlichen oder drohenden Vorfalls mit personenbezogenen Daten ergreift Entrust schnelle Maßnahmen, um die Auswirkungen des Vorfalls zu minimieren und meldet den Vorfall, wenn dies gesetzlich vorgeschrieben ist. In den meisten Fällen wird die Antwort lauten:

- Untersuchung des Vorfalls, um die Art, die Ursache und das Ausmaß des entstandenen Schadens zu ermitteln;
- Durchführung der erforderlichen Maßnahmen, um zu verhindern, dass der Vorfall weitergeht oder sich wiederholt, und um den Schaden für die betroffenen Personen zu begrenzen;
- Beurteilung, ob eine Verpflichtung besteht, andere Parteien (z. B. nationale Datenschutzbehörden, betroffene Personen) zu benachrichtigen und diese Benachrichtigungen vorzunehmen. Wenn eine Verpflichtung zur Benachrichtigung der Datenschutzbehörden besteht, muss die Meldung in der Regel innerhalb von 72 Stunden erfolgen, nachdem das Unternehmen oder einer seiner Mitarbeiter von dem Vorfall Kenntnis erlangt hat; und
- Aufzeichnung von Informationen über den Vorfall mit personenbezogenen Daten und die daraufhin unternommenen Schritte, einschließlich einer Dokumentation, in der die Entscheidung für oder gegen eine Benachrichtigung erläutert wird.

3.11 Speicherung und Sicherung von personenbezogenen Daten

Entrust nutzt mehrere Serverstandorte zur Speicherung und Sicherung von personenbezogenen Daten. Weitere Informationen zu von Dritten genutzten Serverstandorten, die von Entrust mit der Verarbeitung personenbezogener Daten im Namen von Mitarbeitern und Kunden beauftragt werden, finden Sie in den entsprechenden Datenschutz-Folgenabschätzungen für personenbezogene Mitarbeiterdaten und auf der Seite „Externe Unterauftragsverarbeiter“ sowie den produktbezogenen Datenschutzhinweisen für personenbezogene Kundendaten. Diese Dokumente finden Sie entweder intern auf der Seite Compliance oder extern auf der Seite Rechtliches & Compliance unter den Symbolen zum Datenschutz. Für eine aktuelle Liste der

Standorte von unternehmenseigenen Datenservern wenden sich Mitarbeiter bitte direkt an die IT-Abteilung.

3.12 Internationale Datenübermittlung und Übermittlung an Dritte

Gemäß der DSGVO kann Entrust personenbezogene Daten in Länder außerhalb des Europäischen Wirtschaftsraums ("EWR") übermitteln, wenn in diesem Land ein angemessenes Schutzniveau besteht oder wenn Entrust geeignete Maßnahmen zur Gewährleistung des Datenschutzes ergriffen hat.

Unternehmen innerhalb der Entrust-Gruppe (d.h. alle Körperschaften und Tochtergesellschaften) müssen die konzerninterne Datenübertragungsvereinbarung abschließen, um angemessene Garantien für die Übermittlung personenbezogener Daten außerhalb des EWR, aber innerhalb der Entrust-Gruppe zu gewährleisten.

Unternehmen außerhalb der Entrust-Gruppe, die personenbezogene Daten für oder im Namen von Entrust verarbeiten und für die Entrust als Datenverantwortlicher oder Datenverarbeiter tätig ist, müssen mit Entrust eine Datenverarbeitungsvereinbarung abschließen, um angemessene Garantien für die Übermittlung personenbezogener Daten außerhalb des EWR zu gewährleisten. Diese Vereinbarung enthält Formulierungen, die sicherstellen, dass der Dritte geeignete technische und organisatorische Maßnahmen ergreift, um die DSGVO einzuhalten und den Schutz der Rechte der betroffenen Personen zu gewährleisten.

