


ArcelorMittal IT Department AM_IT_PR_004.00	ArcelorMittal Data Protection Procedure	 ArcelorMittal
--	--	---

Document Information

Short description: Practical and legal measures in order to protect Personal Data handled under ArcelorMittal responsibility.

Scope: See Article 2

Business Owners: Emmanuel CAUVIN Writer (prepared by): Emmanuel CAUVIN	Creation date (first version): 18/04/2013 Review date (new version): Not applicable
Reviewed by : Not applicable	Implementation Date: See Data Protection Compliance Program

Version History

Version	Date	Person	Description
1.0	18/04/2013	Emmanuel CAUVIN	Creation

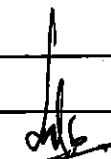
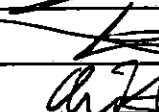


Reference Documents

Reference or date	Title
1 0	/Initial Version

Validation

Validated by	Position	Approval date	Signature
25 Data Protection Authorities (EU), with the Luxembourg Data Protection Authority acting as "leading Authority".	/	1 Feb 2013	http://www.cnpd.public.lu/fr/actualites/national/2013/02/bcr-arcelormittal/index.html

Approval

Approved by	Position	Validation Date	Signature
Davinder Chugh	Senior EVP	30 May 13	
Simon Evans	Group General Counsel	30 May 2013	
Christophe JUNG	Compliance Programme Officer	29 May 2013	
Emmanuel CAUVIN	Data Protection Officer	6 June 2013	

ArcelorMittal IT Department AM_IT_PR_004.00	ArcelorMittal Data Protection Procedure	 ArcelorMittal
--	--	---


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 this 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

Article 1 - Status of the Procedure	Page 4
Article 2 - Scope of the Procedure	Page 5
Article 3 - Principles for processing Personal Data	Page 5
Article 4 - Security and confidentiality	Page 7
Article 5 - Rights of Data Subjects	Page 8
Article 6 - Data Transfers	Page 9
Article 7 - Implementation of this Procedure and enforcement mechanisms	Page 11
Article 8 - Liability	Page 15

Schedule I – Principles for processing Personal Data (checklist)
Schedule II – Rules for setting up a new Information System
Schedule III – ArcelorMittal IT Baseline Security Controls
Schedule IV – Security Assessment Questionnaire
Schedule V – ArcelorMittal Standard Contractual Clause for external Processors
Schedule VI – Data Protection Correspondents & ITCS
Schedule VII – Audit Checklist
Schedule VIII – Description of the transfers
Schedule IX – Data Protection Committee

ArcelorMittal IT Department AM_IT_PR_004.00	ArcelorMittal Data Protection Procedure	 ArcelorMittal
--	--	---

Definitions

Subsidiary

"Subsidiary" means any company or legal entity fully consolidated and controlled by ArcelorMittal SA, registered with the Company and Trade Register of Luxembourg under n°B. 82 454.

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 by an Subsidiary 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;

Special Categories of Data ("Special Data")

"Special Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.

HR Data

"HR Data" means any Personal Data relating to employees, candidates, trainees, temporary workers or retirees of any ArcelorMittal Subsidiary.

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

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.

ArcelorMittal Processor


"ArcelorMittal Processor" means a Processor that is an ArcelorMittal Subsidiary.

Europe ("EU")

Europe means the 27 member states of the European Union as at November 2010 + the 3 members of the EEA:

Iceland

Liechtenstein

ArcelorMittal IT Department AM_IT_PR_004.00	ArcelorMittal Data Protection Procedure	 ArcelorMittal
--	--	---

Norway
 Austria
 Belgium
 Bulgaria
 Cyprus
 Czech Republic
 Denmark
 Estonia
 Finland
 France
 Germany
 Greece
 Hungary
 Ireland
 Italy
 Latvia
 Lithuania
 Luxembourg
 Malta
 Netherlands
 Poland
 Portugal
 Romania
 Slovakia
 Slovenia
 Spain
 Sweden
 United Kingdom

Data Exporter

"Data Exporter" means any Subsidiary located in Europe processing Personal Data in Europe, such Personal Data being further transferred or made available to an Subsidiary outside of Europe.

Data Importer

"Data Importer" means any Subsidiary located outside of Europe processing Personal Data, such Personal Data having being transferred or made available by a Subsidiary located in Europe.


The terms in this Procedure shall be interpreted in accordance with the EU Directives 95/46/EC and 2002/58/EC.

Article 1 - Status of the Procedure

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

All directors, officers and employees of ArcelorMittal and its Subsidiaries worldwide 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.

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

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".

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 covers:

- (i) any and all Personal Data processed in the EU by or on behalf of ArcelorMittal, including employees, customers and suppliers' Personal Data
- and
- (ii) any and all Personal Data processed in the EU by or on behalf of ArcelorMittal, and further transferred or made available outside of the EU, including employees, customers and suppliers' Personal Data.

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 identifiable.

This Procedure does not cover data processed ab initio locally outside of the EU by a Subsidiary, and not further transferred, neither in whole nor in part, to an EU member country. Such Personal Data shall be processed in accordance with local law applicable at the place where the Personal Data are processed.

Current in-scope processes are further described in Schedule VIII 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 Data Subject has unambiguously given his consent; or
- 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 controller is subject; or
 - The processing is necessary in order to protect the vital interests of the Data Subject; 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 controller or in a third party to whom the data are disclosed. Personal Data may also be processed (i) if any ArcelorMittal Subsidiary is required to do so by law or legal process (ii) to 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 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 controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the Data Subject.

3.2. Rules for processing Personal Data

Personal Data will be processed fairly and lawfully.

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 to and not excessive for the purposes for which they are collected and used.

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.

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.

