PERSONAL DATA SECURITY BREACHES POLICY

Madrid 3 November 2020

CONTENTS:

PERSONAL DATA SECURITY BREACHES POLICY

1. INTRODUCTION

The proper handling of security breaches is a matter of vital importance, taking into account the impact they can have on the rights and freedoms of the data subjects affected. In addition, the Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter, "**GDPR**"), also states that these security incidents may involve physical, tangible or intangible harm to natural persons, such as loss of control over their personal data, restriction of their rights, identity theft, unauthorised reversal of pseudonymisation, reputational damage, loss of confidentiality of data subject to professional secrecy or other significant economic or social harm.

In this way, Article 12 of the Acerinox Group's Code of Conduct and Best Practices establishes the confidentiality of the data of the employees, customers and suppliers and the obligation to report any leak thereof.

In addition, the Acerinox Group approved its Internal Data Protection Policy, Article 8.7 of which includes, inter alia, the essential aspects of the handling of security breaches affecting personal data.

This Policy implements the content of the Code of Conduct and Best Practices of Acerinox, S.A. and its Group of Companies, as well as the Internal Data Protection Policy, specifying the procedure to handle correctly security breaches that have an impact on the personal data of individuals.

2. PURPOSE

This Policy applies to security breaches that affect automated or paper personal data. It defines the functions and obligations that the Acerinox Group must fulfil in the event of a security breach affecting personal data.

3. SCOPE AND ENFORCEABILITY

This Policy applies to each and every company that is a member of the Acerinox Group to which the GDPR applies and, therefore, to each and every employee, manager and member of the management bodies of the following companies:

- Acerinox, S.A.
- Acerinox Europa, S.A.U.
- Roldan, S.A.
- Inoxfil, S.A.U.
- Inoxidables de Euskadi, S.A.U.
- Inoxcenter, S.L.U.
- Inoxcenter Canarias, S.A.U.
- Metalinox Bilbao, S.A.U.
- Cedinox
- Acerinox Benelux SA-NV
- Acerinox Deutschland GmbG
- Acerinox France S.A.S.
- Acerinox Italia S.R.L.
- Acerinox Polska SP Z.O.O.
- Acerinox Scandinavia AB
- Acerinox UK, Ltd.
- Acerol - Comércio e Indústria de Aços Inoxidáveis, Unipessoal, Lda.
- Inoxplate - Comércio de Productos de Aço Inoxidável, Sociedade Unipessoal, Lda.
- InoxRe S.A.
- VDM Metals Holding GmbH
- VDM Metals International GmbH
- VDM Metals GmbH
- VDM Metals Austria GmbH
- VDM Metals Benelux B.V.
- VDM Metals France S.A.S.
- VDM Metals Italia S.r.l.
- VDM Metals U.K. Ltd.

4. DEFINITIONS

Personal Data

"Personal data" means any information about an identified or identifiable natural person (**data subject**). For this purpose, an "identifiable natural person" is any person whose identity may be determined, directly or indirectly, in particular through an identifier, such as a name, an identification number, location data, an online identifier or some other elements relating to the physical, physiological, genetic, mental, financial, cultural or social identity of that person.

Personal Data Security Breach

Usually, "security breach" means an unexpected or unwanted event, which causes consequences at the expense of the security of the information system in which it occurs. With regard to personal data, the GDPR defines personal data security breaches, more commonly known as "security breaches", very broadly. Hence, "security breach" means any incident that causes the accidental or unlawful destruction, loss or alteration of personal data transmitted, retained or otherwise processed, as well as unauthorised communication or access to data.

