

## **Procédure de Protection des Données d'ArcelorMittal**

Version Finale

Le traitement d'informations se rapportant à des personnes est réglementé dans plusieurs pays où ArcelorMittal est présent. ArcelorMittal reconnaît que les Données à Caractère Personnel doivent être traitées avec prudence, qu'il s'agisse des données de ses employés ou de celles de ses partenaires commerciaux. ArcelorMittal souhaite par conséquent adopter des mesures pratiques et juridiques visant à protéger les Données à Caractère Personnel traitées sous sa responsabilité.

La présente Procédure vise à établir des normes uniformes adéquates et globales en matière de protection des données et à faciliter, à l'échelle du Groupe, les transferts de Données à Caractère Personnel conformément aux exigences juridiques en matière de protection des données.

### **Définitions**

<b>Article 1 – Statut de la Procédure</b>	.....
<b>Article 2 – Champ d'application de la Procédure</b>	.....
<b>Article 3 – Principes de Traitement des Données à Caractère Personnel</b>	.....
<b>Article 4 – Sécurité et confidentialité</b>	.....
<b>Article 5 – Droits des Personnes Concernées</b>	.....
<b>Article 6 – Transfert de Données à un Sous-traitant de données</b>	.....
<b>Article 7 – Mise en œuvre de la présente Procédure et mécanismes d'application</b>	.....
<b>Article 8 – Responsabilité</b>	.....
<b>Article 9 – Catégories Particulières de Données</b>	.....

**Annexe I – Principes de Traitement des Données à Caractère Personnel (liste de contrôle)**

**Annexe II – Procédure de vérification de la Protection des Données avant de terminer la phase de conception d'un projet**

**Annexe III – Contrôles de sécurité informatique de base d'ArcelorMittal**

**Annexe IV – Questionnaire d'Évaluation de Sécurité**

**Annexe V – Clause contractuelle type pour les Sous-traitants extérieurs d'ArcelorMittal**

**Annexe VI – Correspondants à la Protection des Données et Agents chargés de la CSI**

**Annexe VII – Questionnaire d'Audit**

**Annexe VIII – Description du Traitement des données**

**Annexe IX – Comité de Protection des Données**

## **Définitions**

### **Filiale**

« Filiale » désigne toute société ou entité juridique entièrement consolidée et contrôlée par ArcelorMittal SA, immatriculée au Registre de Commerce et des Sociétés du Luxembourg sous le n° B. 82 454.

Le terme « contrôle » désigne la possession, directe ou indirecte, par un ou plusieurs intermédiaires, du pouvoir d'administrer ou de faire administrer la gestion et les politiques d'une société ou d'une entité juridique, par la possession de titres avec droit de vote, par contrat ou de toute autre manière.

### **Données à Caractère Personnel**

« Données à Caractère Personnel » désigne toute information se rapportant à une personne physique identifiée ou identifiable. Une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

### **Personne Concernée**

« Personne Concernée » désigne une personne physique dont les Données à Caractère Personnel sont traitées par une Filiale dans le cadre d'une procédure relevant du champ d'application de la présente Procédure.

### **Traitement**

Le « Traitement » de Données à Caractère Personnel désigne toute opération ou ensemble d'opérations effectuées sur des Données à Caractère Personnel, que ce soit ou non à l'aide de moyens automatisés, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

### **Catégories Particulières de données (« Données Spéciales »)**

« Données Spéciales » désigne les Données à Caractère Personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques ou l'appartenance syndicale ainsi que les données relatives à la santé ou la vie sexuelle.

### **Données RH**

« Données RH » désigne toute Donnée à Caractère Personnel se rapportant aux employés, candidats, stagiaires, travailleurs temporaires ou retraités d'une Filiale d'ArcelorMittal.

### **Outils Globaux/Bases de Données Globales**

« Outils Globaux/Bases de Données Globales » se