ENTRUST

GLOBALE RICHTLINIE FÜR DEN SCHUTZ PERSONENBEZOGENER DATEN

Dokumentversion	1.2
Datum	10.September 2020

Inhalt

1. Einführung

Als Unternehmen und Arbeitgeber ist es für die Entrust Corporation und ihre Tochtergesellschaften und verbundenen Unternehmen (zusammen „Entrust“ oder das „Unternehmen“) notwendig, personenbezogene Daten über unsere Mitarbeiter, vorübergehend Beschäftigte, Kunden, Lieferanten und andere Dritte, mit denen wir in unserem Namen Produkte oder Dienstleistungen anbieten, zu erheben, zu speichern und zu verarbeiten.

Mit der Einführung der Europäischen Datenschutz-Grundverordnung („DSGVO“) am 25. Mai 2018 und anderer geltender Datenschutzgesetze unterliegen wir erhöhten Anforderungen an die Art und Weise, wie wir personenbezogene Daten erheben, verwenden und speichern.

2. Zweck

Der Zweck dieser Richtlinie ist es, uns allen dabei zu helfen, unseren gesetzlichen Verpflichtungen nachzukommen und es allen Personen, über die wir personenbezogene Daten besitzen, Vertrauen in uns zu ermöglichen. Diese Richtlinie gilt für alle Mitarbeiter von Entrust, vorübergehend Beschäftigte und Dritte, die Daten im Auftrag von Entrust verarbeiten. Sofern nicht anders angegeben, gilt diese Richtlinie in allen Ländern, in denen Entrust präsent ist, und/oder Geschäfte tätigt.

3. Richtlinienanforderungen

3.1 Definitionen

„Datenverantwortlicher“ bezeichnet die Stelle, die den Zweck und die Mittel der Verarbeitung personenbezogener Daten bestimmt.

„Datenverarbeiter“ bezeichnet die Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.

„Datenschutzgesetze“ bezeichnet alle geltenden Datenschutzgesetze und -bestimmungen, insbesondere die EU-Datenschutzgrundverordnung (DSGVO), das kanadische Datenschutzgesetz (Personal Information Protection and Electronic Documents Act, PIPEDA) und das kalifornische Verbraucherdatenschutzgesetz (California Consumer Privacy Act, CCPA).

„Betroffene Person“ bezeichnet die identifizierte oder identifizierbare Person bzw. den identifizierten oder identifizierten Haushalt, auf die bzw. den sich personenbezogene Daten beziehen.

„Datennutzer“ bezeichnet alle Mitarbeiter, Berater, unabhängigen Auftragnehmer, Praktikanten, Zeitarbeiter oder Dritten, die im Namen von Entrust handeln (einschließlich der Datenverarbeiter), und deren Tätigkeit die Verarbeitung personenbezogener Daten für Entrust beinhaltet.

„Personenbezogene Daten“ hat die Bedeutung, die in Datenschutzgesetzen Bezeichnungen wie „persönlich identifizierbare Informationen“, „persönliche Informationen“, „persönliche Daten“ usw. zugewiesen ist.

„Vorfall mit personenbezogenen Daten“ hat die Bedeutung, die in Datenschutzgesetzen den Bezeichnungen „Sicherheitsvorfall“, „Sicherheitsverletzung“ oder „Verletzung des Schutzes personenbezogener Daten“ zugewiesen ist und bezieht sich auf alle Situationen, in denen dem Anbieter bekannt wird, dass auf personenbezogene Daten zugegriffen oder wahrscheinlich zugegriffen wurde oder solche Daten von unbefugten Personen auf unbefugte Weise offengelegt, verändert, verloren, zerstört oder verwendet wurden.

