DATENSCHUTZ-RICHTLINIE

KONTEXT UND ÜBERBLICK

Wichtige Details

- Richtlinie vorbereitet von: Alison Rait
- Genehmigt vom Management am: 18/04/2018
- Die Richtlinie wurde am: 01/05/2018
- Datum der nächsten Überprüfung: 01/05/2018

Einführung

RP Technologies Ltd muss bestimmte Informationen über Einzelpersonen sammeln und verwenden.

Dazu gehören Kunden, Lieferanten, Geschäftskontakte, Mitarbeiter und andere Personen, mit denen die Organisation in Verbindung steht oder die möglicherweise in Kontakt treten müssen.

Diese Richtlinie beschreibt, wie diese personenbezogenen Daten erhoben, verarbeitet und gespeichert werden müssen, um die Datenschutzstandards des Unternehmens zu erfüllen und die gesetzlichen Bestimmungen einzuhalten.

Warum diese Richtlinie existiert

Diese Datenschutzrichtlinie gewährleistet RP Technologies Ltd:

- Erfüllt die Datenschutzgesetze und folgt den guten Praktiken
- Schützt die Rechte von Mitarbeitern, Kunden und Partnern
- Ist offen darüber, wie Daten von Einzelpersonen gespeichert und verarbeitet werden
- Schützt sich vor den Risiken einer Datenverletzung

Datenschutz Act

Der Datenschutz Act 1998 beschreibt, wie Organisationen - einschließlich RP Technologies Ltd - personenbezogene Daten sammeln, verarbeiten und speichern müssen.

Diese Regeln gelten unabhängig davon, ob Daten elektronisch, auf Papier oder auf anderen Materialien gespeichert sind.

Um dem Gesetz zu entsprechen, müssen persönliche Informationen gesammelt, fair verwendet, sicher gespeichert und nicht rechtswidrig verbreitet werden.

Das Datenschutzgesetz wird durch acht wichtige Grundsätze untermauert. Diese sagen aus, wie persönliche Daten sein müssen:

1. Ffair und rechtmäßig
2. Nur für bestimmte, rechtmäßige Zwecke erhalten werden
3. Angemessen, relevant und nicht übermäßig
4. Genau und auf dem Laufenden

5. Nicht länger als nötig gehalten werden
6. Verarbeitung gemäß den Rechten der betroffenen Personen
7. Auf geeignete Weise geschützt werden
8. Nicht außerhalb des Europäischen Wirtschaftsraums (EWR) übertragen werden, es sei denn, dieses Land oder Territorium gewährleistet auch ein angemessenes Schutzniveau

MENSCHEN, RISIKEN UND VERANTWORTUNG

Diese Richtlinie gilt für:

- Der Hauptsitz von RP Technologies Ltd
- Alle Niederlassungen von RP Technologies Ltd
- Alle Mitarbeiter und Freiwilligen von RP Technologies Ltd
- Alle Auftragnehmer, Lieferanten und andere Personen, die im Auftrag von RP Technologies Ltd handeln,

Dies gilt für alle Daten, die das Unternehmen in Bezug auf identifizierbare Personen erhebt, selbst wenn diese Informationen technisch nicht unter das Datenschutzgesetz von 1998 fallen. Dazu können gehören:

- Namen von Personen
- Postanschriften
- E-mailadressen
- Telefonnummern
- ... und andere Informationen zu Personen

DATENSCHUTZ RISIKEN

Diese Richtlinie hilft RP Technologies Ltd vor einigen sehr realen Sicherheitsrisiken zu schützen, darunter:

- **Verletzungen der Vertraulichkeit.** Zum Beispiel, Informationen werden unsachgemäß gegeben.
- **Fehlende Wahlmöglichkeit.** Zum Beispiel sollten alle Personen frei wählen können, wie das Unternehmen Daten verwendet, die sich auf sie beziehen.
- **Reputationsschäden**. Zum Beispiel könnte das Unternehmen leiden, wenn Hacker erfolgreich Zugriff auf sensible Daten erhalten.

