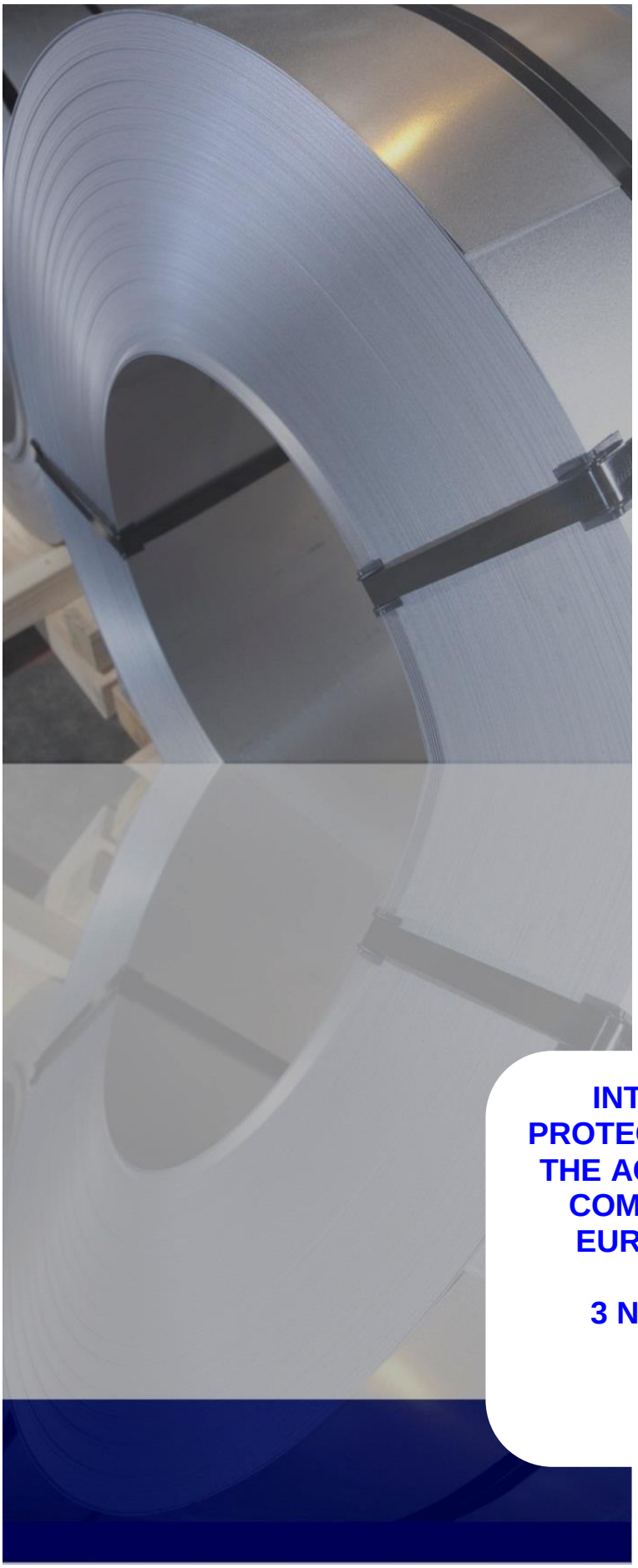

INTERNAL DATA PROTECTION POLICY OF THE ACERINOX GROUP COMPANIES IN THE EUROPEAN UNION

3 November 2020

INTERNAL DATA PROTECTION POLICY OF THE ACERINOX GROUP COMPANIES IN THE EUROPEAN UNION

INDEX

1. INTRODUCTION

On 4 May, 2016, the 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, and repealing Directive 95/46/EC (hereinafter the GDPR), was published in the Official Journal of the European Union.

This regulation that comes into force on 25 May 2018, directly applies to all Member States of the European Union, not requiring transposition.

The GDPR incorporates a series of significant new developments relating to the obligations that, to date, have had to be put in place by companies. Greater competences have been conferred to the supervisory authorities and a stricter sanctioning regime has been added to the regulatory developments, which incorporate new citizen's rights, new requirements to justify processing, security measures, etc.

