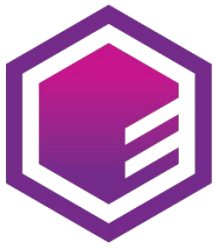

ENTRUST

GLOBALE RICHTLINIE FÜR DEN SCHUTZ PERSONENBEZOGENER DATEN

Klassifizierung	Öffentlich
Dokumentenversion	2.0
Datum der Veröffentlichung	26. Februar 2026

Inhalt

1. Einführung

Die Entrust Corporation und ihre Tochtergesellschaften (zusammen „Entrust“ oder das „Unternehmen“) verarbeiten personenbezogene Daten unserer Mitarbeiter sowie die von geschäftlichen Kontaktpersonen bei unseren Vertriebspartnern, Lieferanten und Kunden in unserer Rolle als Datenverantwortlicher. Entrust verarbeitet in seiner Rolle als Datenverarbeiter auch personenbezogene Daten von Mitarbeitern und Endnutzern unserer Kunden. Wo Entrust personenbezogene Daten verarbeitet, tun wir dies in Übereinstimmung mit unseren gesetzlichen und vertraglichen Verpflichtungen und mit voller Transparenz.

2. Zweck

Diese Richtlinie legt die Anforderungen und Elemente unseres globalen Datenschutzprogramms fest, das Entrust eingerichtet hat, um sicherzustellen, dass wir die einschlägigen gesetzlichen und vertraglichen Verpflichtungen sowie alle nötigen Zertifizierungs- und Prüfungsanforderungen erfüllen. Diese Richtlinie gilt weltweit für alle Verarbeitungen personenbezogener Daten, die von Entrust durchgeführt werden.

3. Definitionen

„Datenverantwortlicher“ ist die Stelle, die den Zweck und die Methode der Verarbeitung personenbezogener Daten festlegt. Sie hat dieselbe Bedeutung wie der „PII Controller“ gemäß ISO 27701.

„Datenverarbeiter“ ist die Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Sie hat dieselbe Bedeutung wie der „PII Processor“ gemäß ISO 27701.

„Datenschutz-Folgenabschätzung“ bezieht sich auf eine dokumentierte Analyse durch einen Datenverantwortlichen oder Datenverarbeiter, in der die Risiken für den Schutz der Privatsphäre bewertet werden, wenn die Verarbeitung wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Person führt.

„**Datenschutzgesetze**“ bezeichnet alle auf Entrust anwendbaren Gesetze und Vorschriften rund um persönliche Daten, insbesondere u. a. die Datenschutz-Grundverordnung der EU (DSGVO), die General Data Protection Regulation des Vereinigten Königreichs (UK GDPR), den Data Protection Act des Vereinigten Königreichs (DPA 2018), das Schweizer Bundesgesetz über den Datenschutz (DSG, Stand 1. September 2023), den kanadischen Personal Information Protection and Electronic Documents Act (PIPEDA), den japanischen Act on Protection of Personal Information (APPI), das chinesische Personal Information Protection Law (PIPL) und die Datenschutzgesetze der US-Bundesstaaten, jeweils in der geänderten, ergänzten oder ersetzten Fassung.

„Betroffene Person“ ist die identifizierte oder identifizierbare Person oder der Haushalt, auf die/den sich die personenbezogenen Daten beziehen. Sie hat die gleiche Bedeutung wie „PII Principal“ gemäß ISO 27701.

„Datenübertragungs-Folgenabschätzung“ bezieht sich auf eine dokumentierte Analyse durch einen Datenverantwortlichen oder Datenverarbeiter über die Auswirkungen und Sicherheitsimplikationen einer Übermittlung personenbezogener Daten aus dem EWR oder dem Vereinigten Königreich (UK) in ein Land außerhalb des EWR/UK, für das die Europäische Kommission oder das Information Commissioner's Office keine Angemessenheitserklärung abgegeben hat.

„Folgenabschätzung über berechtigtes Interesse“ bezieht sich auf eine dokumentierte Analyse durch einen Datenverantwortlichen oder Datenverarbeiter, ob berechtigtes Interesse als Rechtsgrundlage für die Verarbeitung personenbezogener Daten verwendet werden kann. Die Bewertung umfasst einen dreistufigen Test, bei dem untersucht wird, ob die Verarbeitung personenbezogener Daten der Verfolgung eines berechtigten Interesses dient, ob sie für dieses Interesse erforderlich ist und ob die Interessen der betroffenen Person das berechtigte Interesse überwiegen.

