DUTCH WEBSITE NOTICE

17 november 2026

KENNISGEVING VAN EEN INBREUK OP DE BESCHERMING VAN PERSOONSGEGEVENS

WAT IS ER GEBEURD?

Op 25 juli 2026 ontdekten WireCo World Group Inc. en haar dochterondernemingen („WireCo", „wij" of „ons") ongeoorloofde activiteiten op haar interne IT-systemen, waarvan wij vervolgens vernamen dat het ging om een cyberaanval uitgevoerd door een bekende en geavanceerde cybercrimineel. Zodra het incident werd ontdekt, hebben wij de getroffen systemen geïsoleerd en op advies van onze juridische adviseurs externe cyberbeveiligingsexperts ingeschakeld om een uitgebreid onderzoek naar ons interne netwerk uit te voeren en te helpen bij het onderzoek, het indammen van de schade en het herstel. De ongeoorloofde activiteit lijkt te hebben plaatsgevonden tussen 9 juli 2026 en 25 juli 2026. Nadat wij onze interne IT-systemen hadden beveiligd, hebben wij vervolgens vastgesteld dat de cybercrimineel toegang had verkregen tot bepaalde gegevens die persoonsgegevens bevatten en dat hij deze had buitgemaakt. Sinds de ontdekking van de aanval hebben wij continu gewerkt aan het doorlopen van de getroffen gegevens om de persoonsgegevens te identificeren. Het heeft enige tijd geduurd om dit proces te voltooien.

OM WELKE PERSOONSGEGEVENS GAAT HET?

Het incident betrof persoonsgegevens die in het bezit waren van WireCo, waaronder mogelijk:

- Volledige namen en contactgegevens (adressen, telefoonnummers, e-mailadressen)
- Nationale identificatienummers, nationale verzekeringsnummers of sofinummers
- Kopieën van paspoorten of andere door de overheid uitgegeven identiteitsdocumenten
- Geboortedatum
- Bankrekening- en creditcardgegevens

En, indien u in dienst was bij of voor WireCo hebt gewerkt, kunnen de persoonsgegevens ook het volgende omvatten:

- Werknemersgegevens, waaronder functioneringsgesprekken, disciplinaire maatregelen en informatie met betrekking tot vakbondslidmaatschap en strafrechtelijke antecedenten
- Gegevens over afwezigheid en gezondheid (zoals ziekteverzuimgegevens en informatie over de gezondheid op het werk)
- Gegevens van naaste familieleden en contactpersonen voor noodgevallen

WAT ZIJN DE MOGELIJKE GEVOLGEN?

Gezien de aard van de betrokken gegevens bestaat het risico dat u te maken kunt krijgen met:

- Identiteitsdiefstal of identiteitsfraude
- Phishingpogingen (frauduleuze e-mails of berichten die bedoeld zijn om verdere persoonlijke informatie te verkrijgen)
- Financiële fraude, met name wanneer bankgegevens of burgerservicenummers worden misbruikt

- Ongewenst contact of pogingen tot social engineering

Wij willen u eerlijk informeren over deze risico's, zodat u passende maatregelen kunt nemen om uzelf te beschermen.

WAT WIJ DOEN

Vóórdat het incident plaatsvond, beschikten wij over een meerlagig cyberbeveiligingsprogramma, bestaande uit administratieve, technische en organisatorische beveiligingsmaatregelen die bedoeld waren om de kans op en de gevolgen van cyberdreigingen te verminderen en de vertrouwelijkheid, integriteit en beschikbaarheid van onze informatiesystemen en gegevens te beschermen.

Sinds 25 juli 2026 hebben wij diverse maatregelen genomen om ons cyberbeveiligingsprogramma verder te versterken en op het incident te reageren. Wij hebben:

- De getroffen systemen geïsoleerd en beveiligd om verdere ongeoorloofde toegang te voorkomen
- Toonaangevende cyberbeveiligingsspecialisten ingeschakeld om een forensisch onderzoek uit te voeren
- De nationale en lokale gegevensbeschermingsautoriteiten op de hoogte gebracht
- De versleutelde systemen hersteld vanuit beveiligde back-ups
- Verbeterde beveiligingsmaatregelen geïmplementeerd, waaronder extra monitoring en toegangsbeperkingen voor onze IT-systemen
- Een grondige evaluatie van onze informatiebeveiligingsmaatregelen gestart om herhaling te voorkomen

Wij hebben tevens een externe partij ingeschakeld om het dark web te monitoren om vast te stellen of gegevens uit onze systemen op het dark web beschikbaar zijn gesteld. Hoewel de aanvaller een link naar de getroffen bestanden heeft gepubliceerd, zijn er tot op heden geen aanwijzingen dat er persoonsgegevens verkocht zijn of te koop zijn aangeboden, noch is er bewijs van verder misbruik van die gegevens.

