# Data Protection Policy

## 1. Purpose

The purpose of this Data Protection Policy is to outline the conduct expected of all employees of ArcelorMittal Group who use and process Personal Data. It addresses how the ArcelorMittal Group and any third party acting on its behalf will collect, use, protect and process Personal Data.

## 2. Scope

This Policy applies to all directors, officers and employees of ArcelorMittal Group and to any third party acting on their behalf and to all Processing of Personal Data.

This Policy applies to:

(i) any and all Personal Data processed in the EU by or on behalf of ArcelorMittal S.A. or its EU Subsidiaries, including employees, customers, contractors, local stakeholders, external consultants, business partners and suppliers' Personal Data;

(ii) any and all Personal Data processed in the EU by or on behalf of ArcelorMittal S.A. or its EU Subsidiaries, and further transferred or made available outside of the EU, including employees, customers , contractors, local stakeholders , external consultants, business partners and suppliers' Personal Data; and

(iii) any and all Personal Data Processing activities of a Subsidiary located outside of the EU that offers goods or services or monitors behavior of Data Subjects who are in the EU.

This Policy applies to the Processing of Personal Data wholly or partly by automated means and to the Processing other than by automated means of Personal Data which form part of filing systems or are intended to form part of a filing system.

This Policy does not cover:

(iv) data rendered anonymous. Data are rendered anonymous if individual persons are no longer identifiable, neither directly nor indirectly.

(v) data Processing activities by a Subsidiary established outside of the EU and that are not related to (i) the activities of ArcelorMittal S.A. or a Subsidiary located in the EU or (ii) Data Subjects who are in the Union and who are offered goods or services or whose behavior in the EU is monitored.

This policy is in line with the European General Data Protection Regulation (GDPR) 2016/679 EU and is based on the ArcelorMittal Group's Binding Corporate Rules.

## 3. Definitions

«**ArcelorMittal Controller**» means ArcelorMittal S.A. or a Subsidiary acting as data controller.

«**ArcelorMittal Processor**» means ArcelorMittal S.A. or a Subsidiary acting as data processor.

«**Binding corporate rules**» are Personal Data protection policies which are adhered to by a controller or processor established in the territory of a Member State for transfers or a set of transfers of Personal Data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

«**Data Controller**» or «**Controller**» means the natural or legal person which alone or jointly with others determines the purposes and means of Processing of Personal Data.

«**Data Subject**» means any natural person whose Personal Data are processed in the context of a process falling in the scope of this Policy.

**Consent**» means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data.

«**Personal Data**» means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

«**Personal Data Breach**» refers to any actual or suspected breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

«**Processing**» of Personal Data means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

**«Processor»** means a legal entity which processes Personal Data on behalf of the Data Controller. The word «Processor» has the same meaning as «Service Provider» as commonly used within ArcelorMittal.

**«Recipient»** means a natural or legal person, public authority, agency or any other body to whom Personal Data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

**«Special Categories of Personal Data»** or **«Special Data»** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic and biometric data for the purpose of uniquely identifying a natural person and data concerning health or sex life and sexual orientation.

**«Subsidiary»** means any company or legal entity fully consolidated and controlled by ArcelorMittal S.A. The term «control» means the possession, direct or indirect, through one or more intermediaries of the power to direct or cause the direction of the management and policies of a company or legal entity, whether through the ownership of voting securities, by contract or otherwise.

## 4. Roles and responsibilities

The Board of Directors of ArcelorMittal has overall responsibility for the implementation of the ArcelorMittal Data Protection Policy, as well as related privacy and data protection policies.

An ArcelorMittal Data Protection Committee consisting of the Group Compliance and Data Protection Officer, one nominee each by the ArcelorMittal Group CIO and ArcelorMittal EVP Human Resource, is designated and shall have overall responsibility to oversee the implementation of this Policy as well as related privacy and data protection policies and the performance by the Subsidiaries, including future Subsidiaries of their obligations under this Policy as well as related privacy and data protection policies.

ArcelorMittal S.A. and its Subsidiaries worldwide, including their directors, officers and employees, that process Personal Data must comply with this Policy as well as related privacy and data protection policies.

The ArcelorMittal Group Data Protection Officer shall:

- enjoy the highest management support for the fulfilling of his/her tasks and shall report directly to the highest management level within ArcelorMittal;
- with the assistance of the Data Protection Committee, deal with the Data Protection Authorities' investigations and monitor and annually report on compliance with this Policy at global level.