„Personenbezogene Daten“ oder „PII“ hat die Bedeutung, die in Datenschutzgesetzen Bezeichnungen wie „personenbezogene Daten“, „persönliche Informationen“ usw. zugewiesen ist.

„Vorfall mit personenbezogenen Daten“ hat die Bedeutung, die den Begriffen „Sicherheitsvorfall“, „Sicherheitsverletzung“ oder „Verletzung des Schutzes personenbezogener Daten“ oder gleichwertigen Begriffen, wie sie in den Datenschutzgesetzen definiert sind, zugeschrieben wird. Die Bezeichnung umfasst jede Situation, in der Entrust Kenntnis davon erlangt, dass personenbezogene Daten von unbefugten Personen in unbefugter Weise eingesehen, offengelegt, verändert, verloren, zerstört oder verwendet wurden.

„Verarbeitung“ bezeichnet alle automatischen oder nicht automatischen Vorgänge oder Gruppen von Vorgängen, 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. Die Verarbeitung umfasst auch die Übermittlung oder Weitergabe personenbezogener Daten an Dritte.

„Sensible personenbezogene Daten“ sind eine Teilmenge personenbezogener Daten und beziehen sich auf Informationen über eine betroffene Person, die bei Verlust, Kompromittierung, Zugriff oder unsachgemäßer Offenlegung der betroffenen Person Schaden zufügen könnten oder in einer Bloßstellung, Unannehmlichkeiten oder Ungerechtigkeit für diese Person münden könnten und daher einem verstärkten Schutz unterliegen.

„Daten der Sonderkategorie“ sind eine Teilmenge personenbezogener Daten und beziehen sich auf Informationen über die ethnische Zugehörigkeit oder Herkunft einer Person, politische

Meinungen, religiöse oder philosophische Überzeugungen oder Gewerkschaftszugehörigkeit sowie auf die Verarbeitung genetischer Daten, biometrischer Daten zum Zwecke der eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person.

4. Kernprinzipien der Verarbeitung personenbezogener Daten

Entrust hält sich bei der Verarbeitung personenbezogener Daten als Datenverantwortlicher an die folgenden Kernprinzipien:

- **Rechtmäßigkeit und Angemessenheit**: Wir stellen sicher, dass personenbezogene Daten für einen rechtmäßigen Zweck erhoben werden und auf für diesen Zweck relevante und notwendige Daten beschränkt sind.
- **Genauigkeit und Aufbewahrung**: Wir halten unsere Systeme auf dem neuesten Stand, bieten Mechanismen zur Aktualisierung unrichtiger personenbezogener Daten an und bewahren personenbezogene Daten nicht länger auf, als es für die Erfüllung des rechtmäßigen Zwecks der Verarbeitung erforderlich ist.
- **Vertraulichkeit und Integrität**: Wir sorgen dafür, dass personenbezogene Daten während der Verarbeitung sicher und geschützt bleiben, reagieren jedoch schnell und angemessen auf Vorfälle mit personenbezogenen Daten, wenn sie auftreten, und benachrichtigen betroffene Personen bei Bedarf rechtzeitig.
- **Fairness und Transparenz**: Wir informieren die betroffenen Personen in angemessener Weise, wenn wir ihre personenbezogenen Daten verarbeiten. Wir vermitteln klar, wozu wir die Daten benötigen, wie wir sie verwenden und wie sie behandelt und geschützt werden. Wir stellen Mechanismen zur Verfügung, mit deren Hilfe betroffene Personen die Rechte ausüben können, die ihnen in Bezug auf ihre personenbezogenen Daten nach geltendem Recht zustehen.

Wir alle bei Entrust sind für die ordnungsgemäße Verarbeitung und den Schutz personenbezogener Daten verantwortlich und sind uns darüber im Klaren, dass ein Versäumnis nicht nur das Vertrauen untergraben kann, das Kunden in Entrust haben, sondern auch zu erheblichen Geldstrafen und Bußgeldern für das Unternehmen führen kann.

