

RICHTLIJNEN VOOR HET RAPPORTEREN VAN INBREUK OP PERSOONSGEGEVENS

Datum laatste bijwerking: 10 oktober 2023

Verantwoordelijk team: WireCo Corporate Human Resources & Juridische Zaken

Toepasselijke regio: Europa

Deze richtlijnen gelden voor: Alle werknemers, contractanten, stagiaires en alle anderen die in welke hoedanigheid dan ook werkzaam zijn voor WireCo en zijn gelieerde ondernemingen ("**medewerkers**")

I. Waarom hebben we deze richtlijnen?

Deze WireCo richtlijnen voor het rapporteren van inbreuk op persoonsgegevens zijn bedoeld om de medewerkers van WireCo te ondersteunen bij het identificeren en melden van een daadwerkelijke of potentiële inbreuk op persoonsgegevens aan de verantwoordelijke personen bij WireCo.

Deze richtlijnen zijn gebaseerd op de vereisten voor het omgaan met een inbreuk op persoonsgegevens volgens de regels van de General Data Protection Regulation ("**GDPR**") van de Europese Unie. Van alle medewerkers wordt verwacht dat zij de in deze richtlijnen beschreven aanpak en stappen volgen, zodat WireCo aan zijn toezichthouders een consistente aanpak en naleving van de wettelijke vereisten kan aantonen bij de afhandeling van een inbreuk op persoonsgegevens.

In het kader van de GDPR kan WireCo wettelijk verplicht zijn om zijn toezichthouders in kennis te stellen van bepaalde inbreuken op persoonsgegevens. Om aan deze meldplichten te kunnen voldoen, is het essentieel dat al onze medewerkers begrijpen wat een inbreuk op persoonsgegevens is en dat deze medewerkers helpen bij het identificeren van een daadwerkelijke of potentiële inbreuk op persoonsgegevens.

Deze richtlijnen worden periodiek herzien en waar nodig bijgewerkt door de teams van Corporate Human Resources en Legal om te voldoen aan alle vereisten waaraan WireCo is onderworpen. Zorg ervoor dat je van tijd tot tijd de meest recente versie van deze richtlijnen doorleest. De laatste versie is altijd te vinden op het WireCo-portaal of bij jouw lokale HR-kantoor.

II. Wat zijn de belangrijkste vereisten voor jou?

Je zou:

- moeten begrijpen hoe een daadwerkelijke of potentiële inbreuk op persoonsgegevens kan worden vastgesteld; en
- bekend moeten zijn met de procedures die gevolgd moeten worden als er sprake is van een daadwerkelijke of potentiële inbreuk op persoonsgegevens, zoals deze is uitgelegd in deze richtlijnen.

III. Wat is een inbreuk op persoonlijke gegevens?

Volgens de GDPR is een **inbreuk op persoonsgegevens** een inbreuk op de beveiliging die ertoe leidt dat persoonsgegevens per ongeluk of op onrechtmatige wijze worden vernietigd, verloren, gewijzigd of openbaar gemaakt, geopend, verzonden, opgeslagen of anderszins verwerkt zonder toestemming.

Persoonsgegevens zijn over het algemeen alle informatie die gebruikt kan worden om een persoon te identificeren, direct of indirect. Hieronder vallen bijvoorbeeld met betrekking tot medewerkers hun namen, adressen, e-mailadressen, IP-adressen, rekeningnummers, bankgegevens, ID-nummers en arbeidsgegevens. Het omvat ook persoonsgegevens die WireCo ontvangt en verwerkt namens zijn klanten in verband met het leveren van de diensten van WireCo aan de klanten.

Houd er rekening mee dat onder de GDPR het concept van persoonlijke gegevens breder is dan PII (Personally Identifiable Information) onder de Amerikaanse wetgeving. Dit betekent dat er gegevenscategorieën zijn die onder de GDPR als persoonsgegevens worden aangemerkt, terwijl ze onder de Amerikaanse wetgeving niet als PII worden aangemerkt.

Voorbeelden van de **oorzaken** van inbreuk op persoonsgegevens zijn onder andere:

- handelingen of fouten van werknemers (zoals verlies of diefstal van elektronische apparatuur);
- externe aanvallen door criminele hackers;
- kwetsbaarheden in softwaretoepassingen of bedrijfsprocessen (zoals ongepaste toegangscontroles die ongeoorloofd gebruik mogelijk maken); of
- frauduleuze handelingen.