5. EVENTS WHICH MAY GIVE RISE TO SECURITY BREACHES

Events which may cause a security breach may include, but are not limited to:

- Unauthorised access to the system (password theft, user impersonation, etc.)
- Unauthorised access to document storage files
- Application failure or system disconnection (incomplete data migration, lack of blocking, functionality failure, server failure, system crash or failure, software or communications failure, power cut, etc.)
- Computer attacks and malware (ransomware, trojans, viruses, etc.)
- Disclosure of personal data or unauthorised assignments of personal data
- Theft, loss or removal of information on portable devices (pendrives, CDs, etc.)
- Theft, loss or removal of an access card to a restricted area with potential for massive access to personal data (Data Processing Centre, central documentation files, etc.)
- Natural disasters (flood, fire, earthquake, etc.)
- Errors in the handling or use of a file or software that processes personal data and that may result in a loss or compromise its integrity or availability
- Unauthorised removal of documentation or media with personal data
- Any other incident that causes the destruction, loss or alteration of personal data

6. REPORTING SECURITY BREACHES TO THE DPO

If any employee of the Acerinox Group, data processor or third party, becomes aware of a possible security breach (i.e., when any of the cases referred to in the previous section, or any other event that may trigger a security breach), he or she must inform the Data Protection Officer of the Acerinox Group at the email address dpo@acerinox.com, without undue delay.

However, for VDM, the contact data of the DPO are:

Prof. Dr. Boris Reibach
Adenauerallee 136, 53113 Bonn, Germany
E-mail: datenschutz.vdm@acerinox.com
Tel.: +49 228 227 2260

The Data Protection Officer of the Acerinox Group will need to analyse what impact the security breach has had on the personal data of data subjects. Hence, it is a matter of establishing the extent of the security incident, its characteristics, the type of personal data it affects or the type of consequences it may have for the rights or freedoms of the data subjects. Damage may be tangible or intangible, and can result in possible misuse by those who have accessed personal data in an unauthorised manner, usurpation of identity, financial loss or public exposure of confidential data.

7. REPORTING SECURITY BREACHES TO THE COMPETENT AUTHORITY

7.1. When a security breach must be reported

In the event that the Acerinox Group Data Protection Officer decides that the reported security breach may result in a risk to the rights and freedoms of the data subjects, a report will be made to the competent authority on data protection in the relevant country.

For this purpose, some data protection authorities have set up a specific channel to enable the data controller to report the security breaches they have had.

The GDPR states that there is no obligation to notify the competent authority where the data controller can demonstrate, in accordance with the principle of proactive liability, the improbability of such a security breach entails a risk for the

rights and freedoms of the data subjects. This assessment will be carried out by the Data Protection Officer of the Acerinox Group.

7.2. Assessment criteria for security breaches according to the Spanish Data Protection Agency

The severity of the loss of confidentiality caused by a security breach is graded, following the criteria established by the Spanish Data Protection Agency according to the potential number and type of parties that may have unlawfully accessed the personal data.

Hence, the Spanish Data Protection Agency has established the following criteria for the assessment of security breaches:

VOLUME (number of complete and identified records containing personal data affected by the security breach)

- Fewer than 100 records (1)
- More than 1,000 (2)
- Between 1,000 and 100,000 (3)
- **More than 100,000 (4)**
- **More than 1,000,000 (5)**

TYPE OF DATA (according to GDPR and national law)

- Non-sensitive data (x1)
- **Sensitive data (x2)**

IMPACT (Exposure)

- Nil (2)
- Internal (within the company - controlled) (4)
- **External (supplier perimeter, hacker) (6)**
- **Public (accessible via the Internet) (8)**
- **Unknown (10)**

The calculation of the possible risks can be obtained using the following formula:

Risk = V (Volume) x Impact (Type x Impact)

The Spanish Data Protection Agency must be notified of any security breach that meets the following criteria simultaneously:

- Risk with a quantitative value at a threshold of over 20
- If two qualitative circumstances coincide (marked in **bold**)

In addition, affected data subjects must be notified of any security breach that simultaneously meets the following circumstances:

- Risk with a quantitative value of over 40
- If two qualitative circumstances coincide (marked in **bold**)

7.3. Deadline for filing the report

The report of the security breach to the relevant data protection authority shall be made without undue delay and, in any case, within 72 hours following the discovery of the security breach coming to light (taking into account that the period is counted from the moment that the data controller becomes aware of the security breach).

