

(EU) DATA PROTECTION NOTICE FOR WHISTLEBLOWING SYSTEM

Last modified: December 2020

INTRODUCTION

This notice describes the types of personal data that Ferro Corporation (“Ferro”, the “Company,” “we,” “our,” or “us”) collects when a report (“Report”) is submitted to Company relating to potential serious compliance violations in identified categories, the purposes for which we collect that personal data, the other parties with whom we may share such personal data and the measures we take to protect the security of the data. It also tells you about your rights and choices with respect to personal data and how you can contact us about our data protection practices.

A Report can be submitted either (i) by calling Ferro Corporation’s Legal and Ethical Conduct Hotline (“Hotline”) provided by Lighthouse Services, LLC; or (ii) by using the Lighthouse anonymous reporting system (“Whistleblowing System”) accessible on the Ferro Legal and Ethical Conduct Hotline Web Portal (“Portal”) at the following link www.intouchwebsite.com/ferrohotline (“Website”). This notice applies to individuals submitting a report (“Whistleblowers”) and to individual(s) mentioned in the Report (“Involved Individual(s)").

Please note that the Whistleblowing System is only one method of reporting potential violations, and the usual reporting channels, via direct supervisors or Company management are always the preferred option.

TABLE OF CONTENT

[WHAT IS THE PURPOSE OF THE WHISTLEBLOWING SYSTEM AND HOTLINE?](#)

[WHO IS RESPONSIBLE FOR THE PROCESSING OF YOUR PERSONAL DATA?](#)

[HOW IS YOUR PERSONAL DATA SECURED?](#)

[WHAT TYPES OF PERSONAL DATA DOES FERRO PROCESS?](#)

[FOR WHICH PURPOSES DOES FERRO PROCESS PERSONAL DATA?](#)

[WHO ARE THE RECIPIENTS OF THE REPORT?](#)

[HOW DOES FERRO DEAL WITH INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA?](#)

[WHAT KIND OF INFORMATION WILL THE INVOLVED INDIVIDUAL\(S\) IN THE REPORT RECEIVE?](#)

[WHAT ARE THE DATA PROTECTION RIGHTS?](#)

[WHERE DOES YOUR PERSONAL DATA COME FROM?](#)

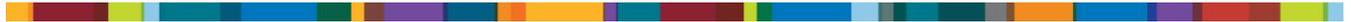
[HOW LONG DOES FERRO RETAIN YOUR PERSONAL DATA FOR?](#)

WHAT IS THE PURPOSE OF THE WHISTLEBLOWING SYSTEM AND HOTLINE?

The Hotline and the Whistleblowing System serve the purpose of securely and confidentially receiving, processing and managing Reports regarding severe violations of European Union (“EU”) and EU Member States laws in certain areas such as, without limitation, public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; product safety and compliance; protection of the environment; protection of privacy and personal data, and security of network and information systems.

Disciplinary measures and/or legal prosecution will be undertaken in case of any abuse or misuse of the Hotline and Whistleblowing System (e.g., submission of false statements in a malicious way against individuals).

(EU) DATA PROTECTION NOTICE FOR WHISTLEBLOWING SYSTEM



WHO IS RESPONSIBLE FOR THE PROCESSING OF YOUR PERSONAL DATA?

The data controller for the purposes of processing personal data in the context of the Hotline and the Whistleblowing System is Ferro Corporation, with a registered office at 6060 Parkland Boulevard, Mayfield Height, Ohio 44124 USA.

Questions, comments, and requests regarding this notice may be addressed to the Director, Risk & Compliance at FerroCompliance@Ferro.com or you may contact our EU Data Protection Coordinator at the following email address: DataProtectionEU@Ferro.com or phone number: +31 10 4784 935.

HOW IS YOUR PERSONAL DATA SECURED?

Operator

The Whistleblowing System is operated by a specialized company, Lighthouse Services, LLC, located at 1710 Walton Road, Suite 204, Blue Bell, PA 19422 USA, on behalf of Ferro.

Security of Personal Data

We will take all reasonable steps to ensure that your data, processed in the context of the Whistleblowing System and the Hotline, is treated securely and in accordance with this privacy policy. Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we have put in place appropriate technical and organizational security measures to protect your data against loss, misuse, unauthorized access, disclosure or alteration.

The security of personal data processed in the context of the Whistleblowing System and the Hotline is ensured by extensive technical and organizational measures. All data stored are encrypted with multiple levels of logical security so that access is restricted to a very small selection of expressly authorized persons at Ferro Corporation. For a more detailed description of the system security strategies, please contact Ferro's Director of Risk and Compliance.

Access to Personal Data

Lighthouse Services, LLC operates a database, in a secured data center, operated by Iron Mountain Data Centers, LLC, that stores the personal data and information processed by the Whistleblowing System and the Hotline. The personal data and information processed by the Whistleblowing System and the Hotline is only accessible to Ferro and Lighthouse Services, LLC. Other third parties do not have access to the personal data and information.

WHAT TYPES OF PERSONAL DATA DOES FERRO PROCESS?

The use of the Whistleblowing System is voluntary. If the Whistleblower submits a Report through the Hotline or the Whistleblowing System, Ferro processes the following personal data that the Whistleblower chooses to provide:

- The name and contact information of the Whistleblower, if he or she chooses to reveal his or her identity;
- The name and surname of persons to whom the Whistleblower reported the violation provided in the Report (i.e., any person responsible for supervision or management and any person outside of Ferro);
- The name and surname of the Involved Individual(s) in the Report;

(EU) DATA PROTECTION NOTICE FOR WHISTLEBLOWING SYSTEM



- Whether the Whistleblower is employed at or in a business relationship with Ferro; and
- Whether the Involved Individual(s) is employed at or in a business relationship with Ferro.

We will also collect additional information and personal data that the Whistleblower chooses to provide us with. The processing of personal data will however be limited to personal data strictly necessary to verify the allegations.

FOR WHICH PURPOSES DOES FERRO PROCESS PERSONAL DATA?

The processing of personal data through the Hotline and the Whistleblowing System is undertaken for the following purposes and corresponding legal basis:

Purpose	Legal Basis
Detecting and preventing misconduct and avoid damage to Ferro, its subsidiaries, its affiliates, its employees and customers, including carrying out investigations regarding the Report.	Legitimate interests.
Compliance with legal obligations Ferro is subject to.	Legal obligation

WHO ARE THE RECIPIENTS OF THE REPORT?

Subject to any applicable laws and regulations, we disclose personal data that we collect or that you provide in the Report to the following recipients:

Within our organization

- Incoming Reports are received by a limited selection of expressly authorized staff members employed by Ferro, its subsidiaries and affiliates competent to receive such Reports (“Authorized Staff Members”) (e.g., Ferro’s Risk & Compliance Director). Authorized Staff Members handle Reports confidentially and perform a comprehensive assessment of the subject matter to protect the interests of the Company.
- During the processing of a Report and in the course of an investigation, it may become necessary to share the information and personal data with additional employees of the Company, its subsidiaries and affiliates in and outside the EU.

To third parties

- The Hotline and Whistleblowing System service provider also has access to your personal data and the information included in the Report.
- It may also be necessary to share information and personal data to other external service providers (e.g., lawyers, auditors, etc.) and public authorities and officials (e.g., prosecutors, judges, etc.) to protect the interests of the Company.
- Your personal data may also be disclosed to a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal data held by the Company is among the assets transferred.

Ferro will only grant access to personal data on a strict need-to know basis.

(EU) DATA PROTECTION NOTICE FOR WHISTLEBLOWING SYSTEM

HOW DOES FERRO DEAL WITH INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA?

Ferro ensures (i) that appropriate safeguards are implemented to secure transfers of personal data outside of the EU; and (ii) that such data transfers are in compliance with applicable data protection laws. The Company is committed to adequately protect personal data relating to the Whistleblower and to the Involved Individual(s) mentioned in the Report.

We have therefore implemented international data transfer agreements based on EU Standard Contractual Clauses to cover our international data transfers and a copy of these clauses can be obtained by contacting the EU Data Protection Coordinator.

WHAT KIND OF INFORMATION WILL THE INVOLVED INDIVIDUAL(S) IN THE REPORT RECEIVE?

We are bound by law to inform the Involved Individual(s) in the Report that we have received a report containing personal data concerning him or her, unless the notification jeopardizes the investigations. In such a case, notification to the Involved Individual(s) in the Report may be delayed as long as such risk exists.

WHAT ARE THE DATA PROTECTION RIGHTS?

The Whistleblower and the Involved Individual(s) in the Report have the following data protection rights:

- Right to access to, rectification and erasure of personal data;
- Right to restriction of processing;
- Right to object to the processing of personal data. If the right of objection is exercised, we will immediately examine to what extent the stored data is still necessary for the processing of a Report. Personal data is immediately deleted when it is no longer required;
- Right to lodge a complaint with the supervisory authority; and
- Right to withdraw consent where the processing is based on consent (i.e. where the Whistleblower consented to disclosing his/her identity to the Involved Individual(s) when submitting the Report)

These data protection rights can be exercised at any time by contacting the EU Data Protection Coordinator.

However, the exercise of these rights may be restricted or delayed not to jeopardize an investigation taking place in the context of the Report, as well as to ensure the protection of the rights and freedoms of others involved in the particular case.

The Involved Individual(s) will not be able to obtain information relating to the identity of the Whistleblower on the basis of his or her right of access to data, except if the allegations made reveal themselves as maliciously made false statements or if the Whistleblower consents to such disclosure.

WHERE DOES YOUR PERSONAL DATA COME FROM?

Personal data relating to the Whistleblower is provided by the Whistleblower himself or herself, if he or she chooses to reveal his or her identity.

Personal data relating to the Involved Individual(s) in the Report is provided to Ferro by the Whistleblower when he or she submits a Report.

(EU) DATA PROTECTION NOTICE FOR WHISTLEBLOWING SYSTEM



We have to disclose the name of the Whistleblower to the Involved Individual(s) subject to consent by the Whistleblower and at the latest one month after the Report was made.

HOW LONG DOES FERRO RETAIN YOUR PERSONAL DATA FOR?

We will not retain personal data processed longer than allowed under the applicable data protection laws. In any case, we will not retain it longer than such personal data is necessary for the purpose for which it was collected or otherwise processed, subject to applicable local retention requirements. As a general rule, personal data processed in the context of the Report will be deleted within twelve (12) months of completion of the investigation, except for personal data from reports coming from the EU, in which case such personal data will be deleted within two (2) months of the completion of the investigation, subject to exceptions under applicable law regarding the facts alleged in a Report.

Where legal proceedings or disciplinary measures are initiated against the Whistleblower or the Involved Individual(s) in the Report, personal data will be retained until the conclusion of these proceedings and the period allowed for any appeal, subject to applicable national laws. In addition, personal data will be stored as long as the applicable statutory provisions require Ferro to do so. Personal data relating to unfounded allegations will be deleted without delay once determined unfounded.