Zu den Fällen, in denen Entrust personenbezogene Daten in ein Land außerhalb des EWR übermittelt, gehören:

- Die betroffene Person hat der vorgeschlagenen Übermittlung ausdrücklich zugestimmt, nachdem Entrust sie über mögliche Risiken im Zusammenhang mit einer solchen Übermittlung (z. B. das Fehlen gleichwertiger Garantien in diesem Land) informiert hat;
- Die Übermittlung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für Maßnahmen erforderlich, die auf Antrag der betroffenen Person vor Abschluss eines Vertrags getroffen werden;
- Die Übermittlung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen Person zu schützen, wenn die betroffene Person aus physischen oder rechtlichen Gründen nicht in der Lage ist, ihre Einwilligung zu geben; oder
- Die Übermittlung ist für die Begründung oder Verteidigung eines Rechtsanspruchs erforderlich.

Bei jeder Übermittlung von Daten in Länder außerhalb des EWR stützt sich Entrust auf die von der Europäischen Kommission festgelegten Standardvertragsklauseln (2001/497/EG, 2004/915/EG und 2010/87/EU).[1] Beachten Sie, dass eine Datenübertragungsvereinbarung auch erforderlich ist, wenn personenbezogene Daten außerhalb Kanadas übertragen werden.

[1] Ab dem 27. Dezember 2022 werden diese Übermittlungen unter Verwendung der neuen Standardvertragsklauseln erfolgen, die im Durchführungsbeschluss (EU) 2021/914 der Kommission vom

3.13 Benachrichtigung der betroffenen Personen

Entrust ist verpflichtet, die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten zu informieren. Diese Informationen sind in der Datenschutzerklärung des Unternehmens enthalten, die öffentlich zugänglich ist unter www.entrust.com, in der Datenschutzerklärung für Bewerber, die öffentlich zugänglich ist unter https://www.entrust.com/legal-compliance/data-privacy/job-applicant-privacy-statement, und in der Datenschutzerklärung für Mitarbeiter, die im Intranet von Entrust verfügbar ist. Solche Aussagen liefern Informationen über:

- Die Arten von personenbezogenen Daten, die Entrust verarbeitet;
- Der Zweck und die Rechtsgrundlage für die Verarbeitung personenbezogener Daten;
- Ob personenbezogene Daten im Zuge der Verarbeitung an Dritte weitergegeben werden;
- Ob personenbezogene Daten außerhalb des EWR und Kanadas übermittelt werden und, falls ja, welche Schutzmaßnahmen getroffen werden;
- Wie lange die personenbezogenen Daten verarbeitet werden oder, falls dies nicht möglich ist, die Kriterien, nach denen das Unternehmen die Dauer der Verarbeitung bestimmt;
- Wie kann die betroffene Person eine Kopie ihrer bei Entrust gespeicherten personenbezogenen Daten erhalten?
- Rechte der betroffenen Person, einschließlich der Möglichkeit, eine Beschwerde einzureichen;
- Falls die personenbezogenen Daten zur Erfüllung eines Gesetzes oder eines Vertrags verarbeitet werden müssen, die möglichen Folgen, wenn die betroffene Person die Daten nicht zur Verfügung stellt oder der Verarbeitung widerspricht; und
- Gegebenenfalls das Vorhandensein und die Einzelheiten automatisierter Entscheidungsprozesse.

Wenn Entrust personenbezogene Daten über eine betroffene Person von einem Dritten erhält, wird das Unternehmen der betroffenen Person auch Informationen darüber geben:

- Die Art der von der dritten Partei erhaltenen personenbezogenen Daten und
- Die Quelle der Daten und ob sie aus einer öffentlich zugänglichen Quelle stammen (z. B. einer öffentlich zugänglichen Website).

3.14 Privacy by Design und Datenschutz-Folgenabschätzungen

Die Datenschutzgesetze verpflichten Entrust, den Datenschutz bereits in der Entwicklungsphase eines neuen Produktangebots zu berücksichtigen. Um dieser Verpflichtung nachzukommen, muss Entrust Maßnahmen ergreifen, um sicherzustellen, dass der

4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ( ) beschrieben sind.

Datenschutz Teil des Designprozesses ist und die Erhebung personenbezogener Daten so weit wie möglich minimiert wird.

