FRENCH WEBSITE NOTICE

17 novembre 2026

INFORMATION CONCERNANT UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

QUE S'EST-IL PASSÉ ?

Le 25 juillet 2026, WireCo World Group Inc. et ses filiales (« WireCo », « nous » ou « notre ») ont détecté une activité non autorisée sur leurs systèmes informatiques internes, dont nous avons par la suite appris qu'il s'agissait d'une cyberattaque menée par un acteur malveillant connu et sophistiqué. Dès la découverte de l'incident, nous avons isolé les systèmes affectés et fait appel à des experts externes en cybersécurité, sur les conseils de nos avocats, afin de mener un examen approfondi de notre réseau interne et nous assister dans les opérations d'investigation, de confinement et de remédiation. L'activité non autorisée semble avoir eu lieu entre le 9 juillet 2026 et le 25 juillet 2026.

Après avoir sécurisé nos systèmes informatiques internes, nous avons par la suite déterminé que l'acteur malveillant avait accédé à certaines informations contenant des données à caractère personnel et les avait exfiltrées. Depuis la découverte de l'attaque, nous travaillons continuellement à l'examen des données impactées afin d'identifier les données à caractère personnel concernées. Ce processus a nécessité un certain temps.

QUELLES DONNÉES À CARACTÈRE PERSONNEL ONT ÉTÉ CONCERNÉES ?

L'incident a concerné des données à caractère personnel détenues par WireCo, qui peuvent notamment inclure :

- Noms complets et coordonnées (adresses postales, numéros de téléphone, adresses e-mail)
- Numéros d'identification nationaux, numéros de sécurité sociale
- Copies du passeport ou d'une pièce d'identité délivrée par une autorité publique
- Date de naissance
- Coordonnées bancaires et informations relatives aux cartes de crédit

Et, si vous avez été employé(e) par WireCo ou avez travaillé pour WireCo, les données à caractère personnel peuvent également inclure :

- Dossiers professionnels, y compris les évaluations professionnelles, les dossiers disciplinaires et des informations relatives à l'appartenance syndicale et aux antécédents en matière d'infractions pénales
- Données relatives aux absences et à la santé (telles que les dossiers médicaux et les informations relatives à la médecine du travail)
- Coordonnées des proches et des personnes à contacter en cas d'urgence

QUELLES SONT LES CONSÉQUENCES POSSIBLES ?

Compte tenu de la nature des données concernées, vous pourriez être exposé(e) aux risques suivants :

- Vol d'identité ou usurpation d'identité

- Tentatives d'hameçonnage (e-mails ou messages frauduleux visant à obtenir davantage de données à caractère personnel)
- Fraude financière, notamment si vos coordonnées bancaires ou votre numéro de sécurité sociale sont utilisés de manière abusive
- Contacts non sollicités ou tentatives d'ingénierie sociale

Nous tenons à vous informer en toute transparence de ces risques afin que vous puissiez prendre les mesures appropriées pour vous protéger.

CE QUE NOUS FAISONS

Avant l'incident, nous disposions d'un programme de cybersécurité à plusieurs niveaux comprenant des mesures de sécurité administratives, techniques et organisationnelles destinées à réduire la probabilité et l'impact des cybermenaces, ainsi qu'à protéger la confidentialité, l'intégrité et la disponibilité de nos systèmes d'information et de nos données.

Depuis le 25 juillet 2026, nous avons pris plusieurs mesures pour renforcer encore notre programme de cybersécurité et faire face à cet incident. Nous avons procédé à :

- L'isolation et la sécurisation des systèmes affectés afin d'empêcher tout nouvel accès non autorisé
- L'engagement de spécialistes de premier plan en cybersécurité pour mener une analyse forensique
- L'information des autorités nationales et locales chargées de la protection des données à caractère personnel
- La restauration des systèmes chiffrés à partir de sauvegardes sécurisées
- L'implémentation de contrôles de sécurité renforcés, incluant la mise en place d'une surveillance accrue et des restrictions d'accès à nos systèmes informatiques
- Un examen approfondi de nos mesures de sécurité de l'information afin d'éviter qu'un tel incident ne se reproduise

Nous avons également fait appel à un tiers pour effectuer une surveillance du dark web afin de déterminer si des données provenant de nos systèmes ont été mises à disposition sur le dark web. Bien qu'un lien vers les fichiers impactés ait été publié par l'acteur malveillant, nous n'avons, à ce jour, connaissance d'aucun élément indiquant que des données à caractère personnel aient été vendues ou mises en vente, et aucune preuve ne démontre qu'elles ont fait l'objet d'une autre utilisation abusive.

