ArcelorMittal Binding Corporate Rules

The processing of information relating to individuals is regulated in many countries where ArcelorMittal is present. ArcelorMittal recognizes that Personal Data must be treated with caution, being it employees' or business partners' data. ArcelorMittal therefore wishes to adopt practical and legal measures in order to protect Personal Data handled under its responsibility.

The aim of the ArcelorMittal Binding Corporate Rules (the "Procedure") is to lay down uniform, adequate and global data protection standards and to facilitate Group-wide transfers of Personal Data compliant with legal data protection requirements.

Definitions

Definitions

ArcelorMittal S.A.
"ArcelorMittal S.A." means ArcelorMittal S.A., a public limited liability company (*société anonyme*) registered with the Company and Trade Register of Luxembourg under n°B. 82 454.

ArcelorMittal/ArcelorMittal Group
"ArcelorMittal" or "ArcelorMittal Group" means ArcelorMittal S.A. and its Subsidiaries.

Data Protection Authorities
"Data Protection Authorities" means the national data protection authorities in the EU.

Subsidiary
"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.

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.

Data Subject
"Data Subject" means any natural person whose personal data are processed in the context of a process falling in the scope of this Procedure.

Processing
"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.

Recipient
"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 ("Special Data")
"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.

HR Data
"HR Data" means any Personal Data relating to employees, candidates, trainees, temporary workers or retirees of ArcelorMittal S.A. or any of its Subsidiaries.

Global Tools/Databases
"Global Tools/Databases" refers to any IT tool (i) including Personal Data (ii) not being restricted to a site, a Business Unit, a segment.
For instance, One HRIS

GDPR
"GDPR" means the European Union Regulation 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.

Data Controller
"Data Controller" or "Controller" means the natural or legal person which alone or jointly with others determines the purposes and means of the processing of Personal Data.

Processor
"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.

Consent
"Consent" of the Data Subject 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 relating to him or her.

ArcelorMittal Controller
"ArcelorMittal Controller" means ArcelorMittal S.A. or a Subsidiary acting as Data Controller.

ArcelorMittal Processor
"ArcelorMittal Processor" means ArcelorMittal S.A. or a Subsidiary acting as Data Processor.

EEA
"EEA" means the European Economic Area.

Europe
"Europe" means the Member States of the European Union ("EU") and the 3 members of the EEA.

Data Exporter
"Data Exporter" means ArcelorMittal S.A. or any Subsidiary located in Europe processing Personal Data in Europe, such Personal Data being further transferred or made available to a recipient outside of Europe.

The terms in this Procedure shall be interpreted in accordance with the GDPR and EU Directive 2002/58/EC, as may be amended, replaced or re-enacted.

Article 1 - Status of the Procedure

The ArcelorMittal Board of Directors has overall responsibility for the implementation of this Procedure.

ArcelorMittal S.A. and its Subsidiaries worldwide, including their directors, officers and employees, that process Personal Data must comply with this Procedure.

Any violator of this Procedure will be subject to disciplinary action, in accordance with local applicable laws and policies.

ArcelorMittal recognizes that certain laws may require stricter standards than those described in this Procedure. In this case, ArcelorMittal Subsidiaries will handle Personal Data in accordance with local law applicable at the place where the Personal Data are processed. Where applicable local law provides a lower level of protection of Personal Data than that established by this Procedure, then the requirements of this Procedure shall apply.

Specific privacy policies have been and will be developed in order to govern the use of some particular tools/databases. In case of contradiction between this Procedure and a specific privacy policy, such specific privacy policy shall prevail. Tools and databases not covered by a specific privacy policy will be solely governed by this Procedure.

This Procedure has been adopted in the context of the European Directive 95/46 as ArcelorMittal's "Binding Corporate Rules" and was subsequently amended to comply with the GDPR and its related guidelines.

Questions about compliance with this Procedure and/or with specific privacy policies may be addressed to the relevant Data Protection Correspondent (See Schedule VI).

The date of entry into force of this Procedure for any particular Subsidiary is subject to the execution of the Data Protection Procedure Signature Form by such Subsidiary.

Article 2 - Scope of the Procedure

This Procedure 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
and
(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.

This Procedure 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 Procedure covers any person whose Data are processed, regardless to his/her nationality.
This Procedure does not cover data rendered anonymous. Data are rendered anonymous if individual persons are no longer identifiable, neither directly nor indirectly.

This Procedure does not cover 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 behaviour in the EU is monitored.

Current in-scope processes and data transfers are further described in Schedule VIII of this Procedure. The structure and contact details of the ArcelorMittal Group and of the ArcelorMittal Controllers bound by this Procedure are described in Schedule X of this Procedure.

Article 3 - Principles for processing Personal Data

3.1. Legitimacy criteria

Personal data shall be processed based on the following grounds:

- The processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; or

- The processing is necessary for compliance with a legal obligation to which the ArcelorMittal Controller is subject; or

- The processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; or

- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the ArcelorMittal Controller
Personal Data may also be processed (i) if any ArcelorMittal Subsidiary is required to do so by law or legal process (ii) if required by law enforcement authorities or other government officials based on an enforceable government request, or in connection with an investigation of suspected or actual illegal activity (iii) when disclosure is necessary or appropriate either because it is in the vital interests of ArcelorMittal or its employees' integrity or physical or mental wellbeing could be affected; or

- The processing is necessary for the purposes of the legitimate interests pursued by the ArcelorMittal Controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data; or

- The Data Subject has given his Consent.

3.2. Rules for processing Personal Data

Personal Data will be processed fairly, lawfully and in a transparent manner in relation to the Data Subjects.

Personal Data will be collected for specified, legitimate purposes and not processed further in ways incompatible with those purposes.

Personal Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and used.

Personal Data will be accurate, and where necessary, kept up-to-date. Every reasonable step will be taken to rectify or delete, without delay, Personal Data that is inaccurate or incomplete.

Personal Data will be kept only as long as it is necessary for the purposes for which it was collected and processed, taking the legal obligations to preserve records into consideration.

Personal Data will be processed in a manner that ensures appropriate security of personal data as described by Article 4 of this Procedure.

Special Categories of Data will be provided with additional safeguards as provided by Article 3.3 of this Procedure.

Personal Data may be accessed only by persons whose function requires the handling of such Personal Data, on a need-to-know basis.

Schedule I includes a checklist of questions to illustrate the above rules.

Schedule II includes precise procedures to be followed when setting up a new information system, the purpose of which is to ensure that the above rules are complied with.

3.3. Special Categories of Data

Processing of Special Data is prohibited expect if:

-The Data Subject has given his 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. anti-discrimination) 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 his Consent; or

-The processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a Health & Safety or Social Responsibility aim and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the Consent of the Data Subjects; 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.

Article 4 - Security and Confidentiality

4.1. ArcelorMittal IT Baseline Security Controls

Appropriate technical, physical, and organizational measures will be taken to prevent unauthorized access, unlawful processing, and unauthorized or accidental loss, alteration, disclosure, destruction, access or damage to data. These measures are notably described in Schedule III attached to this Procedure (ArcelorMittal IT Baseline Security Controls).

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

All Global tools, Segment-specific processes and local software applications falling in the scope of this Procedure must comply with ArcelorMittal IT Baseline Security Controls.

