SENSIBLE PERSONENBEZOGENE DATEN

Während alle Informationen, die eine Person identifizieren oder zur Identifizierung einer Person verwendet werden können, vor unbefugtem Zugriff geschützt werden sollten, gilt bei sensiblen Daten ein höherer Standard. Sensible Daten sind Informationen, deren Veröffentlichung potenziell zu erheblichen Schäden wie Diskriminierung, Identitätsdiebstahl oder Finanzbetrug führen kann. Im Folgenden finden Sie einige Richtlinien, die Sie beim Umgang mit sensiblen Daten beachten sollten.

WISSEN SIE, WARUM SIE ES HABEN

- Kennen und dokumentieren Sie die Gründe, aus denen Sie sensible Daten benötigen, bevor Sie diese sammeln
- Sammeln Sie keine sensiblen Daten, die Sie nicht benötigen
- Fragen Sie Ihren Konzernanwalt, ob Sie eine Einwilligung benötigen, bevor Sie sensible Daten sammeln
- Verwenden Sie keine sensiblen Daten für neue oder andere Zwecke, ohne sich an Ihren Konzernanwalt zu wenden
- Schließen Sie eine DSFA ab, bevor Sie einen Anbieter, ein Tool oder einen Prozess implementieren oder ändern, der sensible Daten verwendet oder sammelt.

PHYSISCH ABSICHERN

- Speichern Sie die sensiblen Daten an einem sicheren Ort mit eingeschränktem Zugriff
- Lassen Sie die sensiblen Daten nicht auf Ihrem Schreibtisch oder anderweitig unbeaufsichtigt
- Überprüfen Sie regelmäßig Dateien und wissen Sie, welche Arten von sensiblen Daten Sie haben
- Geben Sie die sensiblen Daten nicht an Personen weiter, die nicht dazu berechtigt sind oder die sie nicht kennen müssen
- Machen Sie keine unnötigen Kopien sensibler Daten
- Sensible Daten durch Schreddern entsorgen
- Machen Sie keine Fotos von Ihrem Arbeitsbereich, wenn sensible Daten eingesehen werden können

ELEKTRONISCH SICHERN

- Speichern, übertragen und verarbeiten Sie sensible Daten nur in und auf von der IT genehmigten Geräten, Software, Servern und Websites
- Bewahren Sie keine sensiblen Daten auf persönlichen Geräten auf und greifen Sie nicht darauf zu, es sei denn, dies wurde vorab von der IT genehmigt
- Verwenden Sie starke Passwörter oder Verschlüsselung, wenn Sie sensible Daten übertragen oder speichern
- Geben Sie Ihre Anmeldeinformationen oder Verschlüsselungsschlüssel nicht weiter oder stellen Sie sie zur Verfügung.
- Speichern Sie keine personenbezogenen Daten auf Ihrer Festplatte oder Ihrem Desktop
- Beschränken Sie die Berechtigungen und den Zugriff auf sensible Daten, wann immer möglich
- Greifen Sie nicht über eine ungesicherte öffentliche WLAN-Verbindung auf sensible Daten zu

AUFBEWAHRUNG MINIMIEREN

- Bewahren Sie sensible Daten nicht auf unbestimmte Zeit auf
- Weisen Sie allen sensiblen Daten nach Erhalt eine Aufbewahrungsfrist zu
- Sichern Sie keine sensiblen Daten auf einem Gerät oder einer Site, es sei denn, dies wurde im Voraus von der IT genehmigt

PROBLEME BERICHTEN

- Halten Sie nach verdächtigen Aktivitäten Ausschau
- Antworten Sie nicht auf Anfragen nach sensiblen Daten per E-Mail oder Telefon, es sei denn, Sie haben die Legitimität der Anfrage auf andere Weise bestätigt
- Verwenden Sie die Seite meldepflichtige Ereignisse, um Probleme, Bedenken oder Verstöße gegen sensible Daten zu melden
- Zögern Sie nicht, Vorfälle mit sensiblen Daten zu melden

WIR SIND RPM UND UNSER ERFOLG HÄNGT DAVON AB, DASS JEDER VON UNS DEN RICHTIGEN WEG EINSCHLÄGT UND UNSEREN WERT VON 168® ANNIMMT, UM DIE RICHTIGEN ENTSCHEIDUNGEN ZU TREFFEN.

KONTAKTIEREN SIE UNS: DATAPROTECTION@RPMINC.COM

RPM
168168168168168