The ArcelorMittal Data Protection Correspondents will coordinate all measures necessary to ensure Subsidiaries within their scope comply with their obligations under this Data Protection Policy, as well as related privacy and data protection policies.

IT Compliance and Security (ITCS) Officers or teams shall define, implement & monitor deployment of an internal control system within ArcelorMittal IT, required to achieve IT's objectives in the field of Compliance and Security.

## 5. Business benefits

The Processing of Personal Data is regulated in many of the countries where ArcelorMittal is present and does business. ArcelorMittal recognises that Personal Data must be treated with caution, whether it concerns employees' or business partners' Personal Data. ArcelorMittal therefore wishes to adopt practical and legal measures to protect Personal Data handled under its responsibility.

Within the EU, on May 251h, 2018, the General Data Protection Regulation 2016 («the GDPR») replaced the 1995 EU Data Protection Directive and superseded the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. The purpose of the GDPR is to protect the «rights and freedoms» of living individuals, and to ensure that Personal Data is not processed without their knowledge, and, wherever necessary, that it is processed with their consent.

Similar legislation to protect the «rights and freedoms» of living individuals, and to ensure that Personal Data is processed respecting these rights and freedoms exists in countries where ArcelorMittal does business or has a presence.

This Data Protection Policy serves to lay down uniform, adequate and global data protection standards while Processing Personal Data within the ArcelorMittal Group.

ArcelorMittal recognizes that laws in certain countries may require stricter standards than those described in this Policy. In that case, ArcelorMittal Subsidiaries must handle Personal Data in accordance with local law applicable in the countries where the Personal Data are processed.

## 6. Data Protection at ArcelorMittal

The Board of Directors and management of ArcelorMittal are committed to comply with all relevant local and global laws relating to personal data, and to protecting the rights and freedoms of individuals whose Personal Data ArcelorMittal processes. To that end, ArcelorMittal has developed and implemented a documented Privacy management framework for the ArcelorMittal Group which will be maintained, continuously improved and supported with further specific privacy and data protection policies and procedures.

The objectives of ArcelorMittal's Privacy Management Framework are to ensure adequate Personal Data protection and fair Processing to (i) meet its own requirements for the management of personal information;

(ii) support organizational objectives and obligations; (iii) impose controls in line with ArcelorMittal's acceptable level of risk; (iv) ensure that it meets applicable statutory, regulatory, contractual and/or professional duties; and (v) protect the interests of individuals and other key stakeholders.

Please refer to point 2 above for more detail on the scope of data protection at ArcelorMittal.

## 7. Legal basis or grounds for Processing of Personal Data

ArcelorMittal shall not process Personal Data unless it has a legal basis or ground for so doing. Before undertaking any Processing activity, the right legal ground needs to be identified and recorded. If ArcelorMittal processes Personal Data without any legal basis or grounds, the Processing is illegal and should be stopped immediately.

A Legal basis or ground is the legal justification for a Personal Data Processing activity. The Processing of Personal Data shall always be based on one or more of the six legal basis or grounds set out below:

- Performance of a contract;
- Compliance with a legal obligation;
- Protection of the vital interest of the Data Subject;
- Performance of a task carried out in the public interest or in the exercise of official authority;
- Legitimate interest of ArcelorMittal or a third party;
- Prior consent of the Data Subject.

If ArcelorMittal chooses to process Personal Data based on the Consent of Data Subjects, the Consent shall comply with the following requirements:

- be unambiguous;
- be freely given;
- be specific; and
- be informed.

A process for the withdrawal of consent shall be established and it shall be just as easy to withdraw consent as it was to provide it.

## 8. Principles of Personal Data Processing

In the Processing of Personal Data ArcelorMittal shall take into account and comply with the legal principles of Processing of Personal Data, set out below.

### 8.1 Lawfulness, fairness and transparency

*Personal Data shall be processed **lawfully, fairly** and in a **transparent** manner in relation to the Data Subject.*

#### 8.1.1 Lawfulness of Processing

Processing or handling of Personal Data is considered lawful, if it is based on at least one of the legal grounds set out in Article 7 above.