WireCo a informé ses employés actuels de l'incident. Toutefois, nous ne disposons pas des coordonnées d'un petit nombre d'anciens employés, clients, fournisseurs et visiteurs externes. WireCo publie donc le présent avis afin d'informer les personnes qu'elle n'est pas en mesure de contacter directement.

CE QUE VOUS POUVEZ FAIRE

Bien que nous n'ayons connaissance d'aucune fraude ou tentative de fraude résultant d'une utilisation abusive de données à caractère personnel, ni d'aucun préjudice financier subi par les

personnes concernées à la suite de cet incident, nous vous recommandons de prendre les précautions suivantes :

- **Surveillez vos comptes bancaires** : soyez attentif(ve) à toute transaction inhabituelle ou non autorisée et signalez-la immédiatement à votre banque.
- **Restez vigilant(e) face au phishing** : méfiez-vous des e-mails, SMS ou appels téléphoniques inattendus vous demandant des informations personnelles, même s'ils semblent provenir d'une source fiable.
- **Modifiez vos mots de passe** : mettez à jour les mots de passe de vos comptes personnels, en particulier si vous avez réutilisé des mots de passe similaires à ceux utilisés pour vos systèmes professionnels.

Comme toujours, nous vous encourageons à rester vigilant(e) face aux risques d'usurpation d'identité et de fraude et à consulter vos relevés de compte afin de détecter toute activité suspecte ou anomalie.

VOS DROITS

La réglementation relative à la protection des données à caractère personnel vous confère certains droits concernant l'utilisation de vos données à caractère personnel. Les droits potentiellement applicables varient selon les juridictions et peuvent inclure le droit d'accès à vos données à caractère personnel, le droit de rectification et, dans certaines circonstances, le droit à l'effacement. Si vous souhaitez exercer l'un de ces droits, veuillez envoyer une demande écrite en utilisant les coordonnées fournies ci-dessous.

POUR PLUS D'INFORMATIONS

Nous savons que vous nous confiez des informations importantes, et nous tenons à vous assurer que nous prenons cet incident, ainsi que la sécurité et la protection de vos données à caractère personnel, très au sérieux. Nous regrettons sincèrement que cet incident se soit produit. Si vous avez des questions ou des préoccupations, veuillez contacter Daniel Burch à l'adresse DanBurch@WireCo.com.

INFORMATIONS RELATIVES AUX RESPONSABLES DU TRAITEMENT

JURIDICTION	RESPONSABLE DU TRAITEMENT
Danemark	**Euronete Scandinavia A/S** Adresse : Gothersgade 48, 7000 Fredericia, Danemark
France	**Le Drezen SAS** Adresse : 12 rue de Kelareun, 29730 Guilvinec-Treffiagat, France
Allemagne	**WireCo Germany GmbH** Adresse : Casarstraße 1, 66459 Kirkel-Limbach, Allemagne
Pays-Bas	**Lankhorst Engineered Products B.V.** Adresse : Prinsengracht 2, 8607AD Sneek, Pays-Bas **Ekon B.V.** Adresse : Holtum-Noordweg 8, 6121 RE Born, Pays-Bas **Lankhorst Touwfabrieken B.V.** Adresse : Marconiweg 24, 3316 AM Dordrecht, Pays-Bas **Royal Lankhorst-Euronete group B.V.** Adresse : Prinsengracht 2, 8607AD Sneek, Pays-Bas
Pologne	**WireCo Poland sp. z o.o.** Adresse : Polna 26/74, 87-806 Włocławek, Pologne
Portugal	**Oliveira Sá, S.A.** Adresse : Rua Do Outeiro, 906, 4475-150 Maia, Portugal **Lankhorst Euronete Portugal, S.A.** Adresse : Rua da Cerfil (Cap. Gramaxo), nº 45, 4475-468 Maia, Portugal
Royaume-Uni	**Euronete (UK) Limited** Adresse : Enerfield Business Park, Foveran, Ellon, Newburgh, Aberdeenshire, AB41 6AL, Royaume-Uni
Brésil	**WireCo do Brasil Ltda** Adresse : Rua Minas Gerais 1920, Distrito Industrial Queimados, Rio de Janeiro, Brésil **Lankhorst-Euronete (Brasil) – Indústria e Comércio Ltda** Adresse : Rua Minas Gerais 1920, Distrito Industrial Queimados, Rio de Janeiro, Brésil
Mexique	**Aceros Camesa S.A. de C.V.** Adresse : Margarita Maza de Juárez 159, Nueva Industrial Vallejo, Gustavo A. Madero, Mexico 07700, Mexique
Australie	**WireCo Australia Pty Ltd** Adresse : 7 Demand Avenue, Arundel QLD 4214, Australie