Special Categories of Data will be provided with additional safeguards as provided by Article 9 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 except if:

- The Data Subject has given his explicit consent to the processing of those Special Data, except where the applicable laws prohibit it; or

ArcelorMittal IT Department AM_IT_PR_004.00	ArcelorMittal Data Protection Procedure	 ArcelorMittal
--	--	---

- The processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law (e.g. anti-discrimination) in so far as it is authorized by national law providing for adequate safeguards; 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 (such like the ArcelorMittal 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 sensitive data is necessary for the establishment, exercise or defence of legal claims; or
- The processing of the sensitive data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those sensitive 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, destruction, or damage to data, as described in more detail on 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.

ArcelorMittal IT Baseline Security Controls will be updated by the Data Protection Committee, 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", See Schedule VI).

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

4.2. Security breaches

The Data Protection Correspondent and/or the ITCS 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.

The concerned ArcelorMittal Subsidiary(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 Subsidiary(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 then be documented by the Data Protection Committee in order to share the lesson learned and modify the ArcelorMittal IT Baseline Security Controls accordingly (if necessary).

Article 5 - Rights of Data Subjects

5.1. Data Controller

Each ArcelorMittal Subsidiary will be responsible for its compliance with this Procedure.

Each ArcelorMittal 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

This Procedure shall be made readily available to every Data Subject. A copy shall be made available upon request, either on paper or by way of an electronic tool.

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

Before their data is processed Data Subjects will be given the following information:

- The identity of the controller(s) and of his representative, if any,
- The purposes of the processing for which the data are intended,
- Any further information such as:
 - i) the recipients or categories of recipients of the data,
 - ii) the existence of the right of access to and the right to rectify the data concerning him.

Where the data have not been obtained from the Data Subject, the obligation to inform the Data Subject does not apply if the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law.

5.3. Rights of access, rectification, erasure and blocking of data

Every Data Subject has the right to obtain without constraint at reasonable intervals and without excessive delay or expense a copy of all data relating to them that are processed.

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

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

Every Data Subject has the right to obtain the rectification, erasure or blocking of data in particular because the data are incomplete or inaccurate.

Every Data Subject has the right to object, at any time on compelling legitimate grounds relating to their particular situation, to the processing of their Personal Data, unless that processing is required by law. Where the objection is justified, 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.

The Data Subjects can get access to their Personal Data by submitting a request to the concerned Controller. The Controller may disregard requests that are manifestly unreasonable.

5.4. Automated individual decisions

No evaluation of or decision about the Data Subject which significantly effects them will be based solely on automated processing of their data unless that decision:

- is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the Data Subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
- is authorized by a law which also lays down measures to safeguard the Data Subject's legitimate interests.

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 Subsidiary 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.

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

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

Golden Rule #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.

Golden Rule #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 Subsidiary concerned and the Processor, when applicable.

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

The Security Assessment described in this Section 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.

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

→ Step 1: Security Assessment

The concerned ArcelorMittal Subsidiary 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).

When doing this evaluation, the IT Compliance & Security Officer shall be given by the ArcelorMittal Subsidiary the opportunity to discuss with the Vendor, suggest improvement to Vendor's security measures and inspect its systems 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 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, such response shall be included in the contract signed between the ArcelorMittal Subsidiary and the vendor. The response shall become an integral part of the contract.


The contract signed between the ArcelorMittal Subsidiary concerned and the external Processor shall also 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 conflicting with 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 Subsidiary concerned and the Processor, when applicable.

6.2. Data Transfers to an ArcelorMittal Processor

Any ArcelorMittal Processor must comply with ArcelorMittal IT Baseline Security Controls.

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

ArcelorMittal IT Department AM_IT_PR_004.00	ArcelorMittal Data Protection Procedure	 ArcelorMittal
--	--	---

The purpose for which the Personal Data shall be processed by the ArcelorMittal Processor on behalf of its customer shall be mutually agreed in written between ArcelorMittal Processor and its ArcelorMittal customer. 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 customer.

When sub-contracting part of all of the services to an External Processor, ArcelorMittal Processor shall comply with the process described in Section 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 the EU must respect the European rules on transborder data flows (Articles 25-26 of Directive 95/46/EC: for instance making use of the EU Standard Contractual Clauses approved by the EU Commission 2001/497/EC or 2004/915/EC or by other adequate contractual means according to Articles 25 and 26 of the EU Directive).

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)
- 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)

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.

The Data Protection Correspondent will also act as key contact person for any complain arising in his/her scope as described in Section 7.4 of this Procedure ("Internal Complaint Mechanism") and for any Security Breach as described in Section 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 Data Controllers in different countries/segments.

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

The Data Protection Correspondent will keep the Data Protection Committee constantly informed about any complain 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 Section 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 three (3) core members,

- . 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 General Counsel.

The initial 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.

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 General Counsel 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.

ArcelorMittal IT Department AM_IT_PR_004.00	ArcelorMittal Data Protection Procedure	 ArcelorMittal
--	--	---

The Data Protection Committee shall:

- (i) maintain and update the list of ArcelorMittal Subsidiaries bound by this Procedure,
- (ii) 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),
- (iii) oversee the implementation of this Procedure and the performance of the Subsidiaries, including future ArcelorMittal Subsidiaries,
- (iv) resolve any major issues / problems that may arise,
- (v) initiate, validate and update specific policies for Global Tools (no such policy shall be enforceable without Data Protection Committee's prior approval),
- (vi) update Schedule II and Schedule III, IV, V, VI, VII and VIII, 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. As an example, it is expected that the standard clause for external services providers in Schedule V may need to be adapted to national laws and to any evolution thereof, on a country-by-country basis.
- (vii) 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 to the ArcelorMittal 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.
- (viii) ensure that changes of this core document and changes to the list of ArcelorMittal Subsidiaries bound by this Procedure are notified to the Data Protection Authorities granting the authorizations with a brief explanation of the reasons justifying the changes.
- (ix) Keep track of all versions of this Procedure

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 Data Controller is not complying with this Procedure.

