

Dokumentenversion	1.6
Datum	5. Sep. 2023



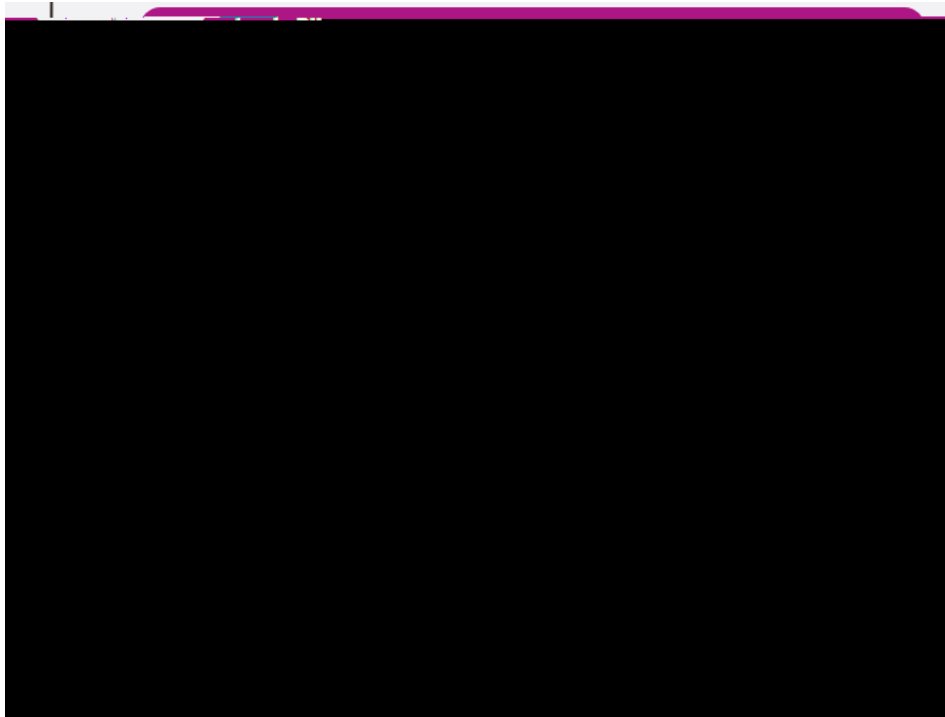
11. Ausnahmen	15
12. Verantwortlichkeit und Überprüfung	15
12.1 Kontaktinformationen	15

1. Einführung

Die Entrust Corporation und ihre Tochtergesellschaften und verbundenen Unternehmen (zusammen „Entrust“ oder das „Unternehmen“) verarbeiten personenbezogene Daten unserer Mitarbeiter, Zeitarbeiter, Partner, Lieferanten und Kunden in unserer Rolle als Datenverantwortlicher sowie personenbezogene Daten unserer Kunden und ihrer Endbenutzer in unserer Rolle als Datenverarbeiter. Wo Entrust personenbezogene Daten verarbeitet, tun wir dies in Übereinstimmung mit unseren gesetzlichen, vertraglichen und ethischen Verpflichtungen und mit voller Transparenz.

2. Zweck

Diese Richtlinie legt die Anforderungen und Elemente unseres globalen Datenschutzprogramms fest, 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 direkt von Entrust und indirekt von Dritten in unserem Auftrag durchgeführt werden.



6. Rechtmäßigkeit und Angemessenheit

6.1 Rechtliche Grundlagen für die Verarbeitung personenbezogener Daten

Das Unternehmen verarbeitet personenbezogene Daten nur im gesetzlich zulässigen Rahmen und mit angemessener Benachrichtigung der betroffenen Person. 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.
- Einwilligung.

Ist die Einwilligung die Rechtsgrundlage für die Verarbeitung (z. B. für Marketingzwecke), 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.

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 Datenschutzbildungen für Mitarbeiter dargelegt, die mit diesen sensiblen Daten und Daten der Sonderkategorie umgehen.

6.3 Vertragliche Schutzmaßnahmen

6.3.1

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

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:

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.

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 Datenschutzzschulungen 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:

- Auskunft über die zu ihrer Person gespeicherten Daten zu verlangen;
- 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.