5. Verzeichnis von Verarbeitungstätigkeiten

Um die Einhaltung der geltenden Datenschutzgesetze zu gewährleisten und unser Engagement für Transparenz und Rechenschaftspflicht aufrechtzuerhalten, führt Entrust ein Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 der DSGVO und anderen einschlägigen Datenschutzvorschriften. Dieses Verzeichnis umfasst alle Verarbeitungstätigkeiten, die personenbezogene Daten betreffen, die gemäß dem Entrust-Standard zur Datenklassifizierung und -handhabung klassifiziert sind.

6. Rechtmäßigkeit und Angemessenheit

6.1 Rechtliche Grundlagen für die Verarbeitung personenbezogener Daten

Wenn das Unternehmen als Datenverantwortlicher handelt, verarbeitet es personenbezogene Daten nur im gesetzlich zulässigen Rahmen. Entrust stützt sich im Wesentlichen auf die folgenden Rechtsgrundlagen für die Verarbeitung:

- Erfüllung eines Vertrags;
- Erfüllung rechtlicher Verpflichtungen, einschließlich, aber nicht beschränkt auf rechtmäßige Anfragen von Strafverfolgungsbehörden;
- Berechtigtes Interesse, es sei denn, die Interessen oder Grundrechte und -freiheiten der betroffenen Person überwiegen dieses Interesse; und
- Einwilligung.

Ist die Einwilligung die Rechtsgrundlage für die Verarbeitung, so stellt Entrust sicher, dass die Einwilligung frei, spezifisch und in Kenntnis der Sachlage erteilt wird und einen eindeutigen Hinweis auf die Wünsche der betroffenen Person darstellt. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit und ohne Angabe von Gründen zu widerrufen.

6.2 Datenschutzbewertungen

6.2.1 Privacy by Design-Bewertung

Entrust bewertet die Verarbeitung personenbezogener Daten anhand der in Abschnitt 4 oben beschriebenen Kernprinzipien im Rahmen der Konzeptfindung und Entwicklung neuer oder wesentlich geänderter Produktangebote und beim Onboarding von Anbieterlösungen, bei denen PII verarbeitet werden, einschließlich lizenzierter Softwareanwendungen Dritter. Diese „Privacy by Design“-Bewertung ist in die Entwicklungs- und Lieferanten-Onboarding-Prozesse von Entrust eingebettet. Der Abschluss der Bewertung erfordert die Überprüfung und Genehmigung durch die Datenschutz- und Informationssicherheitsteams von Entrust. Ohne Genehmigung darf die Entwicklung nicht voranschreiten.

6.2.2 Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA)

Wenn die geplante Verarbeitung personenbezogener Daten ein hohes Risiko für die Rechte und Freiheiten einer Person darstellt, führt Entrust eine förmliche Datenschutz-Folgenabschätzung durch, um den Zweck der Verarbeitung zu dokumentieren und zu bewerten, wie Entrust die einschlägigen Datenschutzgesetze einhalten und potenzielle Risiken für die betroffene Person mindern wird. Bezieht sich eine DPIA auf eine Verarbeitung, bei der Entrust der Datenverantwortliche ist, wird sie vom Datenschutzbeauftragten von Entrust überprüft, der die vorgeschlagene Verarbeitung vor deren Beginn genehmigen muss. DPIAs müssen mindestens jährlich oder bei Bedarf häufiger überprüft und aktualisiert werden, um die kontinuierliche Einhaltung der geltenden Gesetze und Vorschriften zu gewährleisten.

6.2.3 Datenübertragungs-Folgenabschätzung (Data Transfer Impact Assessment, DTIA)

Wenn Entrust beabsichtigt, personenbezogene Daten aus dem Europäischen Wirtschaftsraum (EWR) oder Vereinigten Königreich (UK) in ein Land außerhalb des EWR oder UK zu übermitteln, für das die Europäische Kommission oder das Information Commissioner's Office des UK keine Angemessenheitserklärung abgegeben hat, füllt Entrust eine formelle DTIA aus, um die Auswirkungen und Sicherheitsimplikationen der Übertragung zu analysieren – insbesondere dann, wenn die Gesetze des Empfängerlandes seiner Regierung den Zugriff auf die zu übermittelnden personenbezogenen Daten ermöglichen könnten. Entrust wird nur dann mit der Übertragung fortfahren, wenn es zu dem Schluss kommt, dass das mit der Übertragung verbundene Risiko akzeptabel ist.

