17 November 2026

NOTICE OF PERSONAL DATA BREACH

WHAT HAPPENED?

On 25 July 2026, WireCo World Group Inc. and its subsidiaries ("WireCo," "we," or "us") discovered unauthorised activity on its internal IT systems, which we subsequently learned was a cyberattack carried out by a known and sophisticated threat actor. Upon discovering the incident, we isolated affected systems and engaged external cybersecurity experts at the direction of counsel to conduct a comprehensive review of our internal network and assist with the investigation, containment, and remediation. The unauthorised activity appears to have occurred between 9 July 2026 and 25 July 2026. After securing our internal IT systems, we subsequently determined that the threat actor had accessed and exfiltrated certain data containing personal information. Since discovering the attack we have been working continuously to review the impacted data to identify personal data. This process has taken time to complete.

WHAT PERSONAL DATA WAS INVOLVED?

The incident involved personal data held by WireCo, which may include:

- Full names and contact details (home addresses, telephone numbers, email addresses)
- National Identification numbers, National Insurance or Social Security numbers
- Copies of passport or government issued identification documentation
- Date of birth
- Bank account and credit card information

And, if you were an employee or worked for WireCo, the personal data may also include:

- Employment records, including performance reviews, disciplinary records and information relating to trade union membership and criminal offence history
- Absence and health-related data (such as sickness records and occupational health information)
- Next-of-kin and emergency contact details

WHAT ARE THE LIKELY CONSEQUENCES?

Given the nature of the data involved, there is a risk that you could be subject to:

- Identity theft or identity fraud
- Phishing attempts (fraudulent emails or messages designed to obtain further personal information)
- Financial fraud, particularly where bank details or National Insurance or Social Security numbers are misused
- Unwanted contact or social engineering attempts

We want to be honest with you about these risks so that you can take appropriate steps to protect yourself.

WHAT WE ARE DOING

Prior to the incident, we maintained a multi-layered cybersecurity programme comprising administrative, technical, and organisational security measures designed to reduce the likelihood and impact of cyber threats and to protect the confidentiality, integrity, and availability of our information systems and data.

Since 25 July 2026, we have taken several steps to further strengthen our cybersecurity programme and respond to the incident. We have:

- Isolated and secured the affected systems to prevent further unauthorised access
- Engaged leading cybersecurity specialists to conduct a forensic investigation
- Notified national and local data protection authorities
- Restored encrypted systems from secure backups
- Implemented enhanced security controls, including additional monitoring and access restrictions on our IT systems
- Commenced a thorough review of our information security measures to prevent recurrence

We also have engaged a third party to conduct dark web monitoring to determine whether data from our systems has been made available on the dark web. Although a link to the impacted files has been published by the threat actor, to date, we are not aware of any indication that any personal data has been sold or offered for sale, nor has there been evidence of any further misuse of that data.

WireCo has notified its current employees of the incident. However, we do not hold contact details for a small number of former employees, customers, suppliers and external visitors. WireCo is therefore issuing this public notice in order to notify those individuals who it is unable to contact directly.

WHAT YOU CAN DO

While we are not aware of any actual or attempted fraud resulting from misuse of personal information or any financial harm to involved individuals as a result of this incident, we recommend that you take the following precautionary steps:

- **Monitor your bank accounts and credit reports** — look out for any unusual or unauthorised transactions and report these to your bank immediately.
- **Be vigilant against phishing** — be cautious of unexpected emails, text messages, or telephone calls requesting personal information, even if they appear to come from a trusted source.
- **Change your passwords** — update passwords for personal accounts, particularly where you may have reused passwords similar to those used for work systems.

As always, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports for suspicious activity and to detect errors.

YOUR RIGHTS

Data protection laws provide certain rights regarding the use of personal data. The potentially applicable rights vary by jurisdiction and may include the right to access your data, the right to

rectification, and the right to erasure in certain circumstances. If you want to exercise any of these rights, please submit a written request using the contact information provided below.

FOR MORE INFORMATION

We know that you trust us with important information, and we want you to know that we take this incident and the security and protection of your personal information seriously. We sincerely regret that this incident occurred. If you have any questions or concerns, please contact Daniel Burch at DanBurch@WireCo.com.

Controller Information

JURISDICTION	DATA CONTROLLER
Denmark	**Euronete Scandinavia A/S** **Address:** Gothersgade 48, 7000 Fredericia, Denmark
France	**Le Drezen SAS** **Address:** 12 rue de Kelareun, 29730 Guilvinec-Treffiagat, France
Germany	**WireCo Germany GmbH** **Address:** Casarstraße 1, 66459 Kirkel-Limbach, Germany
Netherlands	**Lankhorst Engineered Products B.V** **Address:** Prinsengracht 2, 8607AD, Sneek, Netherlands **Ekon B.V.** **Address:** Holtum-Noordweg 8, 6121 RE Born, Netherlands **Lankhorst Touwfabrieken B.V.** **Adress:** Marconiweg 24, 3316 AM Dordrecht, Netherlands **Royal Lankhorst-Euronete group B.V.** **Address:** Prinsengracht 2, 8607AD, Sneek, Netherlands
Poland	**WireCo Poland sp. z o.o** **Address:** Polna 26/74, 87-806 Włocławek, Poland
Portugal	**Oliveira Sá, S.A.** **Address:** Rua Do Outeiro, 906, 4475-150, Maia, Portugal **Lankhorst Euronete Portugal, S.A.** **Address:** Rua da Cerfil , (Cap.Gramaxo) nº45, 4475-468, Maia, Portugal
United Kingdom	**Euronete (UK) Limited** **Address:** Enerfield Business Park, Foveran, Ellon, Newburgh Aberdeenshire, AB41 6AL, UK
Brazil	**WireCo do Brasil Ltda** **Address:** Rua Minas Gerais 1920, Distrito Industrial Queimados, Rio de Janeiro, Brazil

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