There may be cases where the report cannot be made within those 72 hours, for example, due to the complexity in fully determining the security breach's scope. In such cases, it is possible to make the report at a later date, accompanied by an explanation of the reasons for the delay. The information may be provided in a stepwise manner when it is not possible to do so at the time of reporting.

7.4. Minimum content of the report

The minimum information to be reported is as follows:

- The nature of the security breach
- The categories of data and data subjects affected by the security breach
- The approximate number of data subjects affected by the security breach
- The consequences that have had, or potentially may have, as a result of the security breach
- Measures taken by Acerinox to address security breaches
- Where appropriate, the measures applied to mitigate the possible negative effects on the data subjects.

8. INFORMING THE DATA SUBJECTS

In cases where the security breach is likely to mean a high risk to the rights or freedoms of data subjects, notification to the data subjects affected must be done.

The high risk criterion must be understood as meaning that the breach of security is likely to cause considerable damage to data subjects in relation to their personal data. For example, in cases where sensitive information, such as passwords or participation in certain activities, sensitive data is disclosed in massive amounts or financial loss may occur to those affected.

Notification to data subjects shall not be necessary where:

- The data controller would have taken appropriate technical or organisational measures prior to the security breach, in particular, measures that make data unintelligible to third parties, such as encryption
- Where the data controller has taken technical measures subsequent to the security breach to ensure that there is no longer any possibility of that high risk materialising
- When the notification involves a disproportionate effort, it should be replaced by alternative measures such as a public statement

9. DUTY TO DOCUMENT ALL DATA PROTECTION SECURITY BREACHES

The GDPR establishes the need for all security breaches to be documented in order to have evidence of their management, retaining them for a period of 3 years.

Security breaches of personal data will be recorded and documented in accordance with the model form in **Annex I** containing a list of the facts, their effects and the corrective measures taken.

This register will be available to the competent control authorities.

10. REFERENCES

- Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, derogating Directive 95/46/EC.
- Guide for the handling and reporting of security breaches published by the Spanish Data Protection Agency.
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the safeguarding of digital rights.
- Internal Data Protection Policy of the Acerinox group of companies in the European Union, approved on 24 May 2018.

Approved by: Chief Executive Officer of Acerinox, S.A.

Date of Approval: 3 November 2020

Executed by: Compliance Department

ID of the standard: SI-2

Version: 1-21

Date of last revision: 24 January 2020

ANNEX I: MODEL OF THE SECURITY BREACH ASSESSMENT REPORT

On [DATA], [ ] detected a security breach with regard to [DESCRIPTION OF THE FACTS AND EFFECTS THAT CAUSED THE SECURITY INCIDENT].

Analysis of the Security Breach

SCALE	[description]	[number]
DATA TYPE(S)	[description]	[number]
IMPACT	[description]	[number]
RISK	**[equation]**	**[number]**

Taking into account the aforementioned and the Personal data security breaches policy, the facts described constitute a **security breach**.

Therefore, having analysed the security breach that has occurred, its severity is assessed as [**MINIMAL, MODERATE, MAXIMUM**], given that [DESCRIPTION OF THE JUSTIFICATION].

Once the security incident was known, action was taken immediately to resolve it and mitigate the damage, [DESCRIPTION OF THE MEASURES TAKEN].

Furthermore, the following action plan has been defined for the eradication of the problem that caused the security breach, in order to prevent any recurrence of the said incident. [DESCRIPTION OF THE ACTION PLANS]

Conclusion

On the basis of all of the foregoing, it is concluded that the security breach that occurred on [DATE] [IS NOT/IS] of sufficient importance that a report [MUST BE/ MUST NOT BE]] filed out to the competent Data Protection Authority. [RATIONALE]
In addition, this security breach [IS NOT/IS] of sufficient importance to be communicated to the data subject. [RATIONALE]