6.2.4 Folgenabschätzung für berechtigtes Interesse (Legitimate Interest Impact Assessment, LIIA)

Wenn Entrust als Datenverantwortlicher auftritt und sich auf ein berechtigtes Interesse als Rechtsgrundlage für die Verarbeitung personenbezogener Daten beruft, führt das Unternehmen eine formelle LIIA durch, um das berechtigte Interesse zu dokumentieren und zu bewerten, festzustellen, ob die Verarbeitung notwendig ist, und zu beurteilen, ob die Interessen, Rechte und Freiheiten der betroffenen Person das berechtigte Interesse überwiegen oder außer Kraft setzen. Entrust wird die Verarbeitung nur dann auf der Grundlage eines berechtigten Interesses vornehmen, wenn die LIIA zu dem Schluss kommt, dass das berechtigte Interesse nicht wie oben erläutert außer Kraft gesetzt wird. Die DTIAs müssen mindestens jährlich, oder bei Bedarf auch häufiger, überprüft und aktualisiert werden, um die fortlaufende Einhaltung der geltenden Gesetze und Vorschriften zu gewährleisten.

6.2.5 Standards für den Umgang mit sensiblen Daten und Daten der Sonderkategorie

In seiner Rolle als Datenverantwortlicher verarbeitet Entrust sensible personenbezogene Daten seiner Mitarbeiter über verschiedene Geschäftssysteme und einige begrenzte Daten der Sonderkategorie auf freiwilliger Basis und im Rahmen der lokalen Gesetze. Es sind geeignete Kontrollen vorhanden und in den entsprechenden Datenschutz-Folgenabschätzungen, dem Standard für die Zugangskontrolle zu sensiblen Daten und Daten der Sonderkategorie sowie in den verstärkten Datenschutzschulungen für Mitarbeiter dargelegt, die mit diesen sensiblen Daten und Daten der Sonderkategorie umgehen.

6.2.6 Regel für große Datenmengen

Sensible personenbezogene Daten, einschließlich menschlicher genomischer, epigenomischer, proteomischer und transkriptomischer Daten, biometrischer Identifikatoren, präziser Geolokalisierungsdaten, persönlicher Gesundheitsdaten, persönlicher Finanzdaten und bestimmter persönlich identifizierender Daten von US-Bürgern, sowie Daten der US-Regierung, einschließlich präziser Geolokalisierungsdaten für Bereiche, die besonders sensibel gegenüber Ausnutzung sind (wie z. B. Militäreinrichtungen, Einrichtungen für die nationalen Sicherheit, die Verteidigung oder den Nachrichtendienst oder Arbeitsstätten von Mitarbeitern des nationalen Nachrichtendienstes auf Bundesebene), unterliegen Ausfuhr-, Weitergabe- und Zugangsbeschränkungen. Diese Daten dürfen nicht an natürliche oder juristische Personen weitergegeben werden, die in einem Land ansässig sind, das Anlass zur Besorgnis gibt, oder von dort kontrolliert werden oder auf Anweisung einer dort ansässigen natürlichen oder juristischen Person handeln. Zu diesen Ländern, die Anlass

zur Besorgnis geben, gehören derzeit China (einschließlich Hongkong und Macau), Kuba, Iran, Nordkorea, Russland und Venezuela.

Auch wenn eine solche Übermittlung oder ein solcher Zugang unter bestimmten Umständen möglich ist, hat Entrust beschlossen, sich nicht an Transaktionen mit Ländern, die Anlass zur Besorgnis geben, zu beteiligen, wenn diese Transaktionen sensible personenbezogene Daten aus den USA oder Daten der US-Regierung betreffen. Weder Entrust noch eine Person, die im Namen von Entrust handelt, darf solche Daten in ein Land, das Anlass zur Besorgnis gibt, oder an eine Person oder Einrichtung in einem solchen Land übermitteln.