The Acerinox Group has undertaken to review and update the process of its organisation to guarantee its suitability for the new legal requirements, presenting in this Internal Policy on Data Protection (hereinafter the Internal Policy), the essential aspects of this update, which will be subject to development, if necessary, through internal instructions annexed to this basic standard.

2. AIM AND SCOPE

2.1. Purpose

The Internal Policy presents the essential aspects of protection of natural persons regarding the processing of their personal data and the standards relating to the free circulation of such data, defining the management structure and supervision of the same, the functions and obligations of the people and Departments involved, and the obligations of the Group regarding personal data and its circulation.

2.2. Material scope

This Internal Policy applies to the fully or partially automated processing of personal data, as well as the non-automated processing of personal data contained in, or to be included in a file.

2.3 Subjective scope

This Internal Policy applies to each and every one of the companies that make up the Acerinox Group, to whom the GDPR applies, and thus, to each and every one of the employees, managers and directors 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 GmbH
- 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 Produtos 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 UK Ltd.

(hereinafter, Companies or individually Data Controller or Controller)

3. OBLIGATORY NATURE

This instruction is compulsory and therefore all employees and managers of the Companies are bound by it as an internal conduct standard and are obliged to be familiar with it and help to implement and enforce it regardless the position they hold within the organisation, or whether they have direct contact with the materials described herein or not.

4. DEFINITIONS

A list of definitions is attached as **Annex I**.

5. STRUCTURE OF THE DATA PROTECTION SYSTEM

5.1 Structure

The following people and entities assume specific functions regarding data protection:

- The Chief Executive Officer
- The Data Protection Officer
- The Processing Contact
- The IT Systems Department
- The Corporate Risk Management
- The Legal Advisory Department
- The Internal Audit Department

5.2. Chief Executive Officer

The Chief Executive Officer will be responsible for appointing the Data Protection Officer, who will functionally report to the former. The CEO will assume responsibility for the supervision and monitoring of the fulfilment of their duties. Likewise, they will be responsible for approving the policies, internal development instructions and training plans on the matter.

5.3 Data Protection Officer

The Acerinox Group has decided to appoint a single Data Protection Officer (hereinafter DPO) for all Group Companies, who will rely on the support and advice of the rest of the organisation in carrying out their functions. The contact details of the DPO will be published on the website of the Group, and their appointment will be reported to the regulatory authorities.

The contact data of the DPO are:

Rodrigo Garcia-Vega Redondo
Calle Santiago de Compostela, 100 (28035) Madrid, España.
E-mail: dpo@acerinox.com
Tel.: +34 91 398 51 05

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 Companies will guarantee that the DPO participates appropriately and at the correct time in all issues regarding personal data protection, and will support them in fulfilling their duties, providing the necessary resources for carrying them out and for the maintenance of their specialist knowledge.

The companies will guarantee that the DPO will be able to operate independently and autonomously when carrying out their duties.

Any interested parties may contact the DPO regarding any matters relating to the processing of their personal data and the exercising of their rights.

The DPO will be obliged to maintain confidentiality in fulfilling their functions, in accordance with the applicable regulations.

The DPO will be able to carry out other duties and tasks. The data processor will guarantee that these duties and tasks will not give rise to a conflict of interests.

The DPO will carry out the following duties:

- Inform and advise the Data Controller or Processor and the employees whose task it is to carry out the processing, of the obligations of the applicable regulations.
- Supervise compliance with the applicable regulations and the policies of the Companies regarding personal data protection, including the assignment of responsibilities, raising awareness and training of the personnel who participate in the processing operations, and the corresponding audits.
- Offer advice requested on the assessment of the impact of data protection and supervise its application accordingly.
- Cooperate with the supervisory authority.
- Act as a point of contact for the supervisory authority for questions regarding the processing, including on request, and carrying out consultations, where appropriate, on any other subject.