The Data Protection Correspondent of the concerned ArcelorMittal Data Controller will be responsible for handling such complaint in a timely manner. A first feedback will be communicated to the claimant within one (1) month following the complaint. The Data Protection Correspondant will then use its best efforts to handle the complaint in a timely manner, taking the complexity and the scope of the complaint into account. It is expected that the investigation period will last between one (1) and six (6) months, except in case of unusual and exceptional circumstances.

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

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

The Data Subject may at any time lodge a claim to the competent Data Protection Authority or file a suit before the jurisdiction of the Data Exporter located in the EU.

7.5 Audit Plan

The group's 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 twice 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 cover all aspects of this Procedure, both inside Europe and outside Europe.

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 General Counsel (iv) to the management of the concerned Subsidiary(s).

Data Protection Authorities can have access to the reports of the audit upon request.


The Audit reports shall not be communicated in any manner to any body or person not mentioned in this Section 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 Section 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 him prevents the Data Controller from fulfilling its obligations under this Procedure and has substantial effect on the guarantees provided by this Procedure, he 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).

<p>ArcelorMittal IT Department AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
--	---	---

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.

Article 8 - Liability

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

Each ArcelorMittal Subsidiary accepts responsibility for any breach of this Procedure, notwithstanding the joint liability mechanism specified in article 8.2 for violation.

The Data Subject may at any time lodge a claim to the competent Data Protection Authority or file a suit before the jurisdiction of the Data Exporter located in the EU, as provided in Section 7.4.

These rights do not extend to those elements of this Procedure pertaining to internal mechanisms implemented within Subsidiaries 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 ArcelorMittal Subsidiary is in breach of this Procedure, such breaching ArcelorMittal 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

In addition, any Data Subject who has suffered damage as a result of any violation of the eight (8) above-listed Data Subject's rights is entitled to receive compensation for the damage suffered.

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

In the event the breaching Subsidiary is not located in Europe, the following rules shall apply:

- Such breaching Subsidiary and the Data Exporter shall be jointly and severally liable for damage to the Data Subject resulting from any violation of the provisions of this Procedure.
- The breaching Subsidiary shall indemnify the Data Exporter for any cost, charge, damages, expenses or loss it has incurred.
- In the event the Data Exporter can prove that the member outside Europe is not liable for the violation, it may discharge itself from any responsibility.

<p>ArcelorMittal IT Department AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
--	---	---

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?
- Do I need to notify the Data Protection Authority and if so is my notification up to date?

"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 Directive 95/46/EC"

- 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?

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

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.

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

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal</p> <p>Data Protection</p> <p>Procedure</p>	 <p>ArcelorMittal</p>
---	---	--

SCHEDULE III

IT BASELINE SECURITY CONTROLS


Last updated version of the Policies : <http://www.....> Arcelormittal Intranet

ArcelorMittal IT Department AM_IT_PR_004.00	ArcelorMittal Data Protection Procedure	 ArcelorMittal
--	--	---

SCHEDULE IV

SECURITY ASSESSMENT QUESTIONNAIRE ("SAQ")

Last updated version of the Questionnaire : <http://www.....> Arcelormittal Intranet

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal</p> <p>Data Protection</p> <p>Procedure</p>	 <p>ArcelorMittal</p>
---	---	--

SCHEDULE V

ArcelorMittal Standard Contractual Clause for external Processors

This clause must be included and is **MANDATORY** in all contracts between an ArcelorMittal Subsidiary acting as Data Controller and an external 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 external 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 data to be transferred or made available to the Processor.

This Schedule also includes a specific version for Germany (See below).

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.

[ArcelorMittal is and will remain the Data Controller and the Vendor will solely act as Data Processor with respect to Personal Data] ()*. Vendor shall not process any Personal Data (including Personal Data originally processed by ArcelorMittal), unless it is acting to provide the services described in this Agreement. Vendor shall use its best efforts to ensure the reliability of any of Vendor's staff who have access to or are responsible for the processing of Personal Data.. 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 relevant 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. ArcelorMittal may as a condition of providing its consent to any proposed sub-processing require Vendor to 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).

<p>ArcelorMittal IT Department AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

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 relevant laws relating to data protection.

When applicable under European Directive 95/46, 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 Directive 95/46/EC, and the Vendor shall abide by them.

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.

In addition, 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 a description of all measures already taken and to be taken by Vendor in order to cure the breach or suspected breach.

Vendor shall fully assist ArcelorMittal with responding to any Data Subject's request to access to 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.

Comments:


In the above contractual provision, "Vendor" designates the Processor and "ArcelorMittal" designates the concerned ArcelorMittal Subsidiary. 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 external Processor.

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

(*) This *[provision]* must be included only if the ArcelorMittal legal entity signing the agreement is located in Europe. This provision is valid only under European laws.

(**) 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](http://www.....arcelormittal.com) Intranet