6.3 Vertragliche Schutzmaßnahmen

6.3.1 Vereinbarung über konzerninterne Datenübertragung (Intra-Group Data Transfer Agreement, IGDTA)

Die Entrust Corporation und ihre Tochtergesellschaften schließen die Vereinbarung über konzerninterne Datenübertragung ab, um sicherzustellen, dass im Falle einer Weitergabe personenbezogener Daten innerhalb der Entrust-Gruppe diese durch geeignete Datenweitergabeklauseln (einschließlich Klauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß der DSGVO) abgedeckt ist. Das IGDTA stellt zudem sicher, dass angemessene Schutzmaßnahmen (d. h. Standardvertragsklauseln) für den Fall bestehen, dass die Weitergabe personenbezogener Daten innerhalb der Entrust-Gruppe die Übermittlung personenbezogener Daten aus dem EWR/Vereinigten Königreich (UK) in ein Land außerhalb des EWR/UK beinhaltet, für das keine Angemessenheitsfeststellung der Europäischen Kommission oder des Information Commissioner's Office vorliegt.

6.3.2 Datenverarbeitungsvereinbarung (Data Processing Agreement, DPA)

Unternehmen außerhalb des Entrust-Konzerns, die personenbezogene Daten für oder im Namen von Entrust verarbeiten, müssen eine Datenverarbeitungsvereinbarung mit Entrust abschließen, um sicherzustellen, dass der jeweilige Dritte (z. B. Verkäufer, Lieferant, Vertriebspartner) über angemessene technische und organisatorische Maßnahmen verfügt, um die einschlägigen Datenschutzgesetze einzuhalten. Entrust geht entsprechende Verpflichtungen mit seinen Kunden ein, wenn es als Datenverarbeiter im Rahmen einer standardmäßigen Kunden-DPA auftritt.

6.3.3 Allgemeine Datenschutzbestimmungen

Vertragsformulierungen zum Datenschutz sind auch in Standardvereinbarungen mit Kunden, Lieferanten und Partnern sowie in der Standard-Verschwiegenheitserklärung (Non-Disclosure Agreement, NDA) von Entrust enthalten. Verträge mit Verkäufern und Lieferanten enthalten ebenfalls Verpflichtungen zur Einhaltung der Regel für große Datenmengen.

7. Genauigkeit und Aufbewahrung

7.1 Records Management

Das globale Records-Management-Programm stellt sicher, dass formell eine Aufbewahrungsfrist für die Verarbeitung personenbezogener Daten festgelegt wird, um zu gewährleisten, dass sie nur so

lange aufbewahrt werden, wie sie benötigt werden, und dass personenbezogene Daten nach Ablauf der zugewiesenen Aufbewahrungsfrist gelöscht, vernichtet oder anonymisiert werden. Die globale Records-Management-Richtlinie legt die Anforderungen an den Umgang mit sämtlichen Datensätzen fest – nicht nur mit denen, die personenbezogene Daten enthalten – und der beiliegende Zeitplan der Datenaufbewahrung definiert die Aufbewahrungsfrist für jede Art von Datensatz, die vom Unternehmen verwaltet wird.

7.2 Speicherung und Sicherung von personenbezogenen Daten

Entrust speichert und sichert personenbezogene Daten an mehreren Serverstandorten, die direkt und indirekt vom Unternehmen verwaltet werden. Die IT-Abteilung und die einschlägigen Anbieter (für nicht von der IT-Abteilung verwaltete, in der Cloud gehostete Anwendungen) erhalten Standardanleitungen für den ordnungsgemäßen Umgang mit personenbezogenen Daten auf diesen Servern, auch in Bezug auf Speicherung und Sicherungen.
Entrust entfernt am Ende der Aufbewahrungsfrist keine Kopien personenbezogener Daten von seinen Sicherungsmedien und Servern, wenn dies wirtschaftlich nicht vertretbar wäre; personenbezogene Daten, die von Entrust auf diese Weise aufbewahrt werden, sind jedoch durch dieselben Sicherheitsstandards geschützt, die die personenbezogenen Daten auch schützen, während sie in Gebrauch sind; und die personenbezogenen Daten unterliegen weiterhin der Vertraulichkeit und dürfen nicht zugänglich gemacht werden, es sei denn, dies ist nach geltendem Recht erforderlich.