„Verarbeitung“ bezeichnet alle automatischen oder nicht-automatischen Operationen oder Gruppen von Operationen, die mit personenbezogenen Daten durchgeführt werden, wie z. B. Erfassung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Anpassung oder Änderung, Abfrage, Abruf, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder sonstige Bereitstellung, Abgleich oder Kombination, Filterung, Löschung oder Zerstörung. Zur Verarbeitung gehört auch die Übermittlung oder Offenlegung personenbezogener Daten an Dritte.

„Daten der Sonderkategorie“ sind eine Teilmenge personenbezogener Daten und beziehen sich auf Informationen über die ethnische Zugehörigkeit oder Herkunft einer Person, das Sexualleben oder die sexuelle Orientierung, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten (Augenfarbe, Haarfarbe, Größe, Gewicht), Krankengeschichte oder strafrechtliche Verurteilungen, Straftaten oder damit zusammenhängende Sicherheitsmaßnahmen.

3.2 Unsere Verantwortlichkeit

Je nach Umständen kann Entrust als Datenverantwortlicher oder Datenverarbeiter fungieren. Als Datenverantwortlicher ist Entrust dafür verantwortlich, Praktiken und Richtlinien festzulegen, die den Datenschutzgesetzen entsprechen. Ebenso wichtig ist es, dass Entrust die Einhaltung dieser Gesetze nachweisen kann. Maßnahmen des Unternehmens zur Umsetzung:

- Umsetzung von Richtlinien, die es dem Unternehmen ermöglichen, Datenschutzgesetze wie diese Richtlinie, Richtlinien zur Dokumentenaufbewahrung und Datensicherheit sowie Entrust-Datenschutzerklärungen einzuhalten;
- Mitarbeiter, vorübergehend Beschäftigte und Dritte, die im Namen von Entrust handeln, zu Datenschutzanforderungen schulen und darüber informieren;
- Fälle von Nichteinhaltung der Entrust-Datenschutzrichtlinien untersuchen und geeignete Abhilfe- und/oder Disziplinarmaßnahmen ergreifen;
- Untersuchung und Behebung eines Vorfalls mit personenbezogenen Daten und in einigen Fällen Benachrichtigung über den Vorfall;
- Durchführung von Datenschutz-Folgenabschätzungen, sofern dies für neue Arten von Verarbeitungsaktivitäten erforderlich ist;

- Durchführung regelmäßiger interner Audits zu den Entrust-Datenschutzrichtlinien und -verfahren; und
- Berücksichtigung des Datenschutzes bei der Entwicklung neuer Produkte.

3.3 Verarbeitung Personenbezogener Daten

Für die Verarbeitung aller personenbezogenen Daten durch das Unternehmen oder im Auftrag von Entrust gilt verbindlich:

- Sie muss angemessen, rechtmäßig und transparent sein;
- Sie darf nur für bestimmte, ausdrückliche und rechtmäßige Zwecke erfolgen;
- Sie muss relevant sein und sich auf das beschränken, was für die legitimen Zwecke erforderlich ist, für die die Daten verarbeitet werden;
- Sie muss genau und auf dem neuesten Stand sein, um nach vernünftigem Ermessen sicherzustellen, dass unrichtige personenbezogene Daten unverzüglich gelöscht oder korrigiert werden;
- Die Daten dürfen nicht länger aufbewahrt werden, als es zur Erfüllung der Zwecke erforderlich ist, für welche die Daten erhoben wurden; und
- Die Daten sind in einer Weise zu verarbeiten, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder rechtswidriger Verarbeitung, versehentlichem Verlust, Zerstörung oder Beschädigung.

3.4 Rechtliche Grundlagen Für Die Verarbeitung Personenbezogener Daten

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

Wenn eine Verarbeitung erforderlich ist:

- Zur Erfüllung eines Vertrags, an dem die betroffene Person beteiligt ist, oder um auf Verlangen der betroffenen Person vor Abschluss eines Vertrags Maßnahmen zu ergreifen;
- Zur Erfüllung einer rechtlichen Verpflichtung, der Entrust unterliegt; und/oder
- Zur Verfolgung der legitimen Interessen von Entrust, es sei denn, diese Interessen werden durch die Interessen oder Grundrechte und -freiheiten der betroffenen Person überlagert.