In order to ensure that any future tool or process will comply with this standard, the ArcelorMittal Baseline IT Security controls will be included as part of the specifications (See Schedule II). Any external consultant having access to ArcelorMittal's systems and tools as a user must be committed to follow AM Baseline IT Security controls and any other policies or procedures relevant to data protection as may be communicated by ArcelorMittal.

ArcelorMittal IT Baseline Security Controls will be updated by the Data Protection Committee on the recommendation of the Group IT Security and Compliance Officer, on an as-needed basis.

The level of protection and security so defined is a minimum standard that all ArcelorMittal Subsidiaries must have in place. ArcelorMittal Subsidiaries are encouraged to adopt additional security measures, when appropriate.

Questions about compliance with ArcelorMittal IT Baseline Security controls (Schedule III) may be addressed to the relevant IT Compliance & Security Officer ("ITCS Officer", See Schedule VI).

4.2. Security breaches

The Data Protection Correspondent and/or the ITCS Officers shall immediately notify the Data Protection Committee of any suspected or actual security breach or similar incident that has, or might have, compromised the privacy or security of any Personal Data. More specifically, 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 shall be notified immediately to the Data Protection Committee.

The concerned ArcelorMittal Controller(s) shall provide, within 24 hours after having become aware of the breach, the following information to the Data Protection Committee:

- A description as to the nature of the breach;
- The name and contact details of the Data Protection Correspondent and/or the ITCS Officers;
- A description of the likely consequences of the breach (including whether it is result in a high risk to the rights and freedoms of the Data Subjects);
- A description of the measures taken or proposed to be taken to address the breach including any measures to mitigate its possible adverse effects.

The concerned ArcelorMittal Controller(s) or ArcelorMittal Processor(s) will collaborate with the Data Protection Committee and follow the latter's recommendations regarding any notification required to be made with the Data Protection Authority or to Data Subjects in respect of the security breach.

Personal data breaches that may result in a risk to the Data Subjects shall be notified without undue delay and, where feasible, not later than 72 hours after having become aware of the breach:

- by the concerned ArcelorMittal Controller(s) located in the EU shall notify their competent Data Protection Authority;
- by the concerned ArcelorMittal Controller(s) located outside of the EU or ArcelorMittal S.A. on its/their behalf to the Luxembourg Data Protection Authority.

The concerned ArcelorMittal Controller(s) or ArcelorMittal Processor(s) shall take all actions to address any such known security breach or attempted breach, and shall cause any external providers to cooperate fully, in accordance with Data Protection Committee's direction. Any Data Protection Correspondent so requested by the Data Protection Committee shall assist in security breach detection and identification.

The concerned ArcelorMittal Controller(s) or ArcelorMittal Processor(s) and the Data Protection Correspondent shall cooperate fully with civil or criminal authority in any investigation or action relating to such breach, or attempted breach.

The security breach shall be documented by the Data Protection Committee in collaboration with the concerned ArcelorMittal Controller in order to share the lesson learned and modify the ArcelorMittal IT Baseline Security Controls and any other relevant policies or procedures accordingly (if necessary). Such documentation, which will be kept by the concerned ArcelorMittal Controller and the Data Protection Committee, will comprise the facts relating to the security breach, its effects and the remedial actions taken in relation to it. It shall be made available to the Data Protection Authority upon request.

4.3. Records of processing

To demonstrate its compliance with this Procedure, each ArcelorMittal Controller must maintain a record of all processing activities carried out under its responsibility and containing the information listed under article 30(1) of the GDPR.

Each ArcelorMittal Processor must maintain a record of all categories of processing activities carried out on behalf of an ArcelorMittal Controller containing the information listed under 30(2) of the GDPR.

The records will be made in writing, including in electronic form and made available to the competent Data Protection Authority on request.

4.4. Data protection impact assessments ("DPIA")

Each ArcelorMittal Controller contemplating processing operations that are likely to result in a high risk to the rights and freedoms of Data Subjects by virtue of their nature, scope or purpose must carry out a data protection impact assessment prior to such operations.

The assessment shall contain at least a general description of the envisaged Processing operations, an assessment of the risks to the rights and freedoms of Data Subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the

protection of Personal Data and to demonstrate compliance with this Procedure taking into account the rights and legitimate interests of Data Subjects.

Where the results of the assessment indicate that the Processing would result in a high risk in the absence of measures taken by the relevant ArcelorMittal Controller, the Data Protection Authority should be consulted prior to the Processing.

4.5. Data protection by design and by default

ArcelorMittal shall adopt internal policies and shall implement appropriate measures that meet the principles of data protection by design and data protection by default. These policies include Schedule II which sets out precise procedures to be followed when setting up a new information system.

The principles of data protection by design and data protection by default require that:

- both at the time of the determination of the means for processing and at the time of the Processing itself, ArcelorMittal shall implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Procedure and ensure the protection of the rights of the Data Subjects; and

- ArcelorMittal shall implement mechanisms for ensuring that, by default, only those Personal Data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default Personal Data are not made accessible to an indefinite number of individuals.

Article 5 - Rights of Data Subjects

5.1. Data Controller

Each ArcelorMittal Controller will be responsible for and able to demonstrate compliance with this Procedure.

Each Subsidiary is deemed to be Controller of its HR Data, unless otherwise established by a specific privacy policy or approved by the Data Protection Committee.

(For information purposes only : for non-HR information systems, the legal entity acting as “Business Owner”, as understood under ArcelorMittal usual practices, can be considered as Controller).

5.2. Transparency and information right

5.2.1 Transparency

ArcelorMittal shall process Personal Data in a transparent manner.

Data Subject are entitled to have easy access to this Procedure. This Procedure shall thus be made readily available to every Data Subject. The parts of this Procedure relevant to Data Subjects shall be uploaded onto both ArcelorMittal intranet and internet corporate website. A copy of this Procedure shall also be made available to the Data Subjects, either on paper, upon request to the Data Protection Correspondent for your country/region as set out in Schedule VI, or by way of an electronic tool.

5.2.2 Information Right

The Data Subject shall be informed of the transfer and processing of their Personal Data.

Each ArcelorMittal Controller shall provide the Data Subject with at least the following information, except where the latter already has it:

a) the identity of this ArcelorMittal Controller and of its representative;
b) the contact details of the Data Protection Correspondent, if any;
c) the purposes of the processing and the legal basis for the processing;
d) the recipients or categories of recipients;
e) the categories of Personal Data concerned, where Personal Data have not been obtained from the Data Subject;
f) where the processing is based on the legitimate interest, the legitimate interests pursued by the ArcelorMittal Controller or by a third party;
g) where applicable, the fact that Personal Data will be transferred to a third country or international organization as well as the reference to the appropriate or suitable safeguards and the means by which to review them;
h) the period for which the Personal Data will be stored, or the criteria used to determine that period;
i) the existence of the right to request access to and rectification or erasure of Personal Data or restriction of Processing or to object to Processing as well as the right to data portability;
j) where the Processing is based on the Consent of the Data Subject, the existence of the right to withdraw Consent at any time;
k) the right to lodge a complaint with a Data Protection Authority;
l) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide such data; and
m) the existence of automated decision-making, including profiling, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

Where the data has not been directly obtained from the Data Subjects, the ArcelorMittal Controller will provide the information above at the time of undertaking the recording of Personal Data or if a disclosure to a third party is envisaged, no later than the time the Personal Data are first disclosed.