7.3 Löschung oder Vernichtung personenbezogener Daten

Die globale Richtlinie zur Verwaltung von Aufzeichnungen und der Standard zur Datenklassifizierung und -handhabung legen die Anforderungen für den angemessenen Umgang mit Datensätzen aller Art nach Ablauf der vorgeschriebenen Aufbewahrungsfrist fest. Für Datensätze, die personenbezogene Daten enthalten, gelten insbesondere die folgenden Grundsätze:

- Personenbezogene Daten sollten nicht kopiert werden, es sei denn, dies ist für den angegebenen Zweck der Verarbeitung erforderlich, und alle angefertigten Kopien sollten die ursprünglichen Kennzeichnungen „vertraulich“ oder „geschützt“ beibehalten.
- Papierunterlagen müssen geschreddert und sicher entsorgt werden, wenn sie nicht mehr aufbewahrt werden müssen, und dürfen nicht auf andere Weise entsorgt werden.
- Personenbezogene Daten in elektronischem Format sollten gelöscht oder anonymisiert werden, sobald sie nicht mehr benötigt werden.
- Die IT-Abteilung ist dafür verantwortlich, elektronische Geräte, die personenbezogene Daten enthalten (z. B. Laptops, Desktops, firmeneigene mobile Geräte und Arbeitsdaten auf BYOD-Geräten [Bring Your Own Device]), in Übereinstimmung mit den einschlägigen Informationssicherheitsrichtlinien und -standards zu vernichten oder zu löschen.

8. Vertraulichkeit und Integrität

8.1 Informationssicherheit

Wenn das Unternehmen personenbezogene Daten verarbeitet, ergreift es angemessene Maßnahmen, um sicherzustellen, dass diese Daten sicher bleiben und vor unbefugter oder unrechtmäßiger Verarbeitung, versehentlichem Verlust, Zerstörung oder Beschädigung geschützt sind. Entrust erzielt dies auf folgende Weise:

- Verschlüsselung personenbezogener Daten im gespeicherten Zustand sowie bei der Übertragung, soweit dies gesetzlich oder vertraglich vorgeschrieben, aber auch wirtschaftlich vertretbar ist;
- Gewährleistung der kontinuierlichen Vertraulichkeit, Integrität, Verfügbarkeit und Resilienz von Systemen und Dienstleistungen, die zur Verarbeitung personenbezogener Daten verwendet werden, durch formalisierte Pläne für die Wiederherstellung des Geschäftsbetriebs sowie für Disaster Recovery, die routinemäßig getestet oder geübt werden;
- Sicherstellen der rechtzeitigen Wiederherstellung des Zugriffs auf personenbezogene Daten im Falle eines physischen oder technischen Zwischenfalls;
- Regelmäßige Prüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten;
- Durchsetzung physischer Sicherheitsstandards, die vorschreiben, dass Schreibtische und Schränke, in denen sich personenbezogene Daten befinden, verschlossen bleiben müssen, dass einzelne Monitore/Bildschirme es nicht ermöglichen, dass personenbezogene Daten von vorbeigehenden Personen eingesehen werden können, und dass elektronische Geräte (z. B. Computer, Tablets) gesperrt oder von den Systemen des Unternehmens abgemeldet werden, wenn sie unbeaufsichtigt sind.

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

Wenn Entrust Dritte mit der Verarbeitung personenbezogener Daten in seinem Namen beauftragt, so geschieht dies auf Grundlage schriftlicher Anweisungen von Entrust und vorbehaltlich vertraglicher Bestimmungen (z. B. DPA) zum angemessenen Umgang mit den personenbezogenen Daten und zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen, die den Entrust-eigenen Sicherheitsanforderungen mindestens gleichwertig sind. Personenbezogene Daten werden nicht außerhalb von Entrust weitergegeben, wenn diese Mechanismen nicht vorhanden sind. Verschiedene Sicherheitstools (z. B. DLP) sorgen dafür, dass personenbezogene Daten das Unternehmen nicht unbefugt verlassen.