Abgesehen von diesen Gründen kann Entrust auch personenbezogene Daten verarbeiten, wenn die betroffene Person der Verarbeitung für einen oder mehrere bestimmte Zwecke zugestimmt hat, vorausgesetzt, dass die Zustimmung freiwillig, spezifisch, informiert und mit einem eindeutigen Hinweis auf die Wünsche der betroffenen Person erteilt wird. Wenn Entrust die Einwilligung als Grundlage für die Verarbeitung verwendet, hat die betroffene Person das Recht, die Einwilligung jederzeit und aus jedem Grund zu widerrufen.

Es kann vorkommen, dass Entrust gelegentlich auch spezielle Kategorien von personenbezogenen Daten für Mitarbeiter oder vorübergehend Beschäftigte verarbeiten muss (z. B. wenn dies aufgrund von Sicherheitsvorschriften am Arbeitsplatz erforderlich ist). Wenn Entrust entweder selbst oder über einen Dritten besondere Kategorien von personenbezogenen Daten verarbeitet oder verwendet, stellt Entrust gegebenenfalls sicher, dass die folgenden Bedingungen erfüllt sind:

- Die betroffene Person hat der Verarbeitung der personenbezogenen Daten der Sonderkategorie für einen oder mehrere bestimmte Zwecke ausdrücklich zugestimmt;
- Die Verarbeitung ist notwendig, um Verpflichtungen aus dem Arbeitsrecht, dem Sozialversicherungs- oder Sozialschutzrecht oder einem Tarifvertrag zu erfüllen;
- Die Verarbeitung ist aus präventiv- oder arbeitsmedizinischen Gründen oder zur Beurteilung der Arbeitsfähigkeit eines Mitarbeiters erforderlich;
- Die Verarbeitung ist notwendig, um die wesentlichen Interessen der betroffenen Person oder einer anderen Person zu schützen, wenn die betroffene Person physisch oder rechtlich nicht in der Lage ist, ihre Zustimmung dazu zu erteilen;
- Die Verarbeitung bezieht sich auf personenbezogene Daten, die von der betroffenen Person veröffentlicht wurden; und/oder
- Die Verarbeitung ist zur Begründung oder Abwehr von Rechtsansprüchen erforderlich.

3.5 Verwaltung Aufgezeichneter Daten

Entrust unterhält ein zentrales Register über die Arten von personenbezogenen Daten, die das Unternehmen erhebt, und warum diese Daten erfasst werden. Entrust verarbeitet personenbezogene Daten nur für die im zentralen Register angegebenen speziellen Zwecke oder für andere Zwecke, die von Datenschutzgesetzen speziell als zulässig genannt werden. Entrust wird die betroffenen Personen über diese Zwecke bei der ersten Datenerhebung oder, wenn dies nicht möglich ist, so schnell wie möglich danach informieren.

Entrust verarbeitet personenbezogene Daten nur in dem Umfang, der für die dem Betroffenen zur Verfügung gestellten Zwecke erforderlich ist. Dies bedeutet, dass Entrust nicht mehr personenbezogene Daten anfordern oder in seinen Systemen speichern darf, als erforderlich sind. Das Unternehmen verfügt über geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass nicht mehr benötigte personenbezogene Daten gelöscht oder vernichtet werden.

Das Unternehmen ergreift auch angemessene Maßnahmen, um sicherzustellen, dass die gespeicherten personenbezogenen Daten korrekt und auf dem neuesten Stand sind. Entrust ist bestrebt, die Richtigkeit der personenbezogenen Daten zum Zeitpunkt der Erhebung und in regelmäßigen Abständen danach zu überprüfen. Das Unternehmen ergreift alle angemessenen Maßnahmen, um unrichtige oder veraltete Daten unverzüglich und auf jeden Fall innerhalb eines Monats nach der Anfrage einer betroffenen Person (oder innerhalb von bis zu drei Monaten,

wenn es bestimmte Gründe gibt, warum ein Monat nicht ausreicht) zu löschen, zu vernichten oder zu ändern.