Where the data have not been obtained from the Data Subject, the obligation to inform the Data Subject does not apply if:
- The Data Subject already has the information;

- The provision of such information proves impossible or would involve a disproportionate effort;
- Recording or disclosure is expressly laid down by law; or
- Personal Data must remain confidential subject to an obligation of professional secrecy regulated by applicable law.

5.3. Rights of access, rectification, erasure, restriction and objection to the processing

Every Data Subject will be clearly informed on how he or she can exercise the rights described in the following paragraphs through, depending on the location, Intranet and notice board postings, Privacy Policy and from the Data Protection Correspondent or employee handbook information.

Specific guidelines and procedures shall be in place within ArcelorMittal, at local level, to ensure the exercise of the rights specified below. In particular, identified ArcelorMittal employees will be trained to recognise a Data Subject access, rectification or erasure request. ArcelorMittal Controllers may disregard requests that are manifestly unreasonable.

Data Protection Correspondents and the Data Protection Committee, shall always be at the disposal of both ArcelorMittal Controllers and Data Subjects to provide any help.

5.3.1 Right of access

Every Data Subject has the right to obtain without constraint at reasonable intervals and without excessive delay or expense confirmation as to whether or not data relating to him/her are being processed, and where this is the case, access to at least the following information:

a) the purposes of the processing;
b) the categories of data concerned;
c) the recipients or categories of recipients to whom the data are disclosed;
d) the period for which the Personal Data will be stored;
e) the rights granted to the Data Subjects, including the right to request rectification and erasure of incorrect data;
f) the right to lodge a complaint with a Data Protection Authority;
g) the existence of the right to request from the ArcelorMittal Controller rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the Data Subject or to object to such processing;
h) where the Personal Data are not collected from the Data Subject, any available information as to their source;
i) as the case may be, the existence of automated decision-making, including profiling, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

For the avoidance of doubt, a Data Subject has no right to have access to any Personal Data not relating to him/her.

5.3.2 Right of rectification

Every Data Subject has the right to obtain the rectification, without undue delay, the rectification of incomplete or inaccurate Personal Data concerning him/her.

5.3.3 Right of erasure

Every Data Subjects shall also be entitled to obtain, without undue delay, the right to erasure of Personal Data concerning him or her notably in the following cases:
-The Personal Data are no longer necessary in relation to the purposes for which they were collected or processed;
-The Data Subject has withdrawn his/her Consent to the processing and there is no other legal ground; or
-The Personal Data have been unlawfully processed.

This right of erasure will however not apply where processing is necessary, for instance, for compliance with a legal obligation requiring processing or for the establishment, exercise or defense of legal claims.

5.3.4 Right of restriction

Every Data Subject has the right to obtain from the ArcelorMittal Controller restriction of processing where:
-The accuracy of the Personal Data is contested by the Data Subject, for a period enabling the controller to verify the accuracy of the personal data;
-The Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
-The ArcelorMittal Controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims; and
-The Data Subject has objected to processing, pending the verification whether the legitimate grounds of the ArcelorMittal Controller override those of the Data Subject.

Where Processing has been restricted, such personal data shall, with the exception of storage, only be processed with the Data Subject's Consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another person or for reasons of important public interest.

5.3.5 Right of objection to the processing

Every Data Subject has the right to object, at any time on grounds relating to their particular situation, to the processing of their Personal Data justified on the ArcelorMittal Controller's legitimate interests. Unless the ArcelorMittal Controller demonstrates compelling legitimate grounds for the processing, the processing must cease.

Every Data Subject has the right to object, on request and free of charge, to the processing of Personal Data relating to him/her for the purposes of direct marketing.

5.4. Rights in case automated individual decisions are taken

Every Data Subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless that decision:
a) is based on the Data Subject's Consent;
b) is necessary for the conclusion or execution of a contract between the ArcelorMittal Controller and the Data Subject and the ArcelorMittal Controller has implemented suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests; or
c) is authorized by a law applicable to the ArcelorMittal Controller and which lays down suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests

The suitable measures mentioned in the above paragraph will at least contain the right for Data Subjects to obtain human intervention on the part of the ArcelorMittal Controller, so that the Data Subject may express his or her point of view and to contest the decision.

The Data Subjects are informed that the rights described in this Article 5 may under certain circumstances not be exercised by them due to restrictions imposed under applicable law notably to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Article 6 - Data Transfers

Personal Data can be processed by information systems owned and controlled by an external Processor.

Before transmitting Personal Data to any such provider, the ArcelorMittal Controller concerned must choose a provider providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures and the protection of the Data Subjects' rights.

6.1. Data Transfers to an External Processor ("Vendor") in the EU or outside the EU

1 : No ArcelorMittal Personal Data will be communicated/made available to an external Processor without having a written contract signed between the ArcelorMittal Controller concerned and such external Processor. Such contract shall include the standard provisions attached to this Procedure (See Schedule V).

2 : No ArcelorMittal Personal Data will be communicated/made available to an external Processor, unless such external Processor provides a level of protection equivalent to that afforded by ArcelorMittal IT Baseline Security controls and that of any other policies or procedures relevant to data protection.

3 : In case of cross-border transfer from Europe to any country outside of Europe, the latest standard contractual clauses imposed by the European legislation (set of standard contractual clauses for the cross-border transfer of Personal Data From Controller to Processor) or by any

national law shall also be included in the Agreement signed between the ArcelorMittal Controller concerned and the Processor, when applicable.

The Security Assessment described in this Article must be carried out before contract signature (or contract renewal) in all scenarios where an external Processor will have access to any Personal Data.

The purpose of the Security Assessment is the following: the external Processor must provide the same level of protection for ArcelorMittal's Personal Data as provided by ArcelorMittal's Baseline IT Security controls and any other policies or procedures relevant to data protection.

Before transmitting Personal Data to a provider who is not an ArcelorMittal Subsidiary, the following steps shall be taken by the ArcelorMittal Controller:

→ Step 1 : Security Assessment

The concerned ArcelorMittal Controller shall communicate the attached Security Assessment Questionnaire (Schedule IV) to the Vendor willing to provide services to ArcelorMittal.

The Vendor's response shall be evaluated by the IT Compliance & Security Officer for the purpose of assessing whether the level of protection so afforded is equivalent to that afforded by ArcelorMittal IT Baseline Security Controls (Schedule III) and any other policies or procedures relevant to data protection.
When doing this evaluation, the IT Compliance & Security Officer shall be given by the ArcelorMittal Controller the opportunity to discuss with the Vendor, suggest improvement to Vendor's security measures in order to check whether the Vendor actually provides an equivalent level of protection.

In the event the result of the Assessment is negative, because of a critical problem in Vendor's Policies, the negotiation process will be blocked, and no contract will be signed, unless the Vendor commits to solve the problem(s) raised by the ITCS Officer within a short period of time.

→ Step 2 : Contract

In the event the Vendor's response to the Security Assessment Questionnaire is deemed satisfactory by the ITCS Officer, such response shall be included in the contract signed between the ArcelorMittal Controller and the vendor. The response shall become an integral part of the contract.