8.2 Tests

Personenbezogene Daten dürfen in keiner Testumgebung von Entrust verwendet werden, ohne dass im Voraus eine formelle Sicherheitsausnahme genehmigt wurde. Alle Testumgebungen müssen den aktuellen Standards und Kontrollen entsprechen, die für Produktionsumgebungen gelten, und alle personenbezogenen Daten, die zur Verwendung in Testumgebungen freigegeben wurden, müssen nach Abschluss der Tests unverzüglich entfernt werden. Weitere Einzelheiten finden Sie im Secure-Software Development Lifecycle (S-SDLC).

8.3 Meldung eines Vorfalls mit personenbezogenen Daten

Ein Vorfall mit personenbezogenen Daten kann in vielen Formen auftreten, einschließlich, aber nicht beschränkt auf:

- 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;
- Menschliches Versagen (z. B. wenn ein Mitarbeiter versehentlich eine E-Mail mit personenbezogenen Daten an einen unbeabsichtigten Empfänger sendet oder 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);
- Physische Zerstörung und Verlust (z. B. durch Feuer oder Überschwemmung) oder
- Informationen werden von Dritten durch Täuschung von Entrust erlangt (z. B. Phishing- oder Smishing-Angriffe).

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

- Ungewöhnliche Anmeldung und/oder übermäßige Systemaktivität 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 oder
- Hardware- oder Software-Schlüssellogger, die an Entrust-Systeme angeschlossen oder darauf installiert sind.

Mitarbeiter, die Kenntnis von einem Vorfall mit personenbezogenen Daten erhalten oder Grund zu der Annahme haben, dass ein solcher Vorfall eingetreten ist oder bevorsteht, müssen sich unverzüglich an das Security Operations Center von Entrust wenden: SOC@entrust.com.

8.4 Reaktion bei Vorfällen mit personenbezogenen Daten

Im Falle eines tatsächlichen oder drohenden Vorfalls bei der Verarbeitung personenbezogener Daten wird Entrust die von Information Security aufrechterhaltenen Vorfallsreaktionsverfahren anwenden, um die Auswirkungen des Vorfalls so gering wie möglich zu halten, und Aufsichtsbehörden, betroffene Personen und/oder andere Parteien gemäß den gesetzlichen und/oder vertraglichen Bestimmungen benachrichtigen. Die Reaktion wird in der Regel Folgendes umfassen:

- Untersuchung des Vorfalls, um die Art, die Ursache und das Ausmaß des entstandenen oder potenziellen 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, Vertragsparteien) zu benachrichtigen, und rechtzeitiges Vornehmen dieser Benachrichtigungen und
- Aufzeichnung von Informationen über den Vorfall mit personenbezogenen Daten und die daraufhin unternommenen Schritte, einschließlich der Dokumentation von Entscheidungen über die Benachrichtigung oder Nichtbenachrichtigung von Aufsichtsbehörden oder betroffenen Parteien.

9. Transparenz

Entrust gewährleistet die Transparenz seines globalen Datenschutzprogramms durch umfassende interne und externe Landingpages.

9.1 Datenschutzhinweise

Entrust informiert in seiner Rolle als Datenverantwortlicher und Datenverarbeiter betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten. Diese Information ist in den verschiedenen Entrust-Datenschutzhinweisen für Internetbenutzer, Bewerber und Mitarbeiter sowie in den einzelnen Produkt-Datenschutzhinweisen zu finden, die hier verfügbar sind. Diese Hinweise liefern Informationen über Folgendes:

- Die Arten von personenbezogenen Daten, die Entrust verarbeitet;
- Zweck und Rechtsgrundlage der Verarbeitung;
- Für die Verarbeitung eingesetzte Dritte (sofern zutreffend);
- Ort und Dauer der Verarbeitung;

- Jegliche Übertragung personenbezogener Daten in ein anderes Land;
- Dauer der Verarbeitung;
- Rechte der betroffenen Personen und
- Einzelheiten zu künstlicher Intelligenz/automatisierten Entscheidungsprozessen

9.2 Schulung

Entrust stellt seinen Mitarbeitern eine obligatorische jährliche Schulung über die Verantwortlichkeiten im Bereich des Datenschutzes bereit. Diese Schulung „Einführung in den Datenschutz“ erfolgt bei der Einstellung und danach jährlich. Zusätzlich zur kollektiven Schulung „Einführung in den Datenschutz“ verlangt Entrust die jährliche Teilnahme an der „Erweiterten Schulung zum Datenschutz“ von Mitarbeitern, die mit sensiblen Daten und Daten der Sonderkategorie umgehen, sowie an der Schulung „Privacy by Design“ von Mitarbeitern, die an der Entwicklung und Gestaltung von Softwareprodukten und Dienstleistungen beteiligt sind. Entrust wird bei Bedarf zusätzliche funktionsspezifische Datenschutzschulungen entwickeln und durchführen.