The DPO will carry out their duties paying due attention to the risks associated to the processing operations, taking into account the nature, scope, context and purposes of the processing.

5.4 Processing Contacts of the Processes

The Processing Contacts are those identified as such in the inventory of processing registries of each Company.

The role of the Processing Contacts is essential in the protection of data, constituting the first line of application and respect of the regulations and internal policies on the subject.

The obligations of the Processing Contacts are the following:

- Assist the DPO in the analysis and assessment of the risks of the processing, and of the third parties who process data on behalf of the Companies in order to establish the corresponding security measures.
- Comply with and ensure compliance with the processing of data of those responsible for the applicable regulations and internal policies.
- Assist the DPO in training and awareness raising tasks on data protection.
- Notify the DPO and assess the implications of any changes to the processing for which they are Controller.

5.5 IT Systems Department

Obligations of the IT Systems Department:

- Assist the DPO in the analysis and assessment of the risks of the automated processing, and of the third parties who process data on behalf of the Companies in order to establish the corresponding security measures.
- Apply, maintain and update the IT security measures assigned to the registries.
- Apply, maintain and update the current contingency plan regarding privacy.
- Assist the DPO in managing the procedure for interested parties to exercise their rights as well as the incidents regarding privacy.
- Assist the DPO in the drafting of the internal instructions.
- Assist the DPO in training and awareness raising tasks on data protection.
- Notify the DPO and assess the impact of any technological changes affecting data protection.

5.6 Corporate Risk Management

Obligations of Corporate Risk Management:

- Assist the DPO in the analysis and assessment of the risks of the processing, and of the third parties who process data on behalf of the Companies in order to establish the corresponding security measures.
- Establish a risk management policy on privacy in line with the needs of the business, also defending its risk appetite.
- Regularly monitor and control the privacy risks that exist in the Companies.

5.7 Legal Department

Obligations of the Legal Advisory Department:

- Monitor the legal changes that may arise regarding data protection to be transferred to the DPO.
- Advise and assist the DPO on legal matters, in the investigations and requirements of authorities, and the in legal procedures regarding data protection.

5.8 Internal Audit Department

Obligations of the Internal Audit Department:

- Supervise the application of the Internal Policy in accordance with the three lines of defence model established by the European Confederation of Institutes of Internal Auditing. To do this, the Internal Policy will form part of the Auditing Universe, and the auditors will ensure that the activities, duties and obligations described are carried out, as well as guaranteeing the Fundamental Principles of Data Protection.

- The frequency of the audits will be established through the Annual Plan approved by the Audit Commission.

6. BASIC DATA PROTECTION PRINCIPLES

The basic principle protected in this Internal Policy is the respect for the fundamental rights and freedoms of natural persons, and in particular their right to personal data protection. This right is based on the following principles:

- Principles of legitimacy, loyalty and transparency
- Principle of purpose limitation
- Principle of data minimisation
- Principle of accuracy
- Principle of limitation of the storage period
- Principles of integrity and confidentiality
- Principle of proactive responsibility

7. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The processing of personal data that reveals ethnic or racial origin, political opinions, religious or philosophical convictions, trade union affiliation, and the processing of genetic data, biometric data aimed at unequivocally identifying a natural person, data regarding health or data regarding the sex life or sexual orientation of a natural person is possible only in the following circumstances:

- With the explicit consent of the interested party except when prohibited by the regulations.
- When it is necessary to comply with the obligations and exercise the specific rights of the Processing Contacts or of the interested party in the area of Labour Law and social security and protection.
- When it is necessary to protect the vital interests of the interested party or another natural person, in the case in which the interested party is not physically or legally able to give their consent.
- When it refers to personal data that the interested party has clearly made public.
- When it is necessary for the formulation, execution or defence of claims or when the courts act in carrying out their legal function.
- When it is necessary for reasons of essential public interest.
- When it is necessary for preventive medicine or employment purposes, in the assessment of the ability to work of the employee, medical diagnosis, provision of assistance or health or social treatment, or management of health and social assistance systems and services. The processing will be carried out by a professional who is subject to the obligation to professional confidentiality, or under their responsibility, or by any other person also subject to the obligation of upholding privacy.