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
--	---	---

GERMANY

This is a specific version for Germany

Auftragsdatenverarbeitungsvertrag	Agreement on Data Processing Agency
<p>1. Anwendungsbereich</p> <p>Im Rahmen der Leistungserbringung nach dem Vertrag vom ... [Datum] (nachfolgend „Rahmenvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers oder sonstiger Dritter (nachfolgend „AM-Daten“ genannt) erhält. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien bei der Durchführung des Rahmenvertrages.</p>	<p>2. Scope of Application</p> <p>Rendering the services pursuant to the Framework Contract dating from ... including its annexes (hereinafter consistently referred to as "Framework Contract"), it is required that the Agent has access to personal data of the Principal or of other third persons (hereinafter consistently referred to as "AM Data"). This contract shall clearly define privacy data protection law related rights and duties of the parties when executing the Framework Contract.</p>
<p>2. Auftragsdatenverarbeitung</p> <p>2.1 Der Auftragnehmer erhebt, verarbeitet und/oder nutzt die AM-Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von § 11 BDSG (Auftragsdatenverarbeitung). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle („Herr der Daten“) und ist für die Rechtmäßigkeit der auftragsgemäßen Erhebung, Verarbeitung und/oder Nutzung der AM--Daten verantwortlich.</p> <p>2.2 Die Erhebung, Verarbeitung und/oder Nutzung der AM--Daten hat ausschließlich und vollständig innerhalb der Bundesrepublik Deutschland (BRD) und in der/dem in Anlage 1 dieses Vertrages abschließend festgelegten Art, Umfang und Zweck zu erfolgen. Die Erhebung, Verarbeitung und/oder Nutzung der AM--Daten umfasst die in Anlage 1 dieses Vertrages abschließend festgelegte Art der AM--Daten und den dort festgelegten Kreis der Betroffenen.</p> <p>2.3 Der Auftragnehmer erwirbt an den AM--Daten keine Rechte und ist auf Verlangen des Auftraggebers jederzeit zur Herausgabe der AM--Daten verpflichtet. Zurückbehaltungsrechte in Bezug auf die AM- sind ausgeschlossen.</p> <p>2.4 Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf Anfrage zeitnah die für die Erstellung des eigenen Verzeichnisses gemäß § 4g Abs. 2 BDSG (Internes Verzeichnisses des Auftraggebers) erforderlichen Angaben zu machen,.</p>	<p>2. Commissioned Data Processing</p> <p>2.1 The Agent shall collect, process and/or use the AM Data exclusively in the name and in accordance with the instructions of the Principal in terms of Sec. 11 of the German Federal Data Protection Act (Commissioned Data Processing). The Principal remains the responsible entity in terms of data protection ("data controller") and is responsible for the legality of collecting, processing and/or using the AM Data as instructed.</p> <p>2.2 The collection, processing and/or use of AM Data shall exclusively and entirely occur within the Federal Republic of Germany (FRG) and in the type, extent and purpose exclusively defined in Annex 1 to this contract. The collection, processing and/or use of AM Data comprise the type of AM Data and the circle of affected persons exclusively defined in Annex 1 to this contract.</p> <p>2.3 The Agent shall not acquire any rights with respect to the AM Data and shall be obliged to return the AM Data at any time on the request of the Principal. Rights of retention in relation to the AM Data are excluded.</p> <p>2.4 The Agent shall, upon request of the Principal and in a timely manner, give full particulars to the Principal to the extent such particulars are required for creating or updating the Principal's internal overview of processing personal data (Sec. 4 lit. g para. 2 of the Federal Data Protection Act).</p>

ArcelorMittal Data Protection Procedure



2.5 Der Auftragnehmer ist verpflichtet, einen betrieblichen Datenschutzbeauftragten schriftlich zu bestellen, soweit er in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 4f Abs. 1 Satz 1 bis 4 BDSG).

2.5 In case the Agent generally deploys at least ten (10) persons to carry out the automated processing of personal data, the Agent shall be obliged to appoint a data protection official in writing (Sec. 4 lit. f para. 1 s. 1- 4 Federal Data Protection Act).

3. Weisungen des Auftraggebers

3.1 Der Auftragnehmer verwendet die vom Auftraggeber übermittelten AM-Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers und der in diesem Vertrag enthaltenen Bestimmungen. Der Auftraggeber behält sich insoweit gegenüber dem Auftragnehmer ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung und -nutzung vor.

3.2 Die Weisungen des Auftraggebers erfolgen in der Regel schriftlich oder in Textform. In Ausnahmefällen können Weisungen auch mündlich erteilt werden. Mündlich erteilte Weisungen bedürfen jedoch einer unverzüglichen schriftlichen Bestätigung durch den in Ziffer 3.3 genannten Weisungsberechtigten des Auftraggebers.

3.3 Weisungen dürfen nur von dem Weisungsberechtigten des Auftraggebers oder dessen Stellvertreter erteilt werden. Die Parteien vereinbaren als Weisungsberechtigten des Auftraggebers folgende Person:

Weisungsberechtigter:

Stellvertreter:

3.4 Ein Wechsel in der Person des Weisungsberechtigten oder seines Stellvertreters oder deren dauerhafte Verhinderung ist der anderen Partei unverzüglich schriftlich unter Benennung eines Vertreters mitzuteilen.

3.5 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, hat er

3. Instructions by the Principal

3.1 As regards the use of AM Data, the Agent shall be obliged to fully comply with the instructions arising from the Framework Contract and with the instructions issued by the Principal. The Principal reserves the right to instruct the Agent regarding manner, extent and practice of data processing and data usage.

3.2 Instructions issued in individual cases shall be issued in writing or by email. In substantiated and individual cases, instructions may as well be issued orally; however, the Principal shall subsequently confirm such instructions in writing or by email and in a timely manner by the authorized person as per Clause 3.3 of this contract.


3.3 Instructions may only be issued by persons authorized to issue instructions and their representatives. The parties agree upon the following persons who will give instructions on behalf of the Principal :

Persons Authorized to Issue Instructions:


Representative:

3.4 The parties shall inform the respective other party immediately in writing if the responsible persons are changed or hindered. They will name a substitute.


3.5 If the Agent is of the opinion that an instruction violates any statutory regulation and/or a provision of the Framework Contract, the Agent shall be obliged to inform the Principal accordingly and without any