9.3 Rechte der betroffenen Personen

Wenn Entrust personenbezogene Daten verarbeitet, haben die betroffenen Personen gemäß den Datenschutzgesetzen bestimmte Rechte. Obwohl diese Rechte je nach Rechtsprechung variieren, haben die betroffenen Personen im Allgemeinen das Recht:

- Informationen über die personenbezogenen Daten, die Entrust über sie gespeichert hat, einschließlich einer Kopie dieser Informationen anzufordern;
- Unrichtige personenbezogene Daten berichtigen und unvollständige personenbezogene Daten vervollständigen zu lassen;
- Der Verarbeitung ihrer personenbezogenen Daten durch Entrust zu widersprechen, wenn das Unternehmen dies in Verfolgung seines eigenen berechtigten Interesses tut; Entrust kann die personenbezogenen Daten trotz eines Widerspruchs weiterverarbeiten, wenn das berechtigte Interesse des Unternehmens die Interessen der betroffenen Person überwiegen oder wenn Entrust dies aus rechtlichen Gründen tun muss;
- Entrust aufzufordern, 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 rechtliche Grundlage für die weitere Verarbeitung gibt;
- Von Entrust zu verlangen, dass die Verarbeitung ihrer personenbezogenen Daten auf die Speicherung unter bestimmten Umständen beschränkt wird.

Entrust prüft die Rechte betroffener Personen im Rahmen der Datenschutzgesetze von Fall zu Fall und befolgt bei der Entscheidung darüber, wie einer Anfrage nachzukommen ist, das Verfahren für

Auskunftsersuchen betroffener Personen. Im Allgemeinen wird Entrust die Rechte einer betroffenen Person nach der europäischen DSGVO als Grundlage für die Bearbeitung von Anfragen verwenden und die Rechte, die die betroffene Person gemäß den für sie geltenden Datenschutzgesetzen hat, 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.

Betroffene Personen, die Auskunft über die von Entrust über sie gespeicherten personenbezogenen Daten verlangen möchten, sollten dies durch Einreichung eines formellen Antrags auf Datenübermittlung (Data Subject Request, DSR) tun. Wenn Mitarbeiter direkt eine Anfrage erhalten (ob mündlich oder schriftlich), sollte diese umgehend an privacy@entrust.com weitergeleitet werden.

9.4 Aufsichtsbehörden

Die Kontaktinformationen für die zuständigen Datenaufsichtsbehörden variieren je nach Standort. Die Liste der Organe des Europäischen Datenschutzausschusses finden Sie hier. Das Information Commissioner's Office (ICO) des Vereinigten Königreichs (UK) finden Sie hier. Das Office of the Privacy Commissioner of Canada finden Sie hier.

9.5 Datenschutzbeauftragter

Sofern nicht anders angegeben, ist der Datenschutzbeauftragte von Entrust:

Mishcon de Reya LLP
Africa House, 70 Kingsway, London, WC2B 6AH, Vereinigtes Königreich
DPO@mishcon.com

10. Compliance

Es wird erwartet, dass alle Mitarbeiter und Zeitarbeitskräfte diese Richtlinie 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 Richtlinie werden ernst genommen und können zu Disziplinarmaßnahmen bis hin zur Kündigung führen. Diese Richtlinie kann jederzeit aktualisiert oder geändert werden.

11. Ausnahmen

Es gibt keine Ausnahmen von dieser Richtlinie.

12. Eigentümerschaft und Änderungshistorie

Diese Richtlinie unterliegt der Verantwortlichkeit des Director Privacy und ist jährlich zu überprüfen.