

GEVOELIGE PERSOONLIJKE GEGEVENS

Hoewel alle informatie die een persoon identificeert of kan worden gebruikt om een persoon te identificeren, moet worden beschermd tegen ongeoorloofde toegang, is er een hogere standaard als het gaat om gevoelige gegevens. Gevoelige gegevens zijn informatie die, indien openbaar gemaakt, tot aanzienlijke schade kan leiden, zoals discriminatie, identiteitsdiefstal of financiële fraude. Hieronder vindt u enkele richtlijnen die u moet volgen wanneer u te maken hebt met gevoelige gegevens.



WEET WAAROM JE HET HEBT

- Ken en documenteer de reden(en) waarvoor u gevoelige gegevens nodig heeft voordat u deze verzamelt
- Verzamel geen gevoelige gegevens die u niet nodig heeft
- Vraag uw groepsadvocaat of u toestemming nodig heeft voordat u gevoelige gegevens verzamelt
- Gebruik geen gevoelige gegevens voor nieuwe of andere doeleinden zonder navraag te doen bij uw Groepsadvocaat
- Voltooi een DPIA voordat u een leverancier, tool of proces implementeert of wijzigt dat gevoelige gegevens gebruikt of verzamelt



FYSIEK BEVEILIGEN



- Bewaar de gevoelige gegevens op een veilige locatie met beperkte toegang
- Laat de gevoelige gegevens niet op uw bureau of anderszins onbeheerd achter
- Bekijk regelmatig bestanden en weet welke soorten gevoelige gegevens u heeft
- Deel de gevoelige gegevens niet met iemand die niet geautoriseerd is om ze te hebben of die ze niet hoeft te weten
- Maak geen onnodige kopieën van gevoelige gegevens
- Gooi gevoelige gegevens weg door ze te versnipperen
- Maak geen foto's van uw werkruimte als gevoelige gegevens kunnen worden bekeken

ELEKTRONISCH BEVEILIGEN

- Alleen gevoelige gegevens opslaan, overdragen en verwerken in en op door IT goedgekeurde apparaten, software, servers en websites
- Bewaar of gebruik geen gevoelige gegevens op persoonlijke apparaten, tenzij vooraf goedgekeurd door IT
- Gebruik sterke wachtwoorden of codering bij het overdragen of opslaan van gevoelige gegevens
- Deel of stel uw inloggegevens of coderingssleutels niet beschikbaar
- Bewaar geen persoonlijke gegevens op uw harde schijf of desktop
- Beperk machtigingen en toegang tot gevoelige gegevens waar mogelijk
- Krijg geen toegang tot gevoelige gegevens vanaf een onbeveiligde openbare wifi-verbinding



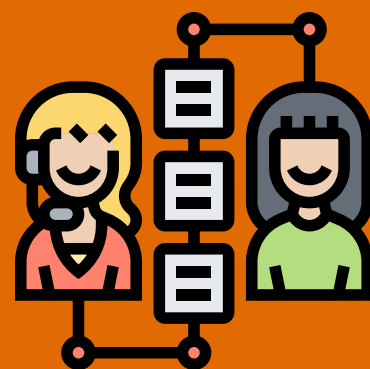
MINIMALISEER RETENTIE



- Bewaar gevoelige gegevens niet voor onbepaalde tijd
- Wijs bij ontvangst een bewaartermijn toe aan alle gevoelige gegevens
- Maak geen back-up van gevoelige gegevens op een apparaat of site, tenzij dit vooraf is goedgekeurd door IT

KWESTIES MELDEN

- Wees op uw hoede voor verdachte activiteiten
- Reageer niet op verzoeken om gevoelige gegevens via e-mail of telefoon, tenzij u de legitimiteit van het verzoek op een andere manier hebt bevestigd
- Gebruik de pagina Rapporteerbare gebeurtenissen om problemen, zorgen of inbreuken op gevoelige gegevens te melden
- Stel geen vertraging in het melden van incidenten met gevoelige gegevens



WIJ ZIJN RPM EN ONS SUCCES HANGT AF VAN HET FEIT DAT IEDER VAN ONS DE JUISTE ROUTE VOLGT EN ONZE VALUE OF 168® OMARMT OM DE JUISTE BESLISSINGEN TE NEMEN.

CONTACTEER ONS: DATAPROTECTION@RPMINC.COM