3.6 Löschung Oder Vernichtung Personenbezogener Daten

Papierakten, die personenbezogene Daten enthalten, müssen vernichtet und sicher entsorgt werden, wenn die Aufbewahrung nicht mehr erforderlich ist. *Papieraufzeichnungen, die personenbezogene Daten enthalten, dürfen nicht anderweitig verwertet werden.*

Bei der Löschung elektronischer personenbezogener Daten sollten alle möglichen Schritte unternommen werden, um die betreffenden Daten unbrauchbar zu machen. Wenn es unmöglich ist, personenbezogene Daten vollständig zu löschen, müssen angemessene Maßnahmen ergriffen werden, um sicherzustellen, dass die Daten so vollständig wie möglich gelöscht werden.

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

3.7 Informationssicherheit

Wenn das Unternehmen personenbezogene Daten verarbeitet, werden angemessene Maßnahmen ergriffen, um die Sicherheit der Daten zu gewährleisten und sie vor unbefugter oder rechtswidriger Verarbeitung, versehentlichem Verlust, Zerstörung oder Beschädigung zu schützen. Entrust realisiert dies durch:

- Verschlüsselung personenbezogener Daten, soweit möglich und sinnvoll;
- Sicherstellung der fortlaufenden 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 Vorfalls; und
- Unterstützung bei der Prüfung, Beurteilung und Bewertung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit.

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

Wenn Entrust Dritte beauftragt, personenbezogene Daten in ihrem Namen zu verarbeiten, so handeln diese auf der Grundlage schriftlicher Anweisungen, sind zur Vertraulichkeit verpflichtet und sind verpflichtet, geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit zu ergreifen. Personenbezogene Daten dürfen nicht an Dritte weitergegeben werden, die nicht Teil von Entrust oder autorisierte Dritte sind.

Schreibtische und Schränke werden verschlossen gehalten, wenn sie personenbezogene Daten oder vertrauliche Informationen irgendeiner Art enthalten. Die Datennutzer stellen sicher, dass gerade in der Nähe befindliche Personen keine personenbezogenen Daten oder vertraulichen Informationen von Monitoren/Bildschirmen ablesen können und melden sich von unbeaufsichtigten Computern/Tablets ab bzw. sperren sie.

3.8 Melden Eines Vorfalls Mit Personenbezogenen Daten

Ein Vorfall mit personenbezogenen Daten kann auf vielfältige Weise erfolgen, einschließlich:

- Verlust eines mobilen Geräts oder einer Papierdatei, die personenbezogene Daten enthält (z. B. versehentliches Zurücklassen eines Geräts in öffentlichen Verkehrsmitteln);
- Diebstahl eines mobilen Geräts oder einer Papierdatei, die personenbezogene Daten enthält (z. B. Diebstahl aus einem Fahrzeug oder Zuhause);
- Menschliches Versagen (z. B. versehentliches Versenden einer E-Mail mit personenbezogenen Daten an einen nicht vorgesehenen Empfänger oder versehentliches Ändern oder Löschen von personenbezogenen Daten);
- Cyberangriff (z. B. Öffnen eines Anhangs zu einer E-Mail eines unbekannten Dritten, der Ransomware oder andere Malware enthält);
- Ermöglichung der unbefugten Nutzung / des unbefugten Zugriffs (z. B. die Berechtigung, dass ein unbefugter Dritter auf sichere Bereiche von Entrust-Niederlassungen oder -Systemen zugreifen kann);
- Unvorhergesehene Umstände wie ein Brand oder eine Überschwemmung; oder
- Wenn Informationen von Entrust von einem Dritten durch Täuschung eingeholt werden.