The contract signed between the ArcelorMittal Controller concerned and the external Processor shall include the standard provisions attached to this Procedure (See Schedule V). However, in the event and to the extent that the Data Protection Laws impose stricter obligations concerning such agreement, the Data Protection Laws shall prevail so that the standard clauses included in Schedule V and providing a lower protection than the Data Protection Laws shall be replaced by new clauses compliant with Data Protection Laws.

In case of cross-border transfer from Europe to any country outside of Europe, the latest standard contractual clauses imposed by the European legislation (set of standard contractual

clauses for the cross-border transfer of Personal Data From Controller to Processor) or by any national law shall also be included in the Agreement signed between the ArcelorMittal Controller concerned and the Processor, when applicable.

6.2. Data Transfers to an ArcelorMittal Processor

Any ArcelorMittal Processor must comply with and implement the requirements contained in the ArcelorMittal IT Baseline Security Controls and any other policies or procedures relevant to data protection as may be communicated by ArcelorMittal.

ArcelorMittal IT Baseline Security Controls are automatically incorporated in any and all contracts signed between any ArcelorMittal Processor and its customers (i.e. ArcelorMittal Controllers).

The purpose for which the Personal Data shall be processed by the ArcelorMittal Processor on behalf of its ArcelorMittal Controller shall be mutually agreed in written between ArcelorMittal Processor and its ArcelorMittal Controller. ArcelorMittal Processor shall not process the Personal Data for any other purpose. ArcelorMittal Processor shall transfer the Personal Data only in accordance with written instructions from its ArcelorMittal Controller.

The contract signed between the ArcelorMittal Controller concerned and ArcelorMittal Processor shall include the standard provisions attached to this Procedure (See Schedule V).

When sub-contracting part of all of the services to an External Processor, ArcelorMittal Processor shall comply with the process described in Article 6.1 above.

6.3. Data Transfers to an External Data Controller

All transfers of Personal Data From Europe to External Data Controllers located out of Europe must respect the EU rules on trans-border data flows.

To the extent that such transfers occur on a regular basis, any of the appropriate safeguards listed under article 46 of the GDPR must be used for transfers to External Data Controllers located outside of Europe in countries not deemed by the European Commission to provide an adequate level of protection for personal data. In practice, the latest standard contractual clauses shall be included in the Agreement signed between the Subsidiary concerned and the External Data Controller, when applicable.

6.4. Data Transfers to a new ArcelorMittal Subsidiary

No transfer of Personal Data to a new ArcelorMittal Subsidiary shall be made before (i) signature of this Procedure by such new Subsidiary, and (ii) appointment of a Data Protection Correspondent, if there is no Data Protection Correspondent in the concerned country/segment.

Article 7 - Implementation of this Procedure and enforcement mechanisms

- Compliance at local/regional level (Data Protection Correspondent and ITCS Officers)
- ArcelorMittal Data Protection Committee
- Training programme
- Internal Complaint Mechanism
- Audit programme
- Mutual assistance and cooperation with Data Protection Authorities
- Actions in case of national legislation preventing respect of this Procedure

7.1. Compliance at local/regional level (Data Protection Correspondent and ITCS Officers)

Data Protection Correspondent

Each ArcelorMittal Country Manager or Segment Manager will designate one or several Data Protection Correspondent(s). A precise geographical and/or organizational scope shall be assigned to each Data Protection Correspondent.

The Data Protection Correspondent will coordinate all measures necessary in order to ensure Subsidiaries within his/her scope comply with their obligations under this Procedure. To this end, an “Audit Checklist", as described under Schedule VII shall be used at local level to make compliance checks for each software application/database processing personal data within the Subsidiaries.

The Data Protection Correspondent will supervise compliance of these Subsidiaries with this Procedure and will monitor training within the Subsidiaries.

The Data Protection Correspondent will also act as key contact person for any complaint arising in his/her scope as described in Article 7.4 of this Procedure (“Internal Complaint Mechanism”) and for any Security Breach as described in Article 4.2 of this Procedure (“Security Breach”). The Data Protection Correspondent has the duty to cooperate fully with his peers in any matter relating to the proper performance of this Procedure, especially in matters involving or impacting several ArcelorMittal Controllers in different countries/segments.

The Data Protection Correspondent will keep the Data Protection Committee constantly informed about any complaint or other issue/problem arising in the scope of this Procedure.

In the event the Data Protection Correspondent does not fulfil its obligations, the Data Protection Correspondent may be discharged by the Data Protection Committee. In such case, a new Data Protection Correspondent will be designated by the Country Manager or the local management.

IT Compliance and Security (ITCS) team

The mission of IT Compliance & Security Officers is to 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.

ITCS Officers will more particularly implement and monitor deployment of ArcelorMittal IT Baseline Security Controls both internally and also with regard to external Processors by checking for equivalent minimum security level as set forth in Article 6.1 of this Procedure.

7.2. ArcelorMittal Data Protection Committee

The Data Protection Committee shall remain in effect for the duration of this Procedure.

The Data Protection Committee shall consist of four (4) core members designated within ArcelorMittal S.A.,

. the Group Compliance and Data Protection Officer,
. One (1) of which shall be designated by the ArcelorMittal Group CIO,
. One (1) of which shall be designated by the ArcelorMittal EVP Human Resource and
. a secretary, designated by ArcelorMittal Group Compliance and Data Protection Officer.

The members of the Data Protection Committee are identified on Schedule IX.

The Data Protection Committee shall also include all or some Data Protection Correspondents, as deemed necessary by the core members to effectively cover the items on the agenda.

In addition, ArcelorMittal's head of Internal Assurance may, at its discretion, participate himself or designate a representative to attend the meetings of the Data Protection Committee.

The Data Protection Committee shall be led by the Group Compliance and Data Protection Officer. Each member may, at his/her discretion, invite other members or consultants to attend meetings of the Data Protection Committee. For sake of clarity, any consultant so invited will not take part in any decision and will not be deemed to be a member of the ArcelorMittal Data Protection Committee.

The Group CIO, the EVP Human Resource and the Group Compliance and Data Protection Officer may withdraw the designation of any of the member(s) designated by him and designate a replacement (whose term shall commence immediately) at any time by giving notice of the withdrawal and replacement to the other members.

The Data Protection Committee shall meet at such times and places as the members of the Data Protection Committee shall from time to time agree, but in no event less than once every three (3) months.

The agenda for each meeting shall be established by the secretary, and communicated to the members of the Data Protection Committee and also to the Data Protection Correspondents.

Within three (3) business days following each meeting of the Data Protection Committee, the secretary of the Data Protection Committee shall prepare and send to the members of the Data Protection Committee a detailed written report of decisions taken at the meeting.

This Report shall also be communicated to the Data Protection Correspondents.

The Group Compliance and Data Protection Officer shall:

(a) enjoy the highest management support for the fulfilling of its tasks and shall report directly to the highest management level within ArcelorMittal,

(b) with the assistance of the Data Protection Committee, deal with the Data Protection Authorities' investigations and monitor and annually report on compliance with this Procedure at global level.

The Data Protection Committee shall:

(i) maintain and update the list of ArcelorMittal Subsidiaries bound by this Procedure,

(ii) ensure that an identified individual keeps a fully updated list of the ArcelorMittal Subsidiaries bound by this Procedure, keeps track of and records any update to this Procedure and provides the necessary information to the Data Subjects or Data Protection Authority upon request.