VERANTWORTLICHKEITEN

Jeder, der für oder mit RP Technologies Ltd. arbeitet, trägt Verantwortung dafür, dass die Daten ordnungsgemäß erfasst, gespeichert und verarbeitet werden.

Jedes Team, das personenbezogene Daten verarbeitet, muss sicherstellen, dass es in Übereinstimmung mit diesen Richtlinien und Datenschutzgrundsätzen behandelt und verarbeitet wird.

Diese Menschen haben jedoch zentrale Verantwortungsbereiche:

- Der **Verwaltungsrat** ist letztendlich dafür verantwortlich, dass RP Technologies Ltd seinen gesetzlichen Verpflichtungen nachkommt.
- Jane Mitchell ist verantwortlich für:
  - o Halten Sie den Vorstand über Datenschutz Verantwortlichkeiten, Risiken und Probleme auf dem Laufenden.
  - o Überprüfung aller Datenschutzverfahren und zugehörigen Richtlinien gemäß einem vereinbarten Zeitplan.
  - o Organisation von Datenschutzschulungen und -beratung für die von dieser Richtlinie betroffenen Personen.
  - o Umgang mit Datenschutzfragen von Mitarbeitern und anderen Personen, die unter diese Richtlinie fallen.

o Umgang mit Anfragen von Einzelpersonen, um die Daten zu sehen, die RP Technologies Ltd über sie besitzt (auch "Anfrage personenbezogener Daten" genannt).
o Überprüfung und Genehmigung von Verträgen oder Vereinbarungen mit Dritten, die mit den sensiblen Daten des Unternehmens umgehen können.
• Der **IT-Manager** Brett Mitchell ist verantwortlich für:
o Sicherzustellen, dass alle Systeme, Dienste und Geräte, die zum Speichern von Daten verwendet werden, akzeptable Sicherheitsstandards erfüllen.
o Regelmäßige Überprüfungen und Scans durchführen, um sicherzustellen, dass Hardware und Software ordnungsgemäß funktionieren.
o Bewertung von Drittanbieterdiensten, die das Unternehmen zur Speicherung oder Verarbeitung von Daten in Erwägung zieht. Zum Beispiel Cloud-Computing-Dienste.
• Die **Marketing Managerin** Alison Rait ist verantwortlich für:
o Genehmigung von Datenschutzerklärungen, die mit Mitteilungen wie E-Mails und Briefen verknüpft sind.
o Beantwortung von Datenschutzanfragen von Journalisten oder Medien wie Zeitungen.
o bei Bedarf mit anderen Mitarbeitern zusammenarbeiten, um sicherzustellen, dass Marketinginitiativen die Datenschutzgrundsätze einhalten.

ALLGEMEINE PERSONALRICHTLINIEN

• Die einzigen Personen, die auf die von dieser Richtlinie erfassten Daten zugreifen können, sollten diejenigen sein, die sie für ihre Arbeit benötigen.

• Daten sollten nicht informell ausgetauscht werden. Wenn Zugang zu vertraulichen Informationen erforderlich ist, können Mitarbeiter dies von ihren Vorgesetzten anfordern.

• RP Technologies Ltd bietet allen Mitarbeitern Schulungen an, um ihnen zu helfen, ihre Verantwortlichkeiten beim Umgang mit Daten zu verstehen.

• Mitarbeiter sollten alle Daten sicher aufbewahren, indem sie sinnvolle Vorsichtsmaßnahmen treffen und die folgenden Richtlinien befolgen.

• Insbesondere müssen starke Passwörter verwendet werden und sie sollten niemals geteilt werden.

• Personenbezogene Daten sollten weder innerhalb des Unternehmens noch extern an unbefugte Personen weitergegeben werden.