WireCo heeft haar medewerkers op de hoogte gebracht van het incident. Wij beschikken echter niet over de contactgegevens van een beperkt aantal voormalige medewerkers, klanten, leveranciers en externe bezoekers. WireCo publiceert daarom deze openbare kennisgeving om de personen te informeren waarmee wij geen rechtstreeks contact kunnen opnemen.

WAT U ZELF KUNT DOEN

Hoewel wij geen kennis hebben van daadwerkelijke of pogingen tot fraude als gevolg van misbruik van persoonsgegevens, noch van financiële schade voor betrokken personen als gevolg van dit incident, raden wij u aan de volgende voorzorgsmaatregelen te nemen:

- **Houd uw bankrekeningen en kredietrapporten in de gaten** — let op ongebruikelijke of ongeautoriseerde transacties en meld deze onmiddellijk aan uw bank.
- **Wees waakzaam tegen phishing** — wees op uw hoede voor onverwachte e-mails, sms-berichten of telefoontjes waarin om persoonlijke gegevens wordt gevraagd, zelfs als deze afkomstig lijken te zijn van een betrouwbare bron.

- **Wijzig uw wachtwoorden** — werk de wachtwoorden voor uw persoonlijke accounts bij, met name wanneer u mogelijk wachtwoorden hebt hergebruikt die vergelijkbaar zijn met die voor de systemen die u op uw werk gebruikt.

Zoals altijd raden wij u aan waakzaam te blijven tegen identiteitsdiefstal en fraude, uw rekeningafschriften te controleren en uw gratis kredietrapporten in de gaten te houden op verdachte activiteiten en fouten.

UW RECHTEN

De toepasselijke privacyregelgeving biedt bepaalde rechten met betrekking tot het gebruik van persoonsgegevens. De mogelijk van toepassing zijnde rechten variëren per rechtsgebied en kunnen onder meer het recht op inzage in uw gegevens, het recht op rectificatie en het recht op verwijdering onder bepaalde omstandigheden omvatten. Indien u een van deze rechten wenst uit te oefenen, dient u een schriftelijk verzoek in te dienen via de hieronder vermelde contactgegevens.

VOOR MEER INFORMATIE

Wij zijn ons ervan bewust dat u ons belangrijke informatie toevertrouwt, en wij willen u laten weten dat wij dit incident en de beveiliging en bescherming van uw persoonsgegevens zeer serieus nemen. Wij betreuren het ten zeerste dat dit incident heeft plaatsgevonden. Mocht u vragen of opmerkingen hebben, neem dan contact op met Daniel Burch via DanBurch@WireCo.com.

Informatie over de verwerkingsverantwoordelijke

RECHTSGEBIED	VERWERKINGSVERANTWOORDELIJKE
Denemarken	**Euronete Scandinavia A/S** **Adres:** Gothersgade 48, 7000 Fredericia, Denemarken
Frankrijk	**Le Drezen SAS** **Adres:** 12 rue de Kelareun, 29730 Guilvinec-Treffiagat, Frankrijk
Duitsland	**WireCo Germany GmbH** **Adres:** Casarstraße 1, 66459 Kirkel-Limbach, Duitsland
Nederland	**Lankhorst Engineered Products B.V.** **Adres:** Prinsengracht 2, 8607AD, Sneek, Nederland **Ekon B.V.** **Adres:** Holtum-Noordweg 8, 6121 RE Born, Nederland **Lankhorst Touwfabrieken B.V.** **Adres:** Marconiweg 24, 3316 AM Dordrecht, Nederland **Royal Lankhorst-Euronete Group B.V.** **Adres:** Prinsengracht 2, 8607AD, Sneek, Nederland
Polen	**WireCo Poland sp. z o.o** **Adres:** Polna 26/74, 87-806 Włocławek, Polen
Portugal	**Oliveira Sá, S.A.** **Adres:** Rua Do Outeiro, 906, 4475-150, Maia, Portugal **Lankhorst Euronete Portugal, S.A.** **Adres:** Rua da Cerfil (Cap. Gramaxo) nr. 45, 4475-468, Maia, Portugal
Verenigd Koninkrijk	**Euronete (UK) Limited** **Adres:** Enerfield Business Park, Foveran, Ellon, Newburgh Aberdeenshire, AB41 6AL, Verenigd Koninkrijk
Brazilië	**WireCo do Brasil Ltda** **Adres:** Rua Minas Gerais 1920, Distrito Industrial Queimados, Rio de Janeiro, Brazilië

	Lankhorst-Euronete (Brazilië) – Indústria e Comércio Ltda **Adres:** Rua Minas Gerais 1920, Distrito Industrial Queimados, Rio de Janeiro, Brazilië
Mexico	**Aceros Camesa S.A. de C.V.** **Adres:** Margarita Maza de Juárez 159, Nueva Industrial Vallejo, Gustavo A. Madero, Mexico-Stad 07700
Australië	**WireCo Australia Pty Ltd** **Adres:** 7 Demand Avenue, Arundel QLD 4214, Australië