Unter bestimmten Umständen (nämlich wenn die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten einer Person mit sich bringen würde) kann Entrust verpflichtet sein, eine förmliche Datenschutz-Folgenabschätzung (DPIA) in Bezug auf die Verarbeitung personenbezogener Daten durchzuführen. Eine solche Bewertung beinhaltet die Dokumentation der Zwecke, für die die Tätigkeit durchgeführt wird, die Art und Weise, wie Entrust die Datenschutzgesetze einhält und wie das Unternehmen potenzielle Risiken für die Privatsphäre des Einzelnen abschwächt. Wenn Sie der Meinung sind, dass eine Datenschutz-Folgenabschätzung erforderlich sein könnte, wenden Sie sich bitte an den Compliance Director unter privacy@entrust.com.

3.15 Rechte der betroffenen Personen

Wenn Entrust personenbezogene Daten verarbeitet, hat die betroffene Person gemäß den Datenschutzgesetzen das Recht auf:

- Auskunft über die zu ihrer Person gespeicherten Daten zu verlangen;
- Unrichtige personenbezogene Daten über sie berichtigen und unvollständige personenbezogene Daten ergänzen zu lassen, sofern Entrust feststellt, dass die Daten tatsächlich unrichtig oder unvollständig sind;
- Der Verarbeitung ihrer personenbezogenen Daten durch Entrust zu widersprechen, wenn das Unternehmen dies in Verfolgung seiner eigenen berechtigten Interessen tut. Entrust kann die personenbezogenen Daten trotz eines Widerspruchs weiterverarbeiten, wenn die berechtigten Interessen des Unternehmens die Interessen der betroffenen Person überwiegen oder wenn Entrust dies zur Geltendmachung oder Verteidigung von Rechtsansprüchen tun muss;
- Entrust auffordern, die über die betroffene Person gespeicherten personenbezogenen Daten zu vernichten. Das Unternehmen kann diesen Antrag ablehnen, wenn die personenbezogenen Daten für die Zwecke, für die sie verarbeitet werden, weiterhin erforderlich sind und es für Entrust eine rechtmäßige Grundlage für die weitere Verarbeitung gibt;
- Von Entrust verlangen, dass die Verarbeitung ihrer personenbezogenen Daten auf die Speicherung beschränkt wird. Dies ist nur möglich, wenn die Richtigkeit der personenbezogenen Daten angefochten wurde und ungeprüft bleibt, wenn Entrust die personenbezogenen Daten nicht mehr benötigt, die betroffene Person sie aber zur Geltendmachung oder Verteidigung von Rechtsansprüchen benötigt, wenn die betroffene Person Widerspruch gegen die Verarbeitung personenbezogener Daten eingelegt hat und wenn Entrust entscheidet, ob ihre berechtigten Interessen die Interessen der betroffenen Person überwiegen oder ob die Verarbeitung unrechtmäßig ist.

Entrust prüft die Rechte der betroffenen Person nach den geltenden Datenschutzgesetzen von Fall zu Fall, um zu entscheiden, wie einem Antrag auf Auskunft über die Daten der betroffenen Person entsprochen werden kann. Im Allgemeinen wird Entrust die Rechte einer betroffenen

Person nach der europäischen DSGVO als Grundlage für die Bearbeitung von Anfragen verwenden und die Rechte nach den geltenden Datenschutzgesetzen anwenden, soweit diese für die betroffene Person vorteilhafter sind. Macht eine betroffene Person von diesen Rechten Gebrauch und hat Entrust die betreffenden personenbezogenen Daten an einen Dritten weitergegeben, so wird das Unternehmen sein Bestes tun, um sicherzustellen, dass der Dritte die Wünsche der betroffenen Person ebenfalls beachtet.

3.16 Rechte der betroffenen Person auf Zugang zu den Daten

Betroffene Personen, die Auskunft über die von Entrust über sie gespeicherten personenbezogenen Daten verlangen möchten, können dies unter Data Subject Access Request (DSAR)tun. Wenn Kolleginnen und Kollegen direkt eine Anfrage erhalten (ob mündlich oder schriftlich), leiten Sie die Einzelheiten der Anfrage unverzüglich an privacy@entrust.comweiter. Eine umfassendere Auflistung der einzelnen Rechte der betroffenen Personen nach Gerichtsbarkeit finden Sie im Verfahren für Zugriffsanforderungen durch betroffene Personen auf der Compliance-Seite.