(iii) maintain and update the list of Data Protection Correspondents, in accordance with the requests of ArcelorMittal managers at local/regional level (See the initial list in Schedule VI),

(iv) oversee the implementation of this Procedure and the performance of the Subsidiaries, including future Subsidiaries,

(v) resolve any major issues / problems that may arise,

(vi) initiate, validate and update specific policies for Global Tools (no such policy shall be enforceable without Data Protection Committee's prior approval),

(vii) update Schedule II and Schedule III, IV, V, VI, VII, VIII and X, with full authority. Such change shall be notified to the Data Protection Correspondents and to the ITCS and will become binding upon the date mentioned in the notification.

(viii) modify this Procedure on an as-needed basis, for example, to comply with changes in laws, regulations, ArcelorMittal practices and procedures, ArcelorMittal corporate structure, or requirements imposed by Data Protection Authorities. Changes of this core document shall be notified without delay to the Subsidiaries, and shall be deemed accepted by each of them after a period of two (2) months, unless specifically rejected in writing by a Subsidiary,

(ix) ensure that changes of this core document and changes to the list of ArcelorMittal Subsidiaries bound by this Procedure are notified once a year to the competent Data Protection Authority with a brief explanation of the reasons justifying the changes,

(x) ensure that changes of this core document that potentially affect the level of protection offered by this Procedure or otherwise significantly affect this

Procedure (e.g. changes to its binding character) are promptly notified to the Data Protection Authority.

7.3 Training programme

Appropriate training on this Procedure shall be provided to personnel who have permanent or regular access to Personal Data, are involved in the collection of Personal Data or in the development of tools used to process Personal Data.

The Data Protection Correspondent will be in charge of this training programme, which may take the form of an e-learning solution.

7.4 Internal Complaint Mechanism

Any Data Subject may complain that any ArcelorMittal Controller is not complying with this Procedure.

The Data Protection Correspondent of the concerned ArcelorMittal Controller, who shall have an appropriate level of independence in the exercise of his or her functions, will be responsible for handling such complaint in a timely manner. The complaint will be dealt with within one (1) month following the complaint. Taking into account the complexity and number of the complaints, this one (1) month period may be extended at maximum by two (2) further months, in which case the Data Subject will be informed accordingly.

In the event an issue cannot be resolved by the Data Protection Correspondent, such issue will be escalated by him/her to the Data Protection Committee.

The Data Subject may at any time lodge a claim to the Data Protection Authorities or file a suit before the jurisdictions described in Article 8 of this Procedure.

7.5 Audit Plan

The ArcelorMittal Group compliance with this Procedure shall be audited on a regular basis by the Internal Assurance Department. The frequency of such audits shall be no less than once a year. The Internal Assurance Department may be assisted by a member of the Data Protection Committee. An external team may also be appointed.

Such audit may specifically cover all aspects of this Procedure including methods of ensuring that corrective actions will take place, both inside Europe and outside Europe. In addition, more general IT audits will also be performed on a regular basis.

Each Audit shall be followed by a report including detailed corrective actions, if necessary (Phase 1). These measures will be taken by the ArcelorMittal Subsidiary(s) within a specific

timeframe specified in the report. A second visit will then be performed in order to ensure that all corrective actions have been taken (Phase 2).

The Internal Assurance Department and the Data Protection Committee shall establish an annual Audit Plan.

A copy of all audit reports shall be communicated (i) to the Data Protection Correspondent(s) concerned (ii) to the Data Protection Committee (iii) to the EVP Human Resource, the Group CIO and the Group Compliance and Data Protection Officer (iv) to the management of the concerned Subsidiary(s) and where appropriate, to the management of ArcelorMittal S.A.
Data Protection Authorities can have access to the reports of the audit upon request. Data Protection Authorities can carry out a data protection audit of any Subsidiary if required.

The Audit reports shall not be communicated in any manner to any body or person not mentioned in this Article 7.5 ("Audit Plan").

7.6. Mutual assistance and cooperation with Data Protection Authorities

- Subsidiaries shall cooperate and assist each other to handle a request or complaint from a Data Subject or an investigation or inquiry by Data Protection Authorities.

- In the event of any breach of this Procedure outside of Europe, the Data Protection Authority in the country where the Data Exporter is located may request an audit to be performed by ArcelorMittal Internal Assurance Department. Such audit shall be performed in accordance with Article 7.5 of this Procedure.

- Subsidiaries will abide by the advice of the Data Protection Authorities on any issues regarding the interpretation of this Procedure.

7.7 Actions in case of national legislation preventing respect of this Procedure

Where a Subsidiary has reasons to believe that the legislation applicable to it prevents such Subsidiary from fulfilling its obligations under this Procedure and has substantial effect on the guarantees provided by this Procedure, the Subsidiary will promptly inform the Data Protection Committee (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

In addition, where there is conflict between national law and the commitments in this Procedure the Data Protection Committee will take a responsible decision on what action to take and will consult the competent Data Protection Authorities in case of doubt.

Notwithstanding the above, where a national law binding a Subsidiary outside of Europe is likely to have a substantial adverse effect on the guarantees provided by this Procedure, the Subsidiary shall report it to the Data Protection Committee. This Committee will, in turn, report such matter to the competent Data Protection Authority.

The above obligation includes reporting any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body. In such a case, the competent Data Protection Authority will be clearly informed by the Data Protection Committee about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

If in specific cases the suspension and/or notification are prohibited, the requested Subsidiary will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

If, in the above cases, despite having used its best efforts, the requested Subsidiary is not in a position to notify the Data Protection Committee for this Committee to then notify the competent Data Protection Authority, the Subsidiary will annually provide general information on the requests it received (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

In any case, transfers of personal data by a Subsidiary to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Article 8 - Liability

Any Data Subject can enforce the following principles as third-party beneficiary rights before the appropriate Data Protection Authority or court, in order to seek remedy and obtain compensation if any Subsidiary does not respect those principles:

- National legislation preventing respect of this Procedure, as described in Article 7.7,
- Rules for processing Personal Data, as described in Article 3.2,
- Right to complain through the internal complaint mechanism described in Article 7.4,
- Cooperation duties with Data Protection Authority as described in Article 7.6,
- Liability and jurisdiction provisions as in the following Article and in Article 7.4.
- Purpose limitation, as described in Article 3.2,
- Data quality and proportionality, as described in Article 3.2,
- Criteria for making the processing legitimate, as described in Article 3.1,
- Transparency and easy access to this Procedure, as described in Article 5.2,
- Rights of access, rectification, erasure, restriction, blocking of data and object to the processing, as described in Article 5.3,
- Rights in case automated individual decisions are taken, as described in Article 5.4,
- Security and confidentiality, as described in Article 4,
- Restrictions on onward transfers outside of the group of companies, as described in Article 6.1 and Article 6.3.
- Rights in relation to liability, as described in this Article 8.

Each Subsidiary accepts responsibility for any breach of this Procedure subject to the liability mechanism specified in Article 8.2 for violation.