Anzeichen dafür, dass ein Vorfall mit personenbezogenen Daten stattgefunden haben könnte, sind unter anderem:

- Ungewöhnliche Anmeldung und/oder übermäßige Systemaktivität, insbesondere in Bezug auf aktive Benutzerkonten;
- Ungewöhnliche Fernzugriffsaktivitäten;
- Das Vorhandensein von gefälschten drahtlosen (WLAN-) Netzwerken, die von der Arbeitsumgebung von Entrust aus sichtbar oder zugänglich sind;
- Geräteausfall oder
- Hardware- oder Software-Key-Logger, die an Entrust-Systeme angeschlossen oder auf Entrust-Systemen installiert sind.

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

3.9 Reaktionsplan Für Vorfälle Mit Personenbezogenen Daten

Im Falle eines tatsächlichen oder bevorstehenden Vorfalls mit personenbezogenen Daten ergreift Entrust schnellstmöglich Maßnahmen, um die Auswirkungen des Vorfalls zu minimieren, und meldet den Vorfall, wenn dies gesetzlich vorgeschrieben ist. In den meisten Fällen werden die Maßnahmen Folgendes beinhalten:

- Untersuchung des Vorfalls, um Art, Ursache und Ausmaß des verursachten oder zu erwartenden Schadens festzustellen;
- Umsetzung der notwendigen Schritte, um zu verhindern, dass der Vorfall fortbesteht oder sich wiederholt, und Begrenzung des Schadens für die betroffenen Personen;
- Prüfung, ob eine Verpflichtung besteht, andere Parteien (z. B. nationale Datenschutzbehörden, betroffene Personen) zu informieren sowie diese Meldungen vorzunehmen. Besteht eine Meldepflicht gegenüber den Datenschutzbehörden, muss die Meldung in der Regel innerhalb von 72 Stunden erfolgen, nachdem das Unternehmen oder mindestens einer seiner Mitarbeiter von dem Vorfall Kenntnis erlangt hat;
- Aufzeichnung von Informationen zu Vorfällen mit personenbezogenen Daten und den daraufhin ergriffenen Maßnahmen, einschließlich Unterlagen, welche die Entscheidung bezüglich der Benachrichtigung oder Nichtbenachrichtigung erläutern.

3.10 Internationale Datenübertragungen Und Übertragungen An Dritte

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

Die Unternehmen der Entrust-Gruppe (d. h. alle Gesellschaften und Tochtergesellschaften der Unternehmensgruppe) müssen sich der konzerninternen Datenübermittlungsvereinbarung anschließen, 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 Auftrag von Entrust verarbeiten, 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, mit denen sichergestellt werden soll, dass der Dritte über geeignete technische und organisatorische Maßnahmen verfügt, um die DSGVO einzuhalten und den Schutz der Rechte der betroffenen Person zu gewährleisten.

Fälle, in denen Entrust personenbezogene Daten in ein Land außerhalb des EWR überträgt, sind unter anderem:

- Die betroffene Person hat ihre ausdrückliche Zustimmung zur geplanten Übermittlung gegeben, nachdem Entrust sie über alle möglichen Risiken im Zusammenhang mit einer

solchen Übermittlung informiert hat (z. B. das Fehlen gleichwertiger Garantien im betreffenden Land);

- Die Übermittlung ist notwendig, um einen Vertrag, an dem die betroffene Person beteiligt ist, zu erfüllen oder um auf Verlangen der betroffenen Person vor Abschluss eines Vertrages Maßnahmen zu ergreifen;
- Die Übermittlung ist notwendig, um die wesentlichen Interessen der betroffenen Person oder einer anderen Person zu schützen, wenn die betroffene Person physisch oder rechtlich nicht in der Lage ist, ihre Zustimmung zu erteilen; oder
- Die Übermittlung ist für die Begründung oder Abwehr einer Rechtsforderung erforderlich.

