

Whistleblowing Channel Privacy Policy

Oliveira Sá, S.A and Lankhorst Euronete Portugal, S.A, hereafter jointly referred to as "WireCo Portugal" are the data controllers in relation to the complaints submitted through the complaint channel in regarding each of them respectively.

WireCo Portugal informs you of its privacy policy regarding the processing of personal data in the context of the communication channel implemented for the reporting of breaches. The processing of personal data and its security are in compliance with the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016), as well as with the respective national implementation law (Law no. 58/2019, of 8 August), Decree Law no.109-E/2021, of 9 December and Law no. 93/2021, of 20 December. Your data is collected and processed within the scope of the implemented whistleblowing channel.

Data controller: Oliveira Sá, S.A and Lankhorst Euronete Portugal, S.A are each the data controllers for the processing of your personal data arising from the reports that concern each entity.

Purposes of data processing: The personal data will be processed for the purpose of managing breach reports, as well as investigation and resolution of breaches related to acts or omissions contrary to the rules contained in European Union acts as well as related to the national rules that implement them in the civil, criminal and administrative offense jurisdictions. Personal data is also processed for the purpose of communication with whistleblowers when their identity is known, as well as with third parties as witnesses called for the investigation and resolution of the reported breach.

Categories of data and data subjects: identification, contact and professional data of whistleblowers and reported persons and all data relevant to the process of analyzing and investigating the report may be processed in the context of the whistleblowing channel.

Lawfulness of processing: The processing of personal data within the whistleblowing channel is based on WireCo Portugal's legitimate interest in the collection and investigation of the allegations made, as well as compliance with legal obligations of corruption prevention and whistleblower protection, including the implementation and management of whistleblowing channels.

Data subject rights: data subjects may exercise their rights of access, rectification, erasure, objection, restriction of processing, portability and the right to withdraw consent in accordance with the GDPR, with the limitations of Law no. No. 59/2019, of August 8, which approves the rules on the processing of personal data for the purposes of prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties transposing Directive (EU) 2016/680 of the

European Parliament and of the Council, by sending a communication addressed to the Data Protection Officer via e-mail _____ or by post, to:

Oliveira Sá, S.A
Rua do Outeiro, 906 4475-150 Maia, Porto

Lankhorst Euronete Portugal, S.A
R da Cerfil 4475-468 Maia, Porto

The data subject may lodge a complaint with the supervisory authority (in Portugal, Comissão Nacional de Proteção de Dados) through the website: www.cnpd.pt.

Data retention: Personal data will be kept for a period of 5 (five) years and independently of this period, for as long as necessary for the purposes, namely during the pendency of judicial or administrative proceedings concerning the reports.

Security measures: The security measures implemented are in compliance with the GDPR and other applicable legislation. Technical and organizational measures were implemented in compliance with the GDPR, to ensure the confidentiality, integrity and availability of data, namely through data pseudonymization and encryption measures, backups and recovery measures in case of incident, as well as access control through the definition of access profiles, by assessing the need to know.

Data transfers: In order to ensure the proper operation of the reporting channel, your data may be communicated to data processors, which implies access to the data, by these entities. When this happens, we take appropriate, contractually prescribed steps to ensure that these third parties provide sufficient and adequate guarantees to perform technical and organizational measures and that they will act only in accordance with our instructions.

Similarly, your data may be transferred to third countries outside the European Economic Area, in particular the United States of America. In this case, we will strictly comply with applicable legal provisions and determine the adequacy of the country or organization in question with regard to the requirements applicable to such transfers. In particular, we will ensure that data transmission is secure, that third parties respect the confidentiality of the data received, that they do not use the data for any purpose other than the purpose for which it was transmitted or for their own benefit or that of any third party.

Questions and information: For any question or request for clarification the Data Protection Officer should be contacted through the contact identified above.