The Data Subject may at any time:

- lodge a complaint before the competent Data Protection Authority (i.e. the authority of the jurisdiction of his or her residence, of his or her place of work or of the place of the alleged infringement); or
- lodge a claim to the competent courts in the jurisdiction of his or her residence or in which the Data Exporter located in the EU is established.

These rights do not extend to those elements of this Procedure pertaining to internal mechanisms implemented within ArcelorMittal such as detail of training, audit programmes, compliance network, and mechanism for updating the rules.

8.1. Obligation to cure any breach

In the event any Subsidiary is in breach of this Procedure, such breaching Subsidiary shall cure the breach and take the necessary actions to comply with this Procedure.

The Subsidiaries agree that they have to remedy any breach, default or non-compliance with this Procedure, in order to avoid reoccurrence of the problem in the future.

8.2. Obligation to pay damages to the Data Subject

Data Subjects have the right to judicial remedies and the right to obtain redress and, where appropriate, compensation for any breach of one of the enforceable principles listed in Article 8 above.

In the event the Subsidiary breaching or allegedly breaching this Procedure is not located in the EU, the following rules shall apply

o The Data Exporter shall be liable for damage to the Data Subject resulting from any violation of the provisions of this Procedure by the breaching Subsidiary.

o The breaching Subsidiary shall indemnify the Data Exporter for any cost, charge, damages, expenses or loss it has incurred in respect of the breach.

o The competent courts or other authorities in the EU will have jurisdiction and the Data Subject will have the rights and remedies against the Data Exporter as if the breach had caused by the latter in the EU Member States in which this Data Exporter is based.

o the Data Exporter will have the burden of proof to demonstrate that the relevant Subsidiary is not liable for any breach of the rules which has resulted in the Data Subject claiming damage.

o In the event the Data Exporter can prove that the relevant Subsidiary is not liable for the violation, it may discharge itself from any responsibility.

SCHEDULE I

PRINCIPLES FOR PROCESSING PERSONAL DATA

CHECKLIST

The purpose of this checklist is to illustrate the way the Data Protection principles must be understood.

"Personal Data will be processed fairly and lawfully"

- Is there a clear business need to process this information?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?

"Personal Data will be collected for specified, legitimate purposes and not processed further in ways incompatible with those purposes"

- Do I know what I'm going to use this Personal Data for?
- If I'm asked to pass on Personal Data, would the people about whom I hold information expect me to do this?

"Personal Data will be adequate, relevant to and not excessive for the purposes for which they are collected and used"

- Do I really need this information about an individual?

"Personal Data will be accurate, and where necessary, kept up-to-date. Reasonable steps will be taken to rectify or delete Personal Data that is inaccurate or incomplete"

- Am I sure the personal information is accurate and up to date?

"Personal Data will be kept only as long as it is necessary for the purposes for which it was collected and processed, taking the legal obligations to preserve records into consideration"

- Do I delete or destroy personal information as soon as I have no more need for it?

"Sensitive Data will be provided with additional safeguards such as provided by the EU Regulation 2016/679"

- Have I trained my staff in their duties and responsibilities under the ArcelorMittal Data Protection Procedure, and are they putting them into practice?

"Personal Data may be accessed only by persons whose function includes the handling of such Personal Data, on a need-to-know basis"

- Is access to Personal Data limited to those with a strict need to know?
- Am I satisfied the information is being held securely?

"*Personal Data may 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 ('integrity and confidentiality')"*

- Do I comply with all internal policies and procedures and follow required applicable security measures in the way I am holding the Personal Data?
- Am I confident that the security technical or organisational measures in place ensure sufficient integrity and confidentiality of the Personal Data held?

"*The Data Controller shall be responsible for, and be able to demonstrate compliance with, the above principles ('accountability')*"

- Am I confident that I can demonstrate such compliance and provide related evidence?

SCHEDULE II

DATA PROTECTION CHECKPOINT BEFORE COMPLETING THE DESIGN PHASE OF A PROJECT

The design phase of any project is crucial to ensure that the resulting process/application is compliant with this Procedure. "Design phase" means the phase where the architecture, the specifications and the functionalities of the system are defined by the project team, on behalf of the Controller(s).

The principles set forth in this Procedure must be integrated into any new Information System or any substantial evolution thereof, as early as the design phase.

This SCHEDULE describes the way this objective will be achieved.

As a preliminary remark, it is worth noting that this Procedure is technology-neutral. In the event an existing system is just re-developed on the basis of a new technology, while keeping the same processes, the same data, the same organizational and security measures, the recommendations issued at the time the existing system had been designed will have to be followed, but no new Data Protection checkpoint will be needed for such re-development.

This SCHEDULE is applicable to any new information system falling in the scope of this Procedure, or any evolution thereof (provided however the way Personal Data will be processed will change).

- New Global Tool

The Data Protection Committee must be consulted by the project team prior to the validation of the design of any new Global Tool.
The Data Protection Committee will advise and assist the project team in ensuring that the design of the system is compliant with this Procedure.
In any event, the IT Baseline Security controls (See SCHEDULE III) shall be included in the specifications.

- Segment-specific processes

The Data Protection Correspondents of the concerned countries must be consulted by the project team prior to the validation of the design of any new Segment-specific process.
The Data Protection Correspondents will advise and assist the project team in ensuring that the design of the system is compliant with this Procedure.
In any event, the IT Baseline Security controls (See SCHEDULE III) shall be included in the specifications.
In the case where the new system is expected to use Personal Data taken from an already-existing tool or process, the project team shall also consult the Data Protection Committee.

- Local software applications

The Data Protection Correspondent of the concerned country must be consulted prior to the validation of the design of the system.
The Data Protection Correspondent will advise and assist the project team in ensuring that the design of the system is compliant with this Procedure.

In any event, the IT Baseline Security controls (See SCHEDULE III) shall be included in the specifications.
In the case where the new software application is expected to use Personal Data taken from an already-existing system, the Data Protection Committee must also be consulted.

This rule can entail different actions, depending on the particular case or application. For example, in some cases it may require eliminating/reducing Personal Data or preventing unnecessary processing, or improving security measures in order to comply with the IT Baseline Security controls.

The Controller(s) will be responsible to translate the recommendations of the Data Protection Correspondent into the reality of the system.

When the Data Protection Correspondent and/or the Data Protection Committee consulted by the project team or by a Data Protection Correspondent have identified that the contemplated tool, process of application is likely to result in a high risk to the rights and freedoms of Data Subjects by virtue of their nature, scope or purpose, a DPIA will be conducted prior to such new operations as set out under Article 4.4 of the Procedure.

Where the results of the assessment made indicate that the processing would result in a high risk in the absence of measures taken by the relevant ArcelorMittal Controller, the Data Protection Authority will be consulted prior to the processing.

Last updated version of the Rules : http://www..... Arcelormittal Intranet

SCHEDULE III

BASELINE IT SECURITY CONTROLS

SCHEDULE IV

SECURITY ASSESSMENT QUESTIONNAIRE ("SAQ")

SCHEDULE V

ARCELORMITTAL STANDARD CONTRACTUAL CLAUSE FOR PROCESSORS

This clause must be included and is MANDATORY in all contracts between an ArcelorMittal Subsidiary acting as Data Controller and a Processor which is acting as a contractor and to which the ArcelorMittal Subsidiary will disclose Personal Data falling in the scope of this Procedure by means of a structured flow of European Personal Data from the ArcelorMittal Subsidiary to the Processor in furtherance of the purpose of the contract.
It is expected that the Business Agreement in which this clause will be included already provides a clear description of (i) the overall purpose of the contract (ii) the services to be performed and (iii) the subject-matter, duration, nature and purpose of the personal data processing to be carried by the Processor by virtue of the contract and (iv) the type of personal data to be transferred or made available to the Processor and the categories of individuals whom these data relate to.