The new processing of sensitive data, as well as the processing of the data of minors, data regarding criminal convictions and offences must be consulted in advance with the DPO.

8. OBLIGATIONS OF THE COMPANIES AS DATA CONTROLLERS

8.1 Security measures

The Companies will apply the appropriate technical and organisational measures in order to guarantee and be able to demonstrate that the processing of personal data conforms to the applicable regulations.

The organisational, technical and physical measures to be applied in the Companies have been updated based on the risk analysis methodology and are adapted to the risk appetite of the Company in order to a) ensure the permanent confidentiality, integrity, availability and resilience of the systems and services that intervene in the processing of personal data, and b) the ability to quickly restore availability and access to personal data, in the event of a physical or technical incident.

These measures that are reflected for each processing in the inventory of registries, will be revised and updated when necessary, and as a minimum, once a year. When assessing the suitability of the security level, the risks presented by the data will be particularly taken into account, in particular as a consequence of the destruction, loss or accidental or illicit alteration of personal data transmitted, stored or processed in any other way, or the unauthorised communication of, or access to this data.

The people who have access to personal data for which the Companies are responsible will only be able to process this data following instructions included in this Internal Policy and in their development regulations.

8.2 Assessment of the impact on privacy

A Privacy Impact Assessment (PIA) will be carried out for current and new processing that poses a high risk to the rights and freedoms of natural persons, and specifically in the following cases:

- When there is a systematic and exhaustive assessment of the personal aspects of natural persons based on automated processing, such as, for example, the creations of profiles.
- Large scale processing of special categories of data or personal data regarding criminal offences and sentences.
- Systematic observation on a large scale of the public access area.

When new processing of personal data is going to be implemented or a change in the existing processing arises that requires a PIA, this must be carried out and formally approved by the DPO and the Processing Contacts.

When a PIA regarding data protection shows that the processing would pose a high risk if the Controller does not take measures to mitigate it, the supervisory authority will be consulted.

8.3 Data protection by design and by default

Taking into account the state of the technique, the cost of the application and the nature, scope, context and purposes of the processing, as well as the risks of varying probability and seriousness posed by the processing to the rights and freedoms of natural persons, the Companies will apply, both when determining the processing methods and at the time of the processing itself, appropriate technical and organisational methods, such as pseudonymisation, designed to effectively apply the data protection principles, such as the minimisation of data, and to integrate the necessary guarantees in the processing, in order to comply with the requirements of the applicable regulations and to protect the rights of the interested parties.

To do this, with regards to the processing already identified when they are modified; and before beginning new processing of data, the Processing Contacts and the rest of the employees of the Companies, must contact the DPO to regularise the said processing at least one month in advance of it being started or of the modification taking place.

Regarding the processing of data by default, the Companies will apply measures to guarantee that personal data (amount of data, extent of its processing, storage period and accessibility) necessary for each one of the purposes of the processing will be subject to such. In particular, these measures will guarantee that by default the personal data is not accessible to an indeterminate number of people, without the intervention of the person.

8.4 Processing co-controllers

When two or more Companies or one of them along with a third party jointly determine the objectives and means of processing, they will be considered as processing co-controllers. The co-controllers will transparently and by mutual agreement determine their respective responsibilities in complying with their obligations except, and to the extent that, their respective responsibilities are governed by the applicable regulations. This agreement may designate a point of contact for the interested parties and will duly reflect the duties and respective relationships of the co-controllers regarding the interested parties.

8.5 Registry of processing activities

An inventory has been drafted of the registries of personal data processing activities of which each one of the Companies are controllers, which includes the obligatory information established in the applicable regulations.

These inventories are centralised, accessible, complete and will be kept up to date to include all of the processing activities that are carried out at all times.