3.17 Schulung

Entrust bietet seinen Mitarbeitern und Zeitarbeitskräften Zugang zu Schulungen über die Verantwortung für den Datenschutz. Diese Schulung erfolgt bei der Einstellung und danach in regelmäßigen Abständen.

3.18 Aufsichtsbehörden

Die Kontaktinformationen für die zuständigen Datenaufsichtsbehörden variieren je nach Standort. Die Liste der Organe des Europäischen Datenschutzausschusses finden Sie hier. Das Büro des kanadischen Datenschutzbeauftragten finden Sie hier.

3.19 Datenschutzbeauftragter

Wenden Sie sich bei Fragen zum Datenschutz-Informationsverwaltungssystem von Entrust an:

Entrust Corporation

Attention: Jenny Carmichael, Compliance Director

1187 Park Place

Shakopee, MN 55379

privacy@entrust.com

Der ernannte Datenschutzbeauftragte der Entrust Deutschland GmbH ist Herr Niels Kill von Althammer & Kill GmbH & Co. KG (kontakt-dsb@althammer-kill.de).

4. Konformität

Es wird erwartet, dass alle Angestellten und befristet Beschäftigten diese Politik einhalten. Darüber hinaus müssen alle Geschäftseinheiten sicherstellen, dass sie über geeignete lokale Standards und Verfahren verfügen, um diese Richtlinie und die geltenden Datenschutzgesetze in ihrem Land einzuhalten. Verstöße gegen diese Politik werden ernst genommen und können zu disziplinarischen Maßnahmen bis hin zur Kündigung führen. Diese Richtlinie kann jederzeit aktualisiert oder geändert werden.

5. Ausnahmen

Es gibt keine Ausnahmen von dieser Richtlinie.

6. Eigentümerschaft und Überprüfung

Für diese Politik ist der Chief Legal and Compliance Officer zuständig. Diese Politik ist jährlich zu überprüfen. Änderungen an diesem Dokument müssen im Einklang mit dem Standard für die Kontrolle von Dokumenten und Aufzeichnungen des Informationssicherheitsmanagementsystems (ISMS) erfolgen.

6.1 Kontaktinformationen

Fragen zu dieser Richtlinie oder Beschwerden über den Umgang mit personenbezogenen Daten sind an den Compliance-Direktor zu richten: privacy@entrust.com.

6.2 Dokumenteigenschaften und Revisionshistorie

Dokumenteneigenschaften	
Eigentum	**Beschreibung**
Zirkulation	Interne und externe Verwendung
Klassifizierung	Öffentlich
Inhaber des Dokuments	Lisa Tibbits, Chief Legal and Compliance Officer
Nächste planmäßige Überprüfung	2022

Dokumentengenehmigungen		
Name des Genehmigers	**Titel**	**Datum**
Lisa Tibbits	Chief Legal and Compliance Officer	3-Mär-2019
Policy Governance Board	N/A	3-Aug-2021
Policy Governance Board	N/A	16. Dezember 2021

Änderungshistorie			
Version	**Datum**	**Beschreibung der Änderungen**	**Überarbeitet von**
1.0	19-Apr-2019	Ursprüngliche Version	Anjali Doherty, Sr. Corporate Atty;

			Jenny Carmichael, Compliance Director
1.1	19-Apr-2020	Jährliche Aktualisierungen	Anjali Doherty, Sr. Corporate Atty; Jenny Carmichael, Compliance Director
1.2	10-Sept-2020	Aktualisiert in eine neue Richtlinienvorlage	Aileen Havel, Leitende Compliance-Spezialistin
1.3	06-Jul-2021	Jährliche Überarbeitungen; Hinzufügung eines Abschnitts über den Zugang zu besonderen Datenkategorien	Aileen Havel, stellvertretende Unternehmensanwältin; Lee Jones, Senior Compliance Assurance Specialist
1.4	10. Dezember 2021	Aktualisierungen zur Einhaltung von Kontrollen und Empfehlungen zur externen Risikobewertung nach ISO 27701	Jenny Carmichael, Compliance Director