• Daten sollten regelmäßig überprüft und aktualisiert werden, wenn sie veraltet sind. Wenn es nicht mehr benötigt wird, sollte es gelöscht und entsorgt werden.

• Mitarbeiter sollten Hilfe von ihrem direkten Vorgesetzten oder dem Datenschutzbeauftragten anfordern, wenn sie sich über einen Aspekt des Datenschutzes unsicher sind.

DATENSPEICHER

Diese Regeln beschreiben, wie und wo Daten sicher gespeichert werden sollten. Fragen zur sicheren Speicherung von Daten können an den IT-Manager oder den Datenschutzbeauftragten gerichtet werden.

Wenn Daten auf Papier gespeichert werden, sollten sie an einem sicheren Ort aufbewahrt werden, an dem sie für Unbefugte nicht sichtbar sind.

Diese Richtlinien gelten auch für Daten, die normalerweise elektronisch gespeichert werden, aber aus irgendeinem Grund ausgedruckt wurden:

• Wenn das Papier oder die Dateien nicht benötigt werden, sollten sie in einer verschlossenen Schublade oder einem Aktenschrank aufbewahrt werden.
• Mitarbeiter sollten sicherstellen, dass Papier und Ausdrucke nicht dort liegen, wo sie von unbefugten Personen wie auf einem Drucker gesehen werden können.
• Datenausdrucke sollten zerkleinert und sicher entsorgt werden, wenn sie nicht mehr benötigt werden.

Wenn Daten elektronisch gespeichert werden, müssen sie vor unbefugtem Zugriff, versehentlichem Löschen und böswilligen Hackerversuchen geschützt werden:

• Daten sollten durch starke Kennwörter geschützt sein, die regelmäßig geändert und nie zwischen Mitarbeitern ausgetauscht werden.
• Wenn Daten auf Wechselmedien (z. B. CD oder USB-Laufwerk) gespeichert sind, sollten diese bei Nichtbenutzung sicher aufbewahrt werden.
• Daten sollten nur auf bestimmten Laufwerken und Servern gespeichert werden und sollten nur auf einen zugelassenen Cloud-Computing-Dienst hochgeladen werden.
• Server, die personenbezogene Daten enthalten, sollten sich an einem sicheren Ort befinden, der nicht im allgemeinen Bürobereich liegt.
• Daten sollten häufig gesichert werden. Diese Backups sollten regelmäßig gemäß den Standard-Backup-Verfahren des Unternehmens getestet werden.
• Daten sollten niemals direkt auf Laptops oder anderen mobilen Geräten wie Tablets oder Smartphones gespeichert werden.
• Alle Server und Computer mit Daten sollten durch eine anerkannte Sicherheitssoftware und eine Firewall geschützt sein.

DATEN VERWENDUNG

Personenbezogene Daten haben keinen Wert für RP Technologies Ltd, es sei denn, das Unternehmen kann davon Gebrauch machen. Es ist jedoch möglich, dass beim Zugriff und der Verwendung personenbezogener Daten das größte Risiko für Verlust, Beschädigung oder Diebstahl besteht:

• Bei der Arbeit mit persönlichen Daten sollten Mitarbeiter sicherstellen, dass die Bildschirme ihrer Computer immer gesperrt sind, wenn sie unbeaufsichtigt bleiben.
• Persönliche Daten sollten nicht informell weitergegeben werden. Insbesondere sollte es niemals per E-Mail versendet werden, da diese Form der Kommunikation nicht sicher ist.
• Daten müssen vor der elektronischen Übertragung verschlüsselt werden. Der IT-Manager kann erklären, wie Daten an autorisierte externe Kontakte gesendet werden.
• Personenbezogene Daten sollten niemals außerhalb des Europäischen Wirtschaftsraums übertragen werden.
• Mitarbeiter sollten keine Kopien von persönlichen Daten auf ihren eigenen Computern speichern. Immer auf die zentrale Kopie aller Daten zugreifen und sie aktualisieren.