8.6 Data processors for whom the Companies are the Controllers

The Companies will choose data processors who offer them sufficient guarantees to apply the appropriate technical and organisational measures, so that the processing complies with the requirements of the applicable regulations and guarantees the protection of the rights of the interested party.

The processing by the processor will be governed by a contract or other legal document in compliance with the applicable regulations, which links the processor to the Controller and establishes the purpose, duration, nature and purpose of the processing, the type of personal data and categories of interested parties, and the obligations and rights of the Controller.

For this purpose, the employees of the Companies must inform the DPO of any new data processing to be made by third parties that they wish to carry out, so that they may be brought into conformity with existing procedures.

When a data processor requests another processor to carry out certain processing activities on behalf of the Controller, this other processor, through a contract or other legal document established according to the applicable regulations, will be obliged to comply with the same data protection obligations as those provided in the contract or other legal document between the Controller and the processor. If this other processor fails to comply with their data protection obligations, the initial processor will continue to be fully responsible before the Data Controller regarding compliance with the obligations of the other processor.

8.7 Breach in security of personal data

Any breach in security of personal data must be immediately reported to the DPO in accordance with the corresponding Internal Instruction so that they can in turn notify the competent supervisory authority without undue delay and, if possible, in no more than 72 hours after becoming aware of said breach, unless it is unlikely that this security breach would constitute a risk to the rights and freedoms of natural persons.

Breaches in security of personal data, including the relevant facts, their effects and the corrective measures adopted will be presented in a registry that will allow the supervisory authority to verify compliance with the applicable regulations.

When it is likely that the breach in security of the personal data poses a high risk to the rights and freedoms of natural persons, this point will be immediately reported to the DPO so that they can in turn report it to the interested party without undue delay.

Communication to the interested party will not be necessary if one of the following conditions is met:

- Technical and organisational measures of protection have been adopted and these measures have been applied to the personal data affected by the breach in security of the personal data, in particular those that make the personal data unintelligible for anyone not authorised to access it, such as encryption.
- Ulterior measures have been taken that guarantee that it will be unlikely that a high risk to the rights and freedoms of the interested party will arise.
- It requires a disproportionate effort. In this case, a public notification or similar measure will be employed instead which will effectively inform all of the interested parties in the same way.

8.8 Destruction of data and storage mediums

A policy has been drafted on the destruction of documentation and automated and non-automated storage mediums that contain personal data once the storage date has expired; this includes instructions to the personnel of the Group entrusted with this function.

9. OBLIGATIONS OF THE COMPANIES AS DATA PROCESSORS

The Companies have drafted and maintain a processing activities registry on behalf of third parties that is centralised, accessible, complete and will be kept up to date to include all of the processing activities that are carried out at all times.

The Companies will notify the data controller without due delay of breaches in security of the personal data of which they are aware.

10. EXTERNAL POLICY ON DATA PROTECTION

An external policy on data protection has been drafted which is available for any interested party. It reflects the rights of the holders of personal data and all elements of information established by the GDPR in an easily comprehensible and structured format, in accordance with the indications drafted by the regulatory authorities in this regard.

This Policy allows third parties to be fully informed of the functioning of the Companies regarding the collection, use, storage, dissemination or destruction of personal data.

The Policy is available on the Acerinox website.

11. INTERNATIONAL DATA TRANSFERS

Transfers of personal data subject to processing or that will be subject to processing following their transfer to a third-party country or organisation will only be made if, the Controller and processor comply with the terms and conditions established by the applicable regulations, including those regarding the ulterior transfers of personal data from the third-party country or international organisation to another third-party country or international organisation.

When it is proposed to make an international data transfer not included in the inventory of processing registries, the DPO must be contacted beforehand.

12. DISSEMINATION AND TRAINING

12.1 Dissemination of the Internal Policy

All employees of the Companies will be informed of the approval of the Internal Policy.

The DPO will decide on the different communication actions that must be carried out to transmit the commitment adopted by the Acerinox Group regarding data protection, the specific message that must be transmitted, the issuers and recipients, the communication channel and the schedule of actions.