Bei jeder Datenübertragung außerhalb des EWR stützt sich Entrust auf die von der Europäischen Kommission festgelegten Standardvertragsklauseln (2001/497/EG, 2004/915/EG und 2010/87/EU). Bitte beachten Sie, dass auch bei der Übermittlung personenbezogener Daten außerhalb Kanadas eine Datenübermittlungsvereinbarung erforderlich ist.

3.11 Benachrichtigung Betroffener Personen

Entrust ist verpflichtet, betroffenen Personen Informationen über die Verarbeitung ihrer personenbezogenen Daten zur Verfügung zu stellen. Diese Informationen sind in der Datenschutzerklärung des Unternehmens enthalten, die unter www.entrust.com öffentlich zugänglich ist, sowie in der Datenschutzerklärung für Mitarbeiter, die im Entrust-Intranet verfügbar ist. Derartige Stellungnahmen geben Aufschluss über:

- Die Arten von personenbezogenen Daten, die Entrust verarbeitet;
- Zweck und Rechtsgrundlage für die Verarbeitung personenbezogener Daten;
- Ob personenbezogene Daten im Rahmen der Verarbeitung an Dritte weitergegeben werden;
- Ob personenbezogene Daten außerhalb des EWR und Kanadas übermittelt werden und wenn ja, welche Schutzvorkehrungen getroffen werden;
- Wie lange die personenbezogenen Daten verarbeitet werden oder, falls dies nicht zu ermitteln ist, nach welchen Kriterien das Unternehmen den Verarbeitungszeitraum festlegt;
- Wie erhält die betroffene Person eine Kopie ihrer bei Entrust gespeicherten personenbezogenen Daten?
- Rechte des Betroffenen, einschließlich der Vorgehensweise zur Einreichung einer Beschwerde;
- Wenn die personenbezogenen Daten verarbeitet werden müssen, um einer Rechtsvorschrift oder einem Vertrag zu genügen, die möglichen Folgen, wenn die betroffene Person die Daten nicht zur Verfügung stellt oder der Verarbeitung widerspricht; und
- Das Vorhandensein und die Einzelheiten automatisierter Entscheidungsprozesse, falls zutreffend.

Wenn Entrust von einem Dritten personenbezogene Daten über eine betroffene Person erhält, wird das Unternehmen der betroffenen Person auch die folgenden Informationen zur Verfügung stellen:

- Die Art der personenbezogenen Daten, die von dem Dritten erhalten wurden; und
- Die Quelle der Daten und ob sie aus einer öffentlich zugänglichen Quelle (z. B. einer öffentlich zugänglichen Website) stammen.

3.12 „Eingebauter Datenschutz“ Und Datenschutz-Folgenabschätzungen

Den Datenschutzgesetzen zufolge muss Entrust den Datenschutz in der Entwicklungsphase eines neuen Produktangebots berücksichtigen. Um dieser Verpflichtung nachzukommen, muss Entrust Maßnahmen ergreifen, um sicherzustellen, dass der Datenschutz Teil des Entwurfsprozesses 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 darstellen würde) kann Entrust verpflichtet werden, in Bezug auf die Verarbeitung personenbezogener Daten eine formelle Datenschutz-Folgenabschätzung (DPIA) durchzuführen. Eine solche Bewertung beinhaltet die Dokumentation der Zwecke, für welche die Tätigkeit ausgeübt wird, wie Entrust die Datenschutzgesetze einhält und wie das Unternehmen potenzielle Risiken für die Privatsphäre von Personen minimiert. Wenn Sie der Meinung sind, dass eine Datenschutz-Folgenabschätzung erforderlich ist, wenden Sie sich bitte an den Compliance Director unter privacy@entrust.com.