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
--	---	---

<p>den Auftraggeber unverzüglich darauf hinzuweisen. Außerdem ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.</p>	<p>undue delay. The Agent shall be entitled to refrain from the execution of such instruction unless the Principal confirms its instruction.</p>
<p>4. Pflichten des Auftraggebers</p> <p>4.1 Der Auftraggeber ist für die rechtliche Zulässigkeit der Erhebung, Verarbeitung und Nutzung der AM--Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich.</p> <p>4.2 Der Auftraggeber ist Eigentümer der AM--Daten und Inhaber aller etwaigen Rechte, die die AM--Daten betreffen.</p>	<p>4. Obligations of the Principal</p> <p>4.1 The Agent acknowledges that the Principal remains responsible for the legality of the processing of AM Data and that the Principal is solely responsible for the protection of the Data subject's rights pursuant to the Data Protection Rules.</p> <p>4.2 The Principal is the owner of the AM Data and holds all rights in relation to the AM Data.</p>
<p>5. Pflichten des Auftragnehmers</p> <p>5.1 Der Auftragnehmer stellt sicher, dass die Datenverarbeitung und -nutzung im Rahmen der Leistungserbringung nach dem Rahmenvertrag in Übereinstimmung mit den geltenden datenschutzrechtlichen Bestimmungen, insbesondere mit den Bestimmungen des BDSG, mit den Weisungen des Auftraggebers, mit den Bestimmungen des Rahmenvertrages sowie dieses Vertrages erfolgt.</p> <p>5.2 Der Auftragnehmer stellt sicher, dass die AM--Daten getrennt von anderen personenbezogenen Daten (insbesondere für andere Auftraggeber verarbeitete personenbezogenen Daten) gespeichert und verarbeitet werden.</p> <p>5.3 Der Auftragnehmer darf ohne vorherige schriftliche Zustimmung durch den Auftraggeber keine Kopien oder Duplikate der AM--Daten anfertigen. Hiervon ausgenommen sind lediglich Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Rahmenvertrag erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.</p> <p>5.4 Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden vom Auftragnehmer besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Eingang und Ausgang werden dokumentiert.</p>	<p>5. Obligations of the Agent</p> <p>5.1 The Processor undertakes to process and use the AM Data in compliance with the Framework Contract in accordance with applicable Data Protection Rules (especially those of the BDSG) and in compliance with the instructions of the Principal and the provisions of this Agreement.</p> <p>5.2 The Agent agrees and warrants that the AM Data will be saved and processed separately from other Data stored on its servers (especially personal data processed for other principals).</p> <p>5.3 The Processor is not allowed to make copies or duplicates of the AM Data without the prior written consent of the Controller, unless such copies or duplicates are necessary or customary to guarantee proper processing of data in accordance with the provisions of the Framework Contract or for the fulfilment of statutory data retention provisions.</p> <p>5.4 The Agent shall specially mark all media that belong to the Principal or are used on behalf of the Principal. Incoming and outgoing media are subject to constant control that shall be documented.</p>

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 ArcelorMittal
--	---	--

<p>5.5 Der Auftragnehmer ist verpflichtet, AM--Daten auf Weisung des Auftraggebers unverzüglich zu berichtigen, zu löschen oder zu sperren (§ 35 BDSG).</p> <p>5.6 Der Auftragnehmer hat dem Auftraggeber auf Anforderung unverzüglich eine Übersicht über die in § 4e S. 1 BDSG genannten Angaben sowie über die zugriffsberechtigten Personen zur Verfügung zu stellen (§ 4g Abs. 2 S. 1 BDSG).</p> <p>5.7 Der Auftragnehmer ist verpflichtet, auf Anfrage des Auftraggebers Änderungen der Bestimmungen in Anlage 1 dieses Vertrages zuzustimmen, soweit er keinen sachlichen Grund zur Verweigerung dieser Zustimmung hat.</p>	<p>5.5 The Agent shall be obliged to correct, erase and/or block the AM Data on the Principal's instruction without any undue delay (Sec. 35 of the Federal Data Protection Act).</p> <p>5.6 The Agent shall, upon request of the Principal be obliged to provide the Principal with a summary of the details enumerated in Sec. 4 lit. e cl. 2 of the Federal Data Protection Act and the persons having access to this data (Sect. 4 lit. g para. 2 s. 1 Federal Data Protection Act) without any undue delay.</p> <p>5.7 On the Principal's request, the Agent shall be obliged to consent to modifications of provisions in Annex 1 to this agreement if and to the extent to which the Agent does not have a factual reason to refuse such consent.</p>
<p>6. Datengeheimnis</p> <p>Der Auftragnehmer hat sämtliche bei der Verarbeitung von AM--Daten beschäftigten Personen gemäß § 5 BDSG schriftlich auf das Datengeheimnis zu verpflichten. Der Auftragnehmer hat weiterhin seine Mitarbeiter zu verpflichten, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und diese Verpflichtung der Mitarbeiter schriftlich zu dokumentieren. Der Auftragnehmer muss dem Auftraggeber auf Anfrage einen geeigneten Nachweis über die Einhaltung dieser Bestimmung liefern.</p>	<p>6. Data Secrecy</p> <p>The Agent shall be obliged to commit the persons employed in collecting, processing and/or using AM Data in written form to data secrecy according to Sect. 5 Federal Data Protection Act. The Agent shall also commit its employees to comply with statutory data protection provisions in written form that has to be kept in records. Upon request of the Principal the Agent has the duty to provide sufficient proof that these obligations are fulfilled.</p>
<p>7. Technische und organisatorische Schutzmaßnahmen</p> <p>7.1 Der Auftragnehmer garantiert, innerhalb und im Rahmen des ihm nach diesem Vertrag zugewiesenen Verantwortungsbereichs diejenigen technischen und organisatorischen Maßnahmen zu treffen und aufrecht zu erhalten, die erforderlich sind, um die Einhaltung der Bestimmungen dieses Vertrages sowie der anwendbaren gesetzlichen Datenschutzvorschriften sicherzustellen. Der Auftragnehmer verpflichtet sich vor Verarbeitung der AM--Daten insbesondere – vorbehaltlich weiterer Anweisungen des Auftraggebers – zur Implementierung der in den Baseline Security Control Measures von AM dieses Vertrages aufgelisteten technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und dem Anhang zu § 9 BDSG. Diese technischen und organisatorischen Maßnahmen können technologischen Weiterentwicklungen angepasst werden. Sämtliche</p>	<p>7. Technical and organizational measures</p> <p>7.1 The Agent guarantees to take the technical and organizational measures - within the Agent's scope and framework of responsibility allotted by the Framework Contract - that are necessary to ensure that the data protection provisions, in particular the provisions of this contract and statutory provisions are complied with. In the framework of the automated processing of AM Data, the Agent guarantees subject to further instructions of the principal to particularly take the technical and organizational measures listed in the Baseline Security Control Measures of AM to this agreement ensuring the fulfilment of the requirements of Sec. 9 of the Federal Data Protection Act jointly with the requirements of the appendix to Sec. 9 first sentence of the Federal Data Protection Act. These technical and organizational measures may be adjusted to technological developments. Any</p>