12.2 Training on privacy and data protection

To close the Internal Policy, the Acerinox Group has considered it fundamental that the employees of the Companies receive appropriate training on data protection and especially on the following matters:

- Privacy in the design according to the different roles or profiles of the employees.
- Security measures to apply to the processing of personal data which may involve: minimisation, encryption, anonymity, and storage periods of the documentation.
- Management of the exercising of the rights of the interested parties.

The aforementioned training will be structured in three levels:

- General training on data protection for all employees.
- Specific training in areas relating to interaction with employees and clients.
- Specific training for the DPO, the personnel of the Compliance Department and the Processing Contacts.

The training regarding data protection will be transmitted internally like any other type of training, with the aid of the respective human resource departments.

In the case of new incorporations into the Companies or promotions of work positions that require specific training regarding data protection, the DPO will identify the training courses or initiatives that may be undertaken.

Without prejudice to the foregoing, if through the internal control system, or any other way, any needs for additional or extraordinary training are detected regarding data protection, the DPO will arrange it.

13. APPROVAL

This Internal Policy has been approved by the Steering Committee of Acerinox, S.A. on November 3, 2020.

ANNEX I: DEFINITIONS

For the purposes if this Internal Policy the following terms will mean:

1) **"personal data"**: all information on an identified or identifiable natural person ("the interested party"); an identifiable natural person will be considered to be any person whose identity can be determined, directly or indirectly, in particular via an identifier, like for example a name, identification number, location data, and online identifier or one or several aspects of physical, physiological, genetic, psychological, economic, cultural or social aspect of the said person.

2) **"processing"**: any operation or set of operations performed on personal data, either through automated procedures or not, such as the collection, recording, organisation, structuring, storage, adaptation or modification, extraction, consulting, use, communication by transmission, diffusion or enabling any other form of access, comparison or interconnection, restriction, erasure or destruction.

3) **"restriction of the processing"**: the labelling of stored personal data in order to restrict its future processing.

4) **"creation of profiles"**: any form of automated processing of personal data that uses personal data to assess specific personal aspects of a natural personal in particular to analyse or predict aspects relating to professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements of the said natural person.

5) **"pseudonymisation":** the processing of personal data in such a way that it may not be attributed to an interested party without additional information, as long as this additional information figures separately and is subject to technical and organisational measures designed to guarantee that the personal data is not attributed to an identified or identifiable natural person.

6) **"file"**: any structural set of personal data, accessible according to specific criteria, whether centralised, decentralised or functionally or geographically spread.

7) **"data controller" or "controller"**: the natural or legal person who, solely or with others, determines the purposes and means of the processing.

8) **"data processor" or "processor"**: the natural or legal person who processes the personal data on behalf of the data controller.

9) **"recipient"**: the natural or legal person, public authority, service or other entity to which the personal data, processed or not, of a third party is transferred.

10) **"third party"**: natural or legal person, public authority, service or other entity other than the interested party, the data controller, the data processor and the people authorised to process personal data under direct authority of the controller or the processor.

11) **“consent of the interested party”**: any demonstration of free, specific, informed and unequivocal will by which the interested party accepts, through a declaration or a clear affirmative action, the processing of personal data that concerns them.

12) **“breach in security of the personal data”:** any breach of security that causes the destruction, loss or accidental or illicit alteration of personal data transmitted, stored or processed in any other way, or the unauthorised communication of, or access to this data.

13) **“genetic data”**: personal data relating to general inherent or acquired characteristics of a natural person that provides unique information on the physiology or the health of that person, obtained in particular from the analysis of a biological sample of that person.

14) **“biometric data”**: personal data obtained from specific technical processing, relating to the physical, physiological or behavioural characteristics of a natural person that allows or confirms the unique identification of that person, such as facial images or fingerprint data.

15) **“data relating to health”:** personal data relating to the physical or mental health of a natural person, including the provision of healthcare services, which reveals information on the state of their health.