Data Protection

"Personal Data" means any data relating to an identified or identifiable person (i) provided by ArcelorMittal or any ArcelorMittal Subsidiary which comes into the possession of Vendor or any Vendor subsidiary pursuant to this Agreement (ii) created under or arising out of data provided by ArcelorMittal or any ArcelorMittal Subsidiaries pursuant to this Agreement (iii) automatically generated by the services provided by Vendor to ArcelorMittal.

Vendor shall process Personal Data (including Personal Data originally processed by ArcelorMittal) only when it is acting to provide the services described in this Agreement and under any other documented instructions from ArcelorMittal agreed upon between the Parties. If Vendor is required by EU or Member States law to process Personal Data for other purposes, it shall inform ArcelorMittal of this requirement. Vendor shall ensure that Vendor's staff who have access to or are responsible for the processing of Personal Data are bound by a contractual or statutory obligation of confidentiality.
Upon termination or expiration of this Agreement or upon written request by ArcelorMittal, Vendor shall: (i) immediately cease processing the Personal Data; and (ii) return to ArcelorMittal, or at ArcelorMittal's option destroy, the Personal Data and all copies, notes or extracts thereof, within seven (7) business days of the date of termination or expiration of this Agreement or of receipt of request. Upon the request of ArcelorMittal, Vendor shall also confirm in writing that Vendor has complied with the obligations set forth in this clause.

Vendor shall at all times comply with the IT Security Policies (*) attached to this Agreement and with all applicable laws and regulations relating to data protection ("Data Protection Laws"). In the event and to the extent that the Data Protection Laws impose stricter obligations including stricter security measures on the Vendor than under this Agreement, the Data Protection Laws shall prevail.

Vendor shall not communicate or otherwise transfer any Personal Data to any third party including any Vendor subsidiary or sub-contractor ("Sub-Processor") without the prior written consent of ArcelorMittal which consent may be withheld for any

reason or for no reason at ArcelorMittal sole discretion. Prior to seeking ArcelorMittal's consent, Vendor shall provide ArcelorMittal with full details of the proposed Sub-Processor's involvement including but not limited to the identity of the Sub-Processor, its data security record, the location of its processing facilities, a description of the access to ArcelorMittal Data proposed and any other information ArcelorMittal may reasonably request in order to assess the risks involved in allowing the Sub-Processor to process Personal Data. For ArcelorMittal to provide its consent to any proposed sub-processing, the Vendor must enter into a written agreement with the Sub-Processor containing equivalent terms to this Agreement (provided that Vendor shall not be entitled to permit the Sub-Processor to further sub-contract or otherwise delegate all or any part of the Sub-Processor's processing without ArcelorMittal's prior written consent at ArcelorMittal's sole discretion).

In any event Vendor shall procure that its authorized Sub-Processor comply in all respects with the data protection obligations contained in this Agreement and with all Data Protection Laws. Vendor resorting to a Sub-Processor shall remain fully liable to ArcelorMittal for the performance of the Sub-Processor's data protection obligation if the latter fails to them.

When applicable under European Union Regulation 2016/679 (the GDPR), ArcelorMittal may require Vendor to execute such additional terms, including without limitation executing the Standard Contract Clauses for the transfer of Personal Information to third countries under the GDPR, and the Vendor shall abide by them.

Vendor shall make available to ArcelorMittal all information necessary to demonstrate compliance with its data protection obligations and allow for and contribute to audits, including inspection, conducted by ArcelorMittal or an auditor mandated by ArcelorMittal. Vendor shall communicate to ArcelorMittal any and all audit reports issued by Vendor's Internal Audit Department related in whole or in part to the services provided to ArcelorMittal.

Taking into account the nature of the personal data processing and the information available to Vendor, Vendor will provide assistance to ArcelorMittal in ensuring compliance with ArcelorMittal's obligations under the GDPR to (i) implement appropriate technical and organisational measures in relation to Personal Data to ensure a level of security appropriate to the risk, (ii) notify personal data breaches to the supervisory authority and to the data subjects and (iii) carry out data protection impact assessment. In particular, Vendor will notify in writing the ArcelorMittal IT Compliance & Security Officer of any security breach or suspected security breach that has, or might have, compromised the privacy or security of any ArcelorMittal data (including Personal Data) within twenty four (24) hours of such breach or suspected breach. Such notification shall include: (i) a description of the nature of the personal data breach (including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned), (ii) the name and contact details of the data protection officer or other contact point where more information can be obtained, (ii) a description of the likely consequences of the personal data breach if such consequences would not be clear to ArcelorMittal (iii)

all measures already taken and to be taken by Vendor in order to cure the breach or suspected breach. Where Vendor cannot provide all this information at the same time within the twenty four (24) hour period, the information may be provided in phases without undue delay.

Vendor shall fully assist ArcelorMittal, including by implementing appropriate technical and organisational measures where possible, with responding to any Data Subject's request to exercise one of his/her data protection rights conferred by the GDPR (including the right to access his/her Personal Data). In the event Vendor is directly required by a Data Subject to provide information regarding his/her Personal Data, Vendor shall immediately forward such request to ArcelorMittal and Vendor shall not provide any response to the Data Subject without being required to do so by ArcelorMittal.

Vendor shall assist ArcelorMittal in fulfilling registration or other applicable requirements under privacy or data protection laws, including without limitation, providing requested information and registering with data protection authorities or joining self-regulatory programs as requested by ArcelorMittal.

For any question regarding the processing of Personal Data by ArcelorMittal in relation to the Agreement, Vendor can contact the ArcelorMittal Data Protection Committee at dataprotection@arcelormittal.com.

Comments:

In the above contractual provision, "Vendor" means the Processor, whether it is part of the ArcelorMittal group or not, and "ArcelorMittal" means the concerned ArcelorMittal Controller.

If necessary, the wording of the above clauses may be adapted to the wording of the Agreement, without affecting the level of commitment of the Processor.

If necessary under applicable EU Member State law, the wording of the above clause may be adapted to comply with such law without affecting the level of commitment of the Processor.

The contract signed between the ArcelorMittal Controller and the Processor must also include an "Audit Right" clause. According to this clause, ArcelorMittal Controller shall have the right to audit Vendor's compliance with ArcelorMittal IT Baseline Security controls, throughout the contract term.

(*) The IT Security Policies mentioned in the third paragraph result from the Security Assessment. In most cases, it will take the form of Vendor's Security Policies, possibly amended in order to comply with ArcelorMittal IT Baseline Security Controls.

Last updated version of the clauses : http://www..... arcelormittal Intranet

SCHEDULE VI

NB : For security reason, this SCHEDULE VI will be left blank in the version made public, outside of ArcelorMittal. This SCHEDULE VI will be included in the copy of the Procedure posted on the Intranet.