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

<p>Anpassungen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers.</p> <p>7.2 Im Falle von Abweichungen oder vermuteten Abweichungen von den in vorstehender Ziffer 7.1 enthaltenen Verpflichtungen, wie insbesondere bei jeglichem Verstoß gegen datenschutzrechtliche Bestimmungen, bei Störungen, Problemen oder Fehlern in der Datenverarbeitung, bei Verlust, Entwendung oder unrechtmäßiger Übermittlung von AM--Daten an Dritte sowie bei jeder sonstigen unrechtmäßigen Kenntniserlangung von AM--Daten durch Dritte ist der Auftragnehmer verpflichtet, den IT Compliance & Security Officer des Auftraggebers unverzüglich (d.h. innerhalb von 24 Stunden) über das jeweilige Ereignis (einschließlich der Ursachen, den genauen Zeitpunkt sowie das Ausmaß der Abweichung, die bereits ergriffenen und die noch zu ergreifenden Maßnahmen, etc.) schriftlich zu informieren.</p> <p>7.3 Weiterhin ist der Auftragnehmer verpflichtet, bei Geschehnissen im Sinne von Ziffer 7.2 im Benehmen mit dem Auftraggeber unverzüglich sämtliche erforderlichen Maßnahmen einzuleiten, um entstandene Gefährdungen für die Integrität und Vertraulichkeit der AM--Daten zu minimieren und zu beseitigen, die AM--Daten zu sichern und Maßnahmen zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.</p> <p>7.4 Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei auf erstes Anfordern unentgeltlich im Rahmen des Zumutbaren zu unterstützen.</p>	<p>adjustments require the written consent of the Principal.</p> <p>7.2 In cases of any deviation or suspected deviation from the provisions stipulated under clause 7.1, especially any infringement of statutory data protection provisions or failures, problems or malfunctions occurring while processing AM Data or in case of loss, theft or illegal transfer to third parties as well as in case of any other unlawful disclosure to third parties, the Agent shall be, without any undue delay, obliged to inform the IT Compliance & Security Officer of the Principal in writing about the specifics of the respective incident (i.e. in particular about the cause, the precise point in time as well as the extent of the deviation, the already taken and still to be taken measures, etc.) without any undue delay (i.e. within 24 hours).</p> <p>7.3 In cases of incidents in terms of clause 7.2 of this contract the Agent shall, without undue delay, take any measures necessary for excluding and minimizing any potential risk with respect to the integrity and confidentiality of AM Data, to backup AM Data and to mitigate potential harm of the persons affected. The Agent shall be obliged to co-ordinate with the Principal.</p> <p>7.4 Insofar as the Principal has any obligations according to Sect. 42 lit. a Federal Data Protection Act, the Agent shall upon first request by the Principal support the Principal in a reasonable extent free of charge.</p>
<p>8. Kontrollrechte</p> <p>8.1 Der Auftraggeber ist jederzeit berechtigt, die Geschäftsräume des Auftragnehmers zu betreten sowie zeitlich und räumlich uneingeschränkt die technischen und organisatorischen Maßnahmen sowie die Datenverarbeitungsprozesse im Hause des Auftragnehmers zu prüfen, um sich von der Einhaltung der Bestimmungen dieses Vertrages sowie der einschlägigen gesetzlichen Datenschutzbestimmungen zu überzeugen.</p> <p>8.2 Der Auftragnehmer gewährt dem Auftraggeber oder einem von diesem beauftragten Dritten in diesem Rahmen die erforderlichen Zugangs-, Auskunfts- und Einsichts-rechte. Der Auftragnehmer verpflichtet sich insbesondere, dem Auftraggeber oder</p>	<p>8. Right of Control</p> <p>8.1 The Principal shall have the right to accede the business premises of the Agent at any time and unrestricted by time or space in order to inspect the technical and organisational measures and the data processing work flows in the Processor's company and to audit the Agent's compliance with the relevant statutory and contractual data protection provisions.</p> <p>8.2 The Agent grants to the Principal or any third party assigned by the Principal the necessary rights of access, information and inspection required for the respective audit. Therefore the Agent shall grant to the Principal or third parties assigned by the</p>

von diesem beauftragten Dritten Zugang zu den Datenverarbeitungseinrichtungen, Dateien und anderen Dokumenten zu gewähren, um die Kontrolle und Überprüfung der relevanten Datenverarbeitungseinrichtungen, Dateien und anderer Dokumentationen zur Verarbeitung und Nutzung der AM--Daten zu ermöglichen. Der Auftragnehmer stellt dem Auftraggeber oder dem von diesem beauftragten Dritten alle für die Kontrolle notwendigen Informationen zur Verfügung.

8.3 Gemäß den Bestimmungen des BDSG unterliegen der Auftraggeber und der Auftragnehmer öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Anforderung durch den Auftraggeber wird der Auftragnehmer die gewünschten Informationen an die Aufsichtsbehörde liefern und dieser die Möglichkeit zur Prüfung im gleichen Umfang einräumen, wie die Aufsichtsbehörde Prüfungen beim Auftraggeber durchführen darf. Davon umfasst sind Inspektionen beim Auftragnehmer durch die Aufsichtsbehörde oder von ihr benannte Personen. Der Auftragnehmer gewährt der zuständigen Aufsichtsbehörde auch in diesem Rahmen die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

8.4 Im Fall von Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde beim Auftragnehmer nach § 38 BDSG oder im Fall von Ermittlungen der zuständigen Behörde beim Auftragnehmer nach §§ 43, 44 BDSG hat dieser den Auftraggeber darüber unverzüglich zu informieren.