Inbreuk op persoonsgegevens zijn er in alle soorten en maten, van grootschalige inbreuken die het hele bedrijf treffen tot veel kleinere inbreuken (zoals het versturen van een e-mail naar de verkeerde persoon of het versturen van e-mails naar meerdere externe ontvangers via een open e-maildistributielijst).

Er zijn drie grote categorieën van inbreuk op persoonsgegevens:

1. **Inbreuk op vertrouwelijkheid** - wanneer er sprake is van onbevoegde of onopzettelijke **bekendmaking van of toegang tot** persoonlijke gegevens.
2. **Inbreuk op integriteit** - wanneer er sprake is van een ongeautoriseerde of onopzettelijke **wijziging** van persoonlijke gegevens.
3. **Inbreuk op beschikbaarheid** - wanneer er sprake is van een onopzettelijk of ongeautoriseerd **verlies van toegang** tot of **vernietiging** van persoonlijke gegevens.

IV. Hoe moet je reageren op een daadwerkelijk of mogelijk datalek?

Als je bewust bent of op de hoogte wordt gesteld van een daadwerkelijke of potentiële inbreuk op je persoonlijke gegevens, breng dan onmiddellijk het WireCo Corporate Legal Team op de hoogte via een e-mail naar WirecoLegal@wireco.com. Je kunt een inbreuk ook melden via de Open Reporting Compliance Tool (<https://wireco.ethicspoint.com/>) van WireCo of door een van de onderstaande nummers te bellen.

Als je niet zeker weet of je deze actie moet ondernemen, spreek dan zo snel mogelijk met je directe manager. Kies altijd voor voorzichtigheid. Houd er rekening mee dat de GDPR voorziet



in korte termijnen waarbinnen een inbreuk op persoonsgegevens gemeld moet worden. Tijd is dus van essentieel belang.

Zodra je een daadwerkelijke of potentiële inbreuk op je persoonlijke gegevens hebt gemeld bij de afdeling Human Resources of de juridische afdeling, zullen zij een onderzoek instellen naar de mogelijke inbreuk op je persoonlijke gegevens en mogelijk contact met je opnemen voor meer informatie.

V. Wat moet je niet doen?

Dat moet je niet doen:

- je eigen onderzoeken of enquêtes uitvoeren naar de inbreuk op persoonsgegevens
- proberen records of e-mails, informatie, logs of notities die betrekking kunnen hebben op de inbreuk op persoonsgegevens te wissen of te wijzigen.
- niemand anders dan de afdeling Corporate Human Resources of de juridische afdeling en, indien nodig, je directe leidinggevende informeren over de inbreuk persoonsgegevens of verdere stappen ondernemen, tenzij je hierom bent gevraagd door de afdeling Corporate Human Resources of de juridische afdeling of tenzij stappen van cruciaal belang zijn om te voorkomen dat er schade wordt aangericht.

VI. Met wie kun je contact opnemen als je vragen hebt over deze richtlijnen?

Als je vragen hebt over deze richtlijnen, kun je altijd contact opnemen met je directe leidinggevende, je lokale HR-manager, het Corporate Human Resources of het Legal team.

Telefoonnummers per land:

V.S. - 800-371-2173

Australië - 1-800-551-155 (Optus) of 1-800-881-011 (Telstra), kies daarna: 844-287-1890

Brazilië - 0800-892-0644

China - 108-888, kies daarna: 844-287-1890

Denemarken - 800-100-10, kies daarna: 844-287-1890

Frankrijk - 0800-90-2876

Duitsland - 0-800-225-5288, kies daarna: 844-287-1890

Mexico - 001-800-658-5454, kies daarna: 844-287-1890

Nederland - 0800-022-9111, kies daarna: 844-287-1890

Polen - 00-800-151-0065

Portugal - 800-800-128, kies daarna: 844-287-1890

Rusland - 363-2400, kies daarna: 844-287-1890

Spanje - 900-99-0011, kies daarna: 844-287-1890

Verenigde Arabische Emiraten - 8000-021, kies daarna: 844-287-1890

Verenigd Koninkrijk - 0-800-89-0011, kies daarna: 844-287-1890