DATENGENAUIGKEIT

Das Gesetz verpflichtet RP Technologies Ltd, angemessene Schritte zu unternehmen, um sicherzustellen, dass die Daten korrekt und aktuell sind.

Umso wichtiger ist es, dass die persönlichen Daten korrekt sind, umso größer ist der Aufwand, den RP

Technologies Ltd für die Gewährleistung seiner Genauigkeit aufbringen sollte.

Es liegt in der Verantwortung aller Mitarbeiter, die mit Daten arbeiten, verantwortungsvolle Schritte zu unternehmen, um sicherzustellen, dass sie so genau und aktuell wie möglich sind.

• Daten werden an so wenigen Stellen wie nötig gespeichert. Mitarbeiter sollten keine unnötigen zusätzlichen Datensätze erstellen.
• Das Personal sollte jede Gelegenheit nutzen, um sicherzustellen, dass die Daten aktualisiert werden. Zum Beispiel durch Bestätigung der Kundendaten beim Anruf.
• RP Technologies Ltd wird es den betroffenen Personen erleichtern, die Informationen, die RP Technologies Ltd über sie besitzt, zu aktualisieren. Zum Beispiel über die Unternehmens-Website.
• Daten sollten aktualisiert werden, wenn Ungenauigkeiten entdeckt werden. Wenn ein Kunde beispielsweise nicht mehr unter seiner gespeicherten Telefonnummer erreichbar ist, sollte er aus der Datenbank entfernt werden.
• Es liegt in der Verantwortung des Marketing-Managers sicherzustellen, dass Marketing-Datenbanken alle sechs Monate mit Branchen-Unterdrückungsdateien abgeglichen werden.

ABFRAGE PERSOENLICHER DATEN

Alle Personen, die von RP Technologies Ltd unterstützt werden, sind berechtigt:

• Fragen Sie, welche Informationen das Unternehmen über sie hält und warum.
• Fragen Sie, wie Sie darauf zugreifen können.
• Seien Sie informiert, wie Sie auf dem Laufenden bleiben.
• darüber informiert werden, wie das Unternehmen seinen Datenschutzverpflichtungen nachkommt.

Wenn eine Person das Unternehmen anruft, das diese Informationen anfordert, wird dies als Abfrage persönlicher Daten bezeichnet.

Betreff-Zugriffsanfragen von Einzelpersonen sollten per E-Mail an Jane Mitchell unter mailto:info@rptechnologies.de gerichtet werden. Der Datenschutzbeauftragte kann ein Standardanforderungsformular bereitstellen, obwohl Einzelpersonen dies nicht verwenden müssen.

Jane Mitchell überprüft stets die Identität von Personen, die eine Anfrage bezüglich des Zugriffs auf ein Thema stellen, bevor er Informationen ausgibt.

DATEN AUS ANDEREN GRÜNDEN ÜBERMITTELN

Unter bestimmten Umständen erlaubt das Datenschutzgesetz die Weitergabe personenbezogener Daten an Strafverfolgungsbehörden ohne Zustimmung der betroffenen Person.

Unter diesen Umständen wird RP Technologies Ltd die angeforderten Daten offenlegen. Der Datenschutzbeauftragte stellt jedoch sicher, dass die Anfrage legitim ist, und ersucht den Vorstand und gegebenenfalls die Rechtsberater des Unternehmens um Unterstützung.

BEREITSTELLUNG VON INFORMATIONEN

RP Technologies Ltd zielt darauf ab, sicherzustellen, dass Einzelpersonen wissen, dass ihre Daten verarbeitet werden und dass sie verstehen:

- Wie die Daten verwendet werden
- Wie man ihre Rechte ausübt

Zu diesem Zweck hat das Unternehmen eine Datenschutzerklärung, in der dargelegt wird, wie personenbezogene Daten von der Firma verwendet werden.