3.13 Rechte Der Betroffenen Person

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

- Informationen zu den über sie gespeicherten personenbezogenen Daten anzufordern;
- Alle unrichtigen personenbezogenen Daten über sie korrigieren und unvollständige personenbezogene Daten vervollständigen zu lassen, sofern Entrust feststellt, dass die Daten tatsächlich unrichtig oder unvollständig sind;
- Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten durch Entrust einzulegen, sofern das Unternehmen dies im Rahmen seiner eigenen legitimen Interessen tut. Entrust kann die Verarbeitung der personenbezogenen Daten ungeachtet eines Widerspruchs fortsetzen, wenn die berechtigten Interessen des Unternehmens die der betroffenen Person überwiegen oder wenn Entrust dies für die Begründung oder Verteidigung eines Rechtsanspruchs tun muss;
- Entrust aufzufordern, die in Bezug auf die betroffene Person gespeicherten personenbezogenen Daten zu vernichten. Das Unternehmen kann diese Anfrage ablehnen, wenn die personenbezogenen Daten für die Zwecke, für die sie verarbeitet werden, weiterhin erforderlich sind und eine legitime Grundlage für die weitere Verarbeitung durch Entrust besteht;

- Entrust aufzufordern, die Verarbeitung ihrer personenbezogenen Daten auf die Speicherung zu beschränken. Dies kann nur verlangt werden, wenn die Richtigkeit der personenbezogenen Daten angefochten wurde und unbestätigt bleibt; wenn Entrust die personenbezogenen Daten nicht mehr benötigt, sondern die betroffene Person sie braucht, um einen Rechtsanspruch zu begründen oder zu verteidigen; wenn die betroffene Person sich gegen die Verarbeitung personenbezogener Daten ausgesprochen hat; und wenn Entrust entscheidet, ob ihre berechtigten Interessen Vorrang vor den Interessen der betroffenen Person haben oder ob die Verarbeitung rechtswidrig ist.

Wenn eine betroffene Person von diesen Rechten Gebrauch macht und Entrust die betreffenden personenbezogenen Daten an einen Dritten weitergegeben hat, wird das Unternehmen sein Bestes tun, um sicherzustellen, dass auch der Dritte den Wünschen der betroffenen Person entspricht.

3.14 Zugriffsanforderungen Durch Betroffene Personen

Betroffene, die Informationen über die personenbezogenen Daten anfordern möchten, die Entrust über sie besitzt, können dies tun, indem sie eine Anforderung zu Erteilung einer Auskunft über personenbezogene Daten (Data Subject Access Request, DSAR) senden. Wenn Mitarbeiter (mündlich oder schriftlich) eine direkte Anforderung erhalten, sind die Einzelheiten der Anforderung unverzüglich an privacy@entrust.com weiterzuleiten.

3.15 Schulungen

Entrust provides its employees and contingent workers with access to training about data protection responsibilities. This training occurs at onboarding and at regular intervals thereafter.

3.16 Datenschutzbeauftragter

Der von der Entrust ernannte DSGVO-Vertreter ist Anjali Doherty, Sr. Corporate Counsel (UK). Der von der Entrust Deutschland GmbH ernannte Datenschutzbeauftragte ist die Kanzlei Kill & Wolff GmbH. Entrust Corporation hat keinen zugewiesenen Datenschutzbeauftragten. Die Aufsicht über das Datenschutzprogramm liegt bei Jenny Carmichael, Compliance Director in der Hauptverwaltung von Entrust in Shakopee, Minnesota, USA.

4. Compliance

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

5. Ausnahmen

In Bezug auf diese Richtlinie gibt es keine Ausnahmen.

6. Verantwortlichkeit Und Überprüfung

Verantwortlich für diese Richtlinie sind der General Counsel und der Chief Compliance Officer. Diese Richtlinie wird jährlich überprüft. Änderungen an diesem Dokument müssen in Übereinstimmung mit dem Document and Records Control Standard des ISMS erfolgen.

6.1 Kontaktinformationen

Fragen zu dieser Richtlinie oder Beschwerden über den Umgang mit personenbezogenen Daten richten Sie bitte an den Compliance Director unter privacy@entrust.com.