9. Beauftragung Dritter

9.1 Der Auftragnehmer ist ohne vorherige schriftliche Zustimmung des Auftraggebers nicht berechtigt, Dritte mit der Verarbeitung oder Nutzung von AM--Daten zu beauftragen. Für mit dem Auftragnehmer im Sinne von §§ 15 ff. AktG verbundene Unternehmen ist eine solche vorherige Zustimmung nicht erforderlich.

9.2 Zur Prüfung einer solchen Zustimmung - bzw. im Falle eines mit dem Auftragnehmer verbundenen Unternehmens zur Information über eine entsprechende Unterbeauftragung - hat der Auftragnehmer dem Auftraggeber eine Kopie der Vereinbarung zur Auftragsdatenverarbeitung zwischen dem Auftragnehmer und dem Dritten zur Verfügung zu stellen. In dieser Vereinbarung hat der Auftragnehmer den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftragnehmer aufgrund

Principal unimpeded access to all data processing facilities, data files and other documentation to accomplish the inspection and review of all this data processing facilities, data files and other documentation needed for processing AM Data. The Agent provides the Principal or third parties assigned by the Principal with all information necessary for the review.


8.3 The Principal and the Agent may be subject to control by public data protection authorities under the provisions of the Federal Data Protection Act. Upon request of the Principal the Agent shall provide public data protection authorities with all desired information as well as allow inspections to the same extent the public data protection authorities are authorized to inspect the Principal. This comprises inspections on the Agent's premises by public data protection authorities or persons assigned by those. Therefore the Agent shall grant public data protection authorities the necessary rights of access, information and inspection.

8.4 In any case of inspections or measures taken by the data protection authorities according to Sec. 38 Federal Data Protection Act or in case of investigations by the competent data protection authorities according to Sec. 43, 44 Federal Data Protection Act on premises of the Agent, the latter shall inform the Principal without undue delay.

9. Subcontracting to Third Parties

9.1 The Agent shall not be entitled to subcontracting a third party with the processing or use of AM Data unless the Principal has given its prior written consent to such subcontracting. This does not apply to companies associated with the Agent in terms of Sect. 15 et seqq. German Stock Companies Act.

9.2 For the purpose of assessing such consent and accordingly for the purpose of information regarding subcontracting in case of a company associated to the Agent the latter shall provide the Principal with a copy of the contract regarding the subcontracting the commissioned data processing between the Agent and the third party. By virtue of this contract, the Agent shall bind the third party in writing in such way and to the extent the Agent is obliged towards the Principal pursuant to contract. However, the

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
--	---	---

<p>dieses Vertrages gegenüber dem Auftraggeber verpflichtet ist. Ein Anspruch des Auftragnehmers auf Erteilung der Zustimmung (soweit erforderlich) besteht nicht.</p> <p>9.3 Der Auftragnehmer hat die Einhaltung der Verpflichtungen des Dritten regelmäßig (d.h. mindestens einmal jährlich) beim Dritten zu überprüfen und den entsprechenden Prüfbericht dem Auftraggeber nach Abschluss der Prüfung unverzüglich zur Verfügung zu stellen.</p>	<p>Principal shall not be under any obligation (if consent is necessary) to declare such a consent.</p> <p>9.3 The Agent shall regularly (i.e. at least once a year) control whether a subcontracted third party complies with its obligations arising from the contract concluded between the Agent and the third party, and shall provide the Principal with the relevant written inspection report without undue delay after the respective inspection of the subcontractor.</p>
<p>10. Rechte der Betroffenen</p> <p>10.1 Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.</p> <p>10.2 Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Löschung oder Sperrung der ihn betreffenden Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.</p> <p>10.3 Für den Fall, dass eine betroffene Person ihre Rechte auf Berichtigung, Löschung oder Sperrung von AM--Daten sowie auf Auskunft über die gespeicherten AM--Daten, den Zweck der Speicherung und die Personen und Orte, an die AM--Daten regelmäßig übermittelt werden, geltend macht, ist der Auftragnehmer verpflichtet, den Auftraggeber bei der Erfüllung dieser Anforderungen zu unterstützen.</p>	<p>10. Rights of data subjects (persons affected)</p> <p>10.1 Data subjects affected by the data processing may exercise their rights vis-à-vis the Principal only.</p> <p>10.2 As far as data subjects contact the Agent to exercise their rights to information, correction, erasure or blocking of the personal data affecting them, the Agent shall forward those requests to the Principal without undue delay.</p> <p>10.3 In case that a data subject exercises its rights to information, correction, erasure or blocking of AM Data as well as disclosure of stored AM Data, the purpose of storage and the persons and places to which AM data are transferred regularly the Agent is obliged to support the Principal to fulfil those obligations.</p>
<p>11. Auskunft an Dritte</p> <p>11.1 Soweit der Auftragnehmer aufgrund gesetzlicher Bestimmungen Dritten Auskunft über AM--Daten erteilen muss, ist der Auftragnehmer verpflichtet, den Auftraggeber vor Auskunftserteilung über den Empfänger, Zeitpunkt und Inhalt der zu erteilenden Auskunft schriftlich zu informieren.</p> <p>11.2 Im Übrigen darf der Auftragnehmer Auskünfte über AM--Daten an Dritte oder Betroffene nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.</p>	<p>11. Information of Third Persons</p> <p>11.1 If and to the extent the Agent is obliged to provide information concerning AM Data to a third party due to a mandatory statutory provision, the Agent is, prior to the provision of such information, obliged to inform the Principal in writing about the identity of the third party, the point in time and the specific information to be given.</p> <p>11.2 Apart from that case the Agent may provide information about AM Data to third parties only with the prior written consent of the Principal.</p>

12. Löschung von Daten und Rückgabe von Datenträgern

12.1 Der Auftragnehmer hat ihm überlassene und alle ergänzend hinzugewonnenen AM--Daten, Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, vollständig und unwiderruflich zu löschen oder zu vernichten sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, spätestens jedoch nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Rahmenvertrages). Gleiches gilt für Vervielfältigungen der AM--Daten (insbesondere Archivierungs- und Sicherungsdateien) in allen Systemen des Auftragnehmers sowie Test- und Ausschussdaten, Notizen, Mitschriften, Entwürfe und Kopien.