DATA PROTECTION CORRESPONDENTS & ITCS

SCHEDULE VII

AUDIT CHECKLIST

Data Protection Compliance Audit

Check-list

Name of the Software Application/Database

Purpose(s) of the Application

Name/Department of the person responsible for this Application
. IT aspects
. functional aspects

Who are the Data Subjects
(all AM employees ? or a specific category of AM employees ? AM customers? …)

How many Data Subjects do we have in this process?
(broad idea)

What Personal Data do we have in this process?
(screen shots)

Are there sensitive data?

Where do the data come from?
(In other words, what is(are) the source(s) of the data ?) Directly from the Data Subjects or what ?

How long will the data be stored?

Who has access to the data?
. within AM
. outside of AM

Access to the data : From where ? Is there any cross-border transfer of data?

Are the data migrated to/used by another Application?
If yes : what Application ?

Data subjects' right to have access to their data: how do you inform the Data Subjects about their right to access ?

Is there any third party (within AM or outside of AM) involved in the process?

If yes: for what purpose (e.g. hosting…)?

Has the Application been notified (when applicable)?

What security measures are in place?

Last updated version of this Questionnaire : http://www.....arcelormittal Intranet

SCHEDULE VIII

DESCRIPTION OF THE TRANSFERS

Categories of Data

HR Data include:
- Identification data
- Electronic identification data
- Banking and financial data
- Physical data
- Evaluation test results / assessment of profiles for career management
- Household composition
- Leisure and interests
- Affiliations and member situations
- Housing characteristics (e.g. when providing housing to certain senior executives)
- Education, training and qualifications
- Profession and job
- Image and photo
- Sounds
- Salaries
- Professional Review
- Security
- Log data and traffic data
- Videos

Business Data includes, relating to Customers, Suppliers and business partners of all kinds:
- Identification data
- Electronic identification data
- Banking and financial data
- Education, training and qualifications
- Profession and job
- Image and photo
- Security
- Log data and traffic data
- Videos

IT Data include:
- Identification data
- Electronic identification data
- Banking and financial data
- Profession and job
- Image and photo
- Sounds
- Salaries
- Security
- Log data and traffic data
- Videos

Corporate Responsibility Data include:
- Identification data
- Electronic identification data
- Banking and financial data
- Evaluation test results / assessment of profiles for career management
- Household composition
- Leisure and interests
- Affiliations and member situations
- Housing characteristics (e.g. when providing housing to certain senior executives)
- Education, training and qualifications
- Profession and job
- Image and photo
- Sounds
- Salaries
- Professional Review
- Security
- Log data and traffic data
- Videos

Health and Safety Data include:
- Identification data
- Electronic identification data
- Physical data
- Life and consumption habits
- Household composition
- Leisure and interests
- Affiliations and member situations
- Housing characteristics (e.g. when providing housing to certain senior executives)
- Education, training and qualifications
- Profession and job
- Image and photo
- Sounds
- Security
- Log data and traffic data
- Videos

Data Subjects

A majority of Data Subjects whose data are processed are ArcelorMittal employees and external consultants.

Apart from ArcelorMittal employees, Data Subjects whose data are processed by ArcelorMittal are:
. Customers as well as their representatives, employees or related individuals (such as contacts within the company)

. Vendors and business partners representatives, employees or related individuals (such as contacts within the company)
. Contractors working on behalf of ArcelorMittal
. local stakeholders representatives, employees or related individuals (such as contacts within the company)

HR Data

Purposes of the transfer/processing

Human Resources and Personnel Management, including all processing purposes necessary for the performance of an employment contract or an employment related contract with the employee (or to take necessary steps at the request of a prospective employee prior to entering into a contract) and for complying with applicable legal requirements, management and administration of recruiting and outplacement, delivering pay, tax issues, travel and expenses, managing careers and skills, training (including e-learning), administering employee compensation and benefits, assessing employees' performance, populating employee directories and employee communications.

Organizational analysis and development and management reporting. Activities such as conducting employee surveys, managing mergers, acquisitions and divestitures, scheduling work, recording time, and processing employee data for management reporting and analysis.

Business Data

Purposes of the transfer/processing

Business Process Execution and Management, including sales activities, purchasing activities, finance, accounting and controlling, management of companies' assets, conducting internal audits and investigations, implementing business controls, provision of central processing facilities for efficiency purposes, managing mergers, acquisitions and divestitures and processing personal data for management reporting and analysis, complying with applicable legal requirements.

Relationship management and marketing for commercial activities includes processing necessary for the development and improvement of ArcelorMittal products or services, account management, client service and the performance of (targeted) marketing activities to establish a relationship with a client or maintaining as well as extending a relationship with a client, business partner or supplier and for performing analyses with respect to personal data for statistical and scientific purposes.

Product development, research and improvement of ArcelorMittal products or services. Processing that is necessary for the development and improvement of ArcelorMittal products or services, research and development.

Performing of agreements with clients, business partners and suppliers including notably communication with individuals and other parties involved in contracts and responding to requests for (further) information for clients, business partners or suppliers, dispute resolution and development.

IT infrastructures Management, including e-mail, access to the ArcelorMittal Intranet and IT Infrastructure (include its software), maintenance of ArcelorMittal's IT Infrastructure, development and use of software, IT training, use of collaborative tools, and more generally user access management of IT applications.

Corporate Responsibility Data

Purposes of the transfer/processing

Corporate Responsibility, including having an understanding of our operating environment and stakeholders' concerns, managing ArcelorMittal ongoing programme of engagement towards local communities.

Health and Security Data

Purposes of the transfer/processing

: Health/security processes are activities to ensure the safety and protection of ArcelorMittal's workers and resources as well as ArcelorMittal clients, suppliers, business partners assets and the authentication of client, suppliers or business partners status and access rights. Examples include:
- protecting occupational health and safety and authenticating worker status to authorize access to ArcelorMittal's resources and facilities; and
- protecting the vital interests of Data Subjects. Where processing is necessary to protect the vital interests of an individual, e.g. for urgent medical reasons.

Data recipients located in third countries

Other than the Subsidiaries cited in Schedule X, the data recipients located in third countries include all external service providers that provide services for ArcelorMittal to achieve the purposes described above, such as:

- HR services providers
- Corporate services providers
- IT services providers
- Accounting services providers
- Marketing services providers
- Security services providers

- Sales services providers

SCHEDULE IX

NB : For security reason, this SCHEDULE IX will be left blank in the version made public, outside of ArcelorMittal. This SCHEDULE IX will be included in the copy of the Procedure posted on the Intranet.

DATA PROTECTION COMMITTEE

The Group Compliance and Data Protection Officer is:
. Henk Scheffer

The initial members of the Data Protection Committee designated by Group CIO are
. Herve Legrand

The initial members of the Data Protection Committee designated by EVP Human Resource are
. Bart Wille

The initial secretary is: Korinna Nagy

Data Subjects can contact the Data Protection Committee.at dataprotection@arcelormittal.com.

This email address is also indicated in the standard contractual clauses signed with Vendors, as set out under Schedule V.

SCHEDULE X

NB : For security reason, this SCHEDULE X will be left blank in the version made public, outside of ArcelorMittal. This SCHEDULE X will be included in the copy of the Procedure posted on the Intranet.

GROUP STRUCTURE AND CONTACT DETAILS