#### 8.1.2 Fairness

ArcelorMittal must process Personal Data in a fair way. This means that:

- ArcelorMittal should handle Personal Data in a way that Data Subjects expect the company to process it (transparency and reasonable expectations);
- ArcelorMittal should not use Personal Data in a way that it has adverse effects on the Data Subject.

#### 8.1.3 Transparency

Data Subjects shall be informed of how their Personal Data is being handled. In general, Personal Data must be collected directly from the individual concerned. When Personal Data is collected, the Data Subject must either be aware of, or informed of

- The identity of the Data Controller
- The purpose of data Processing
- Third parties or categories of third parties to whom the Personal Data might be transmitted

### 8.2 Purpose limitation

*Personal Data shall be **collected for specified, explicit and legitimate** purposes and not further processed in a manner that is incompatible with those purposes.*

#### 8.2.1 Purpose limitation

The specific purposes for which Personal Data are processed should be explicit and legitimate and determined at the time of collection of the Personal Data. Hence, before collecting Personal Data, ArcelorMittal shall carefully consider in sufficient detail, the purposes the Processing is intended for.

Data obtained for a specified purpose must not be used for a purpose that is incompatible with the identified purpose.

#### 8.2.2 Legitimate purpose

Personal Data must be collected for legitimate purposes. This requirement goes beyond the legal grounds for Processing Personal Data listed in Article 7 above to include purposes in accordance with applicable law in the broadest sense. As such, the purposes must be in accordance with all provisions of applicable data protection law, as well as other applicable laws such as employment law, contract law, consumer protection law etc.

Furthermore, a legitimate purpose does not only have to be legal, but also reasonable, and the purpose must be within the reasonable expectations of the Data Subject.

### 8.3 Data minimisation

*Personal Data shall be **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed.*

The principle of data minimisation is closely linked to the purpose of the Processing of Personal Data: no more Personal Data can be processed than those needed to fulfil the purpose for which it is collected. The Personal Data that are being processed need to be:

- Adequate (enough data);
- Relevant (necessary to fulfil the purpose);
- Limited to and not more than needed to fulfil the purpose.

### 8.4 Accuracy

*Personal Data shall be accurate and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*

The Personal Data processed within ArcelorMittal needs to be accurate and up to date. Data should not be kept unless it is reasonable to assume that it is accurate. In order to achieve optimal accuracy (quality) of the Personal Data, ArcelorMittal shall, as far as possible, obtain Personal Data from the Data Subject directly.

### 8.5 Storage limitation

*Personal Data shall be kept in a form which permits identification of Data Subjects for **no longer than is necessary** for the purposes for which the Personal Data are processed.*

Personal Data must not be retained any longer than is necessary for the purposes for which they are processed and in compliance with applicable legal requirements with respect to document retention. The Personal Data must be destroyed, with traceable record, or archived after the retention period when they are no longer necessary for the Processing activity.

### 8.6 Integrity and confidentiality

*Personal Data shall be processed in a manner that ensures appropriate **security** of the Personal Data; including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

- Personal data must be processed in a manner that ensures its integrity. Data needs to be secured in order to achieve and maintain its integrity. Integrity of Personal Data should be considered for the entire lifecycle of a project or process.
- Confidentiality of the Personal Data: ensuring that Personal Data cannot be accessed by people who do not need it (i.e. the «Need to know» principle). ArcelorMittal must ensure that Personal Data are only processed by authorised personnel, on authorised equipment.

### 8.7 Accountability

*ArcelorMittal Controllers shall be responsible for, and be able to **demonstrate compliance with the principles set out in Article 7 and 8 above**.*

ArcelorMittal Controllers are not only responsible for ensuring compliance but for demonstrating that each Processing operation complies with the requirements set out in this Policy.

Specifically, ArcelorMittal as Data Controller and Processor as the case may be is required to:

i. establish clear documentation, procedures and guidelines supplemental to this Policy as well as related privacy and data protection related policies as required;
ii. maintain a record of Processing activities involving Personal Data;
iii. implement appropriate security measures to ensure the security of Personal Data and establish and maintain a process to discover and report in the event of a breach;
iv. perform Data Processing Impact Assessment;
v. establish and maintain a mechanism to comply with Data Subject Rights;
vi. in the event that Personal Data is processed based on consent, ensure that consent is validly obtained and records of such consent and protocols for withdrawal of consent are maintained.

## 9. Data collection and Processing

Being transparent and providing accessible information to individuals about how their Personal Data will be used is a key element of data protection. The most common way to provide this information is in a privacy notice.

The starting point of a privacy notice should be to inform the Data Subject about:

- Why does ArcelorMittal need the Personal Data;
- What ArcelorMittal is going to do with the information; and
- Who it will be shared with.

These are the key points upon which all privacy notices should be built. However, they may contain further information to avoid unfair Processing of Personal Data. This could be the case if a Data Subject is unlikely to know that their Personal Data is processed for a particular purpose or where Personal Data have been collected by observation .

## 10. Processing special categories of Personal Data

ArcelorMittal shall only process and/or retain Special Categories of Personal Data when it has legal grounds to do so. Lawful legal grounds include:

- explicit consent of the Data Subject;
- legal obligation (e.g. when legal claims are filed, obligations in relation to social security, etc).

Processing of Special Categories of Personal Data is prohibited except in the following cases:

- The Data Subject has given their explicit consent to the Processing of those Special Data, except where the applicable laws prohibit it; or
- The Processing is necessary for the purposes of carrying out the obligations and specific rights of the ArcelorMittal Controller in the field of employment , social security and social protection law (e.g. antidiscrimination) in so far as it is authorized by national law providing for adequate safeguards for the fundamental rights and interests of the Data Subjects; or
- The Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving their consent; or
- The Processing relates to Special Data which are manifestly made public by the Data Subject; or
- The Processing of Special Data is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

The Processing of the Special Data is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Special Data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy. Special Data may be processed for these purposes only when

those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

ArcelorMittal employees within the relevant departments are responsible for the lawful Processing and retention of Special Data in line with this Article 10, as well as for the adherence to all applicable duty of secrecy rules and regulations.

ArcelorMittal Subsidiaries are required to comply with any local law variations that may maintain or introduce further conditions, including limitations, with regard to the Processing of genetic data, biometric data or data concerning health.

## 11. Data Subject Rights

Data Subjects have the following rights relating to their Personal Data that is processed by ArcelorMittal:

- Right to access details of the nature of Personal Data held by ArcelorMittal and to whom it has been disclosed or transferred;
- Right to object, restrict, stop or prevent Processing;
- Right to rectify any error in their Personal Data;
- Right to erasure of the Personal Data;
- Right to receive their Personal Data in a structured, commonly used and machine-readable format, and the right to have that Personal Data transmitted to another controller;
- Right to object to any automated decision-making, incl. profiling without consent.

Data Subjects may submit data access requests as described in the ArcelorMittal Data Subjects' rights and requests procedure. This procedure also describes how ArcelorMittal will ensure that its response to the Personal Data access request complies with applicable legal requirements.

The above detailed Data Subject rights are not absolute. ArcelorMittal is subject to legal obligations which may prevent it from giving effect to certain Data Subject Rights requests.

## 12. Consent

Consent means an explicitly and freely given, specific, informed and unambiguous indication of the Data Subject's wish to agree to the Processing of Personal Data relating to him or her. Consent might be given in the form of a statement or of a clear affirmative action. The consent of the Data Subject can be withdrawn at any time.

ArcelorMittal accepts consent as legal basis for Processing only if the Data Subject has been fully informed of the intended Processing and has expressed their agreement (i.e. the Data Subject opted in by ticking a box), while in a fit state of mind to do so and without pressure being exerted upon them.

Consent obtained under duress or on the basis of misleading information will not be a valid legal basis for Processing. Consent cannot be inferred from non-response to a communication. For special categories of Personal Data, explicit written consent of Data Subjects must be obtained unless an alternative legal basis for Processing exists.

ArcelorMittal must be able to demonstrate, for every Data Subject involved, that a valid consent was obtained for all Personal Data Processing activities performed for a specific purpose based on consent.

## 13. Security of Personal Data

ArcelorMittal shall implement all technical and organizational measures required to ensure adequate security of Personal Data.

All employees are responsible for ensuring that Personal Data which ArcelorMittal holds and for which they are responsible, are kept securely and are not under any conditions disclosed to any third party unless that third party has been specifically authorised by ArcelorMittal to receive that information and has entered into a data Processing agreement in accordance with the guidelines on third party data transfers.

Personal Data should be accessible only to those who need to use it, and access may only be granted in line with the ArcelorMittal Procedure related to Human Resource Identity & Secure access to ArcelorMittal Information assets. Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the applicable data retention policy.

Personal Data may only be deleted or disposed of in line with the applicable policy on data retention. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by the applicable procedure relating to secure disposal of storage media.

## 14. Disclosure and transfer of personal data to third parties

ArcelorMittal must ensure that Personal Data is not disclosed to unauthorized third parties. All employees should exercise caution when asked to disclose Personal Data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk, as formulated in ArcelorMittal's training policy. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of ArcelorMittal's business.

Disclosures without consent are only permitted in so far as the information is requested for one or more of the following purposes:

- To safeguard national security; To prevent or detect crime including the apprehension or prosecution of offenders;
- To assess or to collect tax duty; To discharge regulatory functions (including health, safety and welfare of persons at work);
- To prevent serious harm to a third party;
- To protect the vital interests of the individual (in life and death situations).

All requests to provide Personal Data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorized by either of the Data Protection Correspondent or the data owner . The Data Protection Correspondent may consult with the Data Protection Committee for guidance in this regard.

## 15. Data transfer mechanism

ArcelorMittal must ensure that the level of protection of Personal Data contained in this Policy and the Binding Corporate Rules is guaranteed when transferring Personal Data internationally. The rules protecting Personal Data continue to apply regardless of where the Personal Data lands.

Under the GDPR, all EU Member States have the same level of protection for the Processing of Personal Data. Therefore, no additional legal requirements need to be satisfied by ArcelorMittal when transferring Personal Data within the EU.

However, where Personal Data is transferred outside the EU (i.e. to a third country located outside of the EU), ArcelorMittal must review whether the necessary protection, data transfer mechanism, is in place in order to ensure an adequate level of legal protection in the third country. ArcelorMittal shall only transfer Personal Data to a third country when this country ensures an adequate level of protection of the rights and freedoms of the Data Subject in relation to the Processing of their Personal Data.

Data transfer mechanisms protection for cross border exchanges include, but are not limited to:

1. Adequacy Decision;
2. Standard Contractual Clauses;
3. Binding Corporate Rules (intra-group transfers only)

When choosing a Personal Data transfer mechanism, always involve the legal department.

## 16. Retention and disposal of Personal Data

Personal Data may not be retained for longer than it is required. Once the purpose for Processing or the legal basis for Processing expires, it may not be necessary to retain such Personal Data unless otherwise legally required. Some Personal Data will be kept for longer periods than others. It is important that appropriate data retention policies are developed in accordance with local legal and regulatory requirements to guide with record retention and disposal.

Personal Data must be disposed of in a way that protects the rights and freedoms of Data Subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with any guidelines for secure disposal of storage media.

## 17. Follow-up, monitoring and evaluation

Personal Data Protection shall form part of the Group's Compliance Programme. In accordance with the existing ArcelorMittal Compliance Programme each CEO/Head of Function must certify compliance with this Policy and report any possible exceptions.

Each Business Unit/Function must designate a Data Protection Correspondent who shall be responsible for the implementation of this Policy within their Unit/Function. By default, absent a Data Protection Correspondent, the Compliance Officer for the Unit/Function shall be responsible for implementation and compliance.

Each Business Unit/Function should regularly review its internal controls and proceed with a risk assessment in order to assess its risk profile with respect to Personal Data Protection and adapt its internal controls and procedures accordingly.

This Data Protection Policy shall be subject to development, review, evaluation and continuous improvement.

Different tools can be used to follow up and monitor risks related to Personal Data protection in addition to the tools and processes set out in Article 9 above.

ArcelorMittal shall perform management reviews through its Data Protection Committee to follow up on risks relating to protection of Personal Data on a regular basis and shall consider the following:

- Status of actions from previous reviews;
- Changes in internal and external issues relevant to the Personal Data Protection;
- Information on Personal Data Protection performance including trends in;
  - Non-conformities and corrective actions;
  - Measurement evaluation results;
  - Internal and external audit reports;
  - Results and/or trends from the measurement of progress towards the protection of information security and Personal Data.
- Continuous improvement opportunities including the following:
  - Need for changes including its policies and procedures
  - Results of audits and reviews and recommendations
  - Results of audits and reviews of key suppliers and partners and recommendations
  - Techniques, products or services which could be used to improve compliance
    - Results of exercises and tests
    - Risks or issues not adequately addressed
    - Changes (internal or external) that could affect compliance (post-incident reports)
    - Emerging good practice and guidance