12.2 Das Protokoll über die Löschung bzw. Vernichtung der AM- Daten ist dem Auftraggeber auf Anforderung unverzüglich vorzulegen.

12.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

13. Schlussbestimmungen

Die Dauer der Datenverarbeitung im Auftrag richtet sich nach den Bestimmungen zur Laufzeit des Rahmenvertrags.

Änderungen, Ergänzungen und eine Aufhebung dieses Vertrages bedürfen der Schriftform. Gleiches gilt für eine Änderung des Schriftformerfordernisses. Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der betreffenden unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem wirtschaftlichen Zweck der unwirksamen Regelung am nächsten kommt bzw. diese Lücke ausfüllt.

12. Return and Deletion of Data


12.1 The Agent shall completely and irrevocably erase or destroy all AM Data handed over to the Principal as well as any additionally collected AM Data, data resulting from processing and use as well as data associated to the contract as soon as the knowledge of those data is no longer required for the fulfilment of the purpose of storage, however, at the latest subsequently to the fulfilment of rendering the service(s) covered by the Framework Contract (in particular subsequently to the cancellation or to any other termination of the Framework Contract). This clause also applies for duplication of AM Data (including backups for archiving and security reasons) on any of the Agent's systems as well as test data, junked data, notices, notes, drafts and copies.

12.2 Upon request of the Principal, the Agent shall be obliged to make available to the Principal the protocol over the erasure or deletion of the AM Data without undue delay.

12.3 Documentation required to prove data processing according to contractual and legal provisions shall be retained by the agent after the rendering of this contract for the duration of the particular retention period.

13. Final provisions

The duration of the Commissioned Data Processing shall be dependent on the provisions concerning the duration of the Framework Contract. Alterations, amendments and the termination of this contract shall be made in writing. This also applies for an amendment of this provision. Should a provision of this contract be or become invalid as well as be incomplete, the validity of the other provisions of this Agreement shall remain unaffected hereby. The parties agree that, in the place of the invalid provision, a legally binding provision shall apply which comes closest to what the parties would have agreed if they had taken the partial invalidity or incompleteness into consideration.

<p>ArcelorMittal IT Department AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
--	---	---

Ort, Datum / Place, Date

Ort, Datum / Place, Date


Unterschrift (Auftraggeber)

Unterschrift (Auftragnehmer)

ArcelorMittal IT Department AM_IT_PR_004.00	ArcelorMittal Data Protection Procedure	 ArcelorMittal
---	--	--

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen /
Appendix 1: Purpose, type and extent of data processing, type of data and affected persons

1. Zweck der Datenverarbeitung / Purpose of Data Processing,
2. Art und Umfang der Datenverarbeitung / Type and Extent of Data Processing
3. Art der Daten / Type of Data
4. Kreis der Betroffenen / Affected Individuals

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal</p> <p>Data Protection</p> <p>Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

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

Last updated version of this list : <http://www.....arcelormittal> Intranet

ITCS Officers

Last updated version of this list : <http://www.....arcelormittal> Intranet

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal</p> <p>Data Protection</p> <p>Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

SCHEDULE VII

Audit Questionnaire

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's 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

<p>ArcelorMittal IT Department AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
--	---	---

SCHEDULE VIII

Description of the processing of Data

Categories of Data

HR Data

Business Data

IT Data

Corporate Responsibility Data

Health and Safety Data

Data Subjects

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

Apart from ArcelorMittal employees, Data Subjects whose data are processed by ArcelorMittal are:

- Customers representatives (ArcelorMittal is involved in "B2B" activities with no consumer in its customer portfolio)
- Vendors representatives
- Contractors working on behalf of ArcelorMittal
- Local stakeholders

HR Data

Purposes of the transfer/processing

Human Resources and Personnel Management, including recruiting, delivering pay, managing careers and skills, training (e-learning), administering employee benefits, assessing employees' performance, populating employee directories, complying with applicable legal requirements.

Business Data (Personal Data related to Customers, Suppliers and business partners of all kinds).
The persons are identified as ArcelorMittal's contacts within a company, representing that company.

Purposes of the transfer/processing

Business Process Execution and Management, including sales activities, purchasing activities, accounting and controlling, management of companies' assets, complying with applicable legal requirements.

IT infrastructures Management, including e-mail, access to the ArcelorMittal Intranet, use of collaborative tools, and more generally user access management of IT applications ;

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal Data Protection Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

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. Examples include protecting occupational health and safety and authenticating worker status to authorize access to ArcelorMittal's resources and facilities

<p>ArcelorMittal IT Department</p> <p>AM_IT_PR_004.00</p>	<p>ArcelorMittal</p> <p>Data Protection</p> <p>Procedure</p>	 <p>ArcelorMittal</p>
---	---	---

SCHEDULE IX

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 Committee

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

. [Name 2]

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

. [Name 2]

The initial secretary is: Emmanuel CAUVIN

APPENDICES

- 1) Schedule III – 2011 Baseline IT Security Controls



Schedule III -
Baseline IT Security C

- 2) Schedule IV – AM DPA SAQ



Schedule IV - AM
DPA SAQ 1 0.xls

- 3) Schedule VI – AM Compliance Officers network



Schedule VI - AM
Compliance Officers N

- 4) Schedule VI – ITCS Officers



Schedule VI - ITCS
Officers 10.xls

- 5) Data Protection Signature Form Go



Data Protection
Signature Form Go.doc

---- End of Document ----

