WRAŻLIWE DANE OSOBOWE

Podczas gdy wszystkie informacje, które identyfikują lub mogą służyć do identyfikacji osoby, powinny być chronione przed nieuprawnionym dostępem, w przypadku danych wrażliwych istnieje wyższy standard. Dane wrażliwe to informacje, które w przypadku publicznego ujawnienia mogą potencjalnie prowadzić do poważnych szkód, takich jak dyskryminacja, kradzież tożsamości lub oszustwo finansowe. Poniżej znajduje się kilka wskazówek, których należy przestrzegać, gdy masz do czynienia z danymi wrażliwymi.

WIESZ, DLACZEGO TO MASZ

- Poznaj i udokumentuj powody, dla których potrzebujesz danych wrażliwych, zanim je zbierzesz
- Nie zbieraj wrażliwych danych, których nie potrzebujesz
- Zapytaj swojego prawnika grupy, czy potrzebujesz zgody przed zebraniem danych wrażliwych
- Nie używaj danych wrażliwych do nowych lub innych celów bez konsultacji z prawnikiem grupy
- Wypełnij DPIA przed wdrożeniem lub zmianą jakiegokolwiek dostawcy, narzędzia lub procesu, który wykorzystuje lub gromadzi dane wrażliwe

FIZYCZNIE ZABEZPIECZ TO

- Przechowuj poufne dane w bezpiecznej lokalizacji z ograniczonym dostępem
- Nie zostawiaj poufnych danych na biurku lub w inny sposób bez opieki
- Regularnie przeglądaj pliki i dowiedz się, jakie typy poufnych danych posiadasz
- Nie udostępniaj wrażliwych danych nikomu, kto nie jest uprawniony do ich posiadania lub nie ma potrzeby ich poznania
- Nie rób niepotrzebnych kopii danych wrażliwych
- Pozbądź się wrażliwych danych przez niszczenie
- Nie rób zdjęć swojego obszaru roboczego, jeśli można wyświetlić poufne dane

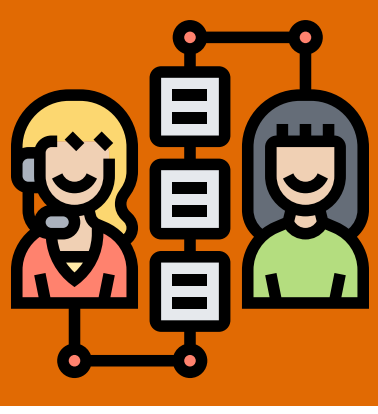
ZABEZPIECZ ELEKTRONICZNIE

- Przechowuj, przesyłaj i przetwarzaj dane wrażliwe wyłącznie w i na urządzeniach, oprogramowaniu, serwerach i stronach internetowych zatwierdzonych przez IT
- Nie przechowuj danych wrażliwych ani nie uzyskuj do nich dostępu na urządzeniach osobistych, chyba że zostało to wcześniej zatwierdzone przez dział IT
- Używaj silnych haseł lub szyfrowania podczas przesyłania lub przechowywania poufnych danych
- Nie udostępniaj ani nie udostępniaj swoich danych logowania ani kluczy szyfrowania
- Nie przechowuj danych osobowych na dysku twardym lub komputerze stacjonarnym
- W miarę możliwości ograniczaj uprawnienia i dostęp do danych wrażliwych
- Nie uzyskuj dostępu do poufnych danych z niezabezpieczonego publicznego połączenia Wi-Fi

MINIMALIZUJ RETENCJĘ

- Nie przechowuj wrażliwych danych w nieskończoność
- Przypisz okres przechowywania wszystkim poufnym danym po otrzymaniu
- Nie twórz kopii zapasowych poufnych danych na żadnym urządzeniu ani w witrynie, chyba że zostało to wcześniej zatwierdzone przez dział IT

ZGŁOŚ PROBLEMY



- Uważaj na podejrzaną aktywność
- Nie odpowiadaj na prośby o dane wrażliwe za pośrednictwem poczty elektronicznej lub telefonu, chyba że w inny sposób potwierdziłeś zasadność żądania
- Użyj strony Zdarzenia podlegające zgłoszeniu, aby zgłosić wszelkie problemy, obawy lub naruszenia wrażliwych danych
- Nie zwlekaj ze zgłaszaniem incydentów z udziałem danych wrażliwych

JESTEŚMY FIRMĄ RPM, A NASZ SUKCES ZALEŻY OD TEGO, CZY KAŻDY Z NAS PODĄŻA WŁAŚCIWĄ DROGĄ I PRZYJMUJE WARTOŚĆ 168®, ABY PODEJMOWAĆ WŁAŚCIWE DECYZJE.

CONTACT US: DATAPROTECTION@RPMINC.COM

RPM
168168168168168