FENEGA
NEW LIFE FOR METALS

SECURITY POLICY FOR THE PROTECTION OF PERSONAL DATA (PRIVACY POLICY)

At **FENEGA, s.r.o.** (hereinafter referred to as the “Company”), we regard information as an essential asset that we manage in accordance with our adopted strategy, which is based on three core pillars: **people, their expertise, and modern technologies**. The applied security policy system reflects all requirements for maintaining the confidentiality, integrity, and availability of information..

Foundations of the Personal Data Protection Policy

1. In collecting personal data, the Company informs clearly, honestly, and transparently about the nature of the personal data it collects and the purpose for which it intends to use it. The use of personal data by the Company for any purpose other than the one initially disclosed is not permitted without providing adequate information to the data subjects and, where possible, obtaining their consent for the specified use. The Company is generally authorized to use personal data for secondary purposes when implementing internal controls and audits and for fulfilling its legal obligations.
2. The Company collects and processes personal data only to the extent permitted by valid and informed consent, or when required to meet the legitimate business interests of the Company, such as the conclusion or performance of a contract, the execution of contractual obligations, or the fulfillment of legal obligations.
3. Any consent given by an individual for the collection and use of their personal data must be provided voluntarily and based on clear information from the Company regarding the intended use of such data. The individual may withdraw this consent at any time without undue complications. The date, content, and validity of such consent must always be documented.
4. The Company retains personal data only for the period necessary to achieve the specified purpose. Specific data retention policies will define the duration after which such data must be deleted, destroyed, or anonymized.
5. We respond to all requests or complaints submitted by individuals concerning their personal data
6. The Company acknowledges that certain categories of personal data are sensitive and require a higher level of protection. Sensitive personal data includes information relating to a person’s health condition, biometric and genetic data, criminal records, and any other information specifically protected under applicable data protection laws. The Company collects and processes such sensitive personal data only when it is strictly necessary for one of the following purposes:

a) the individual has granted explicit consent;
b) the processing is necessary for the Company to comply with employment laws or other legal obligations.

7. The Company implements appropriate security measures to ensure the confidentiality, integrity, and availability of personal data and to prevent the risk of unauthorized or unlawful access, alteration, destruction, or disclosure of such data. These protective measures are based on an impact assessment considering risks to the individual in connection with the specific personal data retained by the Company. The measures include security and organizational safeguards tailored to the type of processing and the nature of the protected data.

8. The Company will promptly inform individuals of any personal data breach involving their personal data and will report such incidents to the competent authorities in accordance with applicable laws.

9. The Company restricts access to personal data solely to those employees or contractors who are required to perform specific tasks in connection with such data. Appropriate awareness measures, training, and confidentiality obligations are applied to ensure that personal data are not shared or disclosed to unauthorized persons, including any additional Company employees who do not require access to personal data.

In Kračúnovce, on 19 September 2023

.....
Ing. Peter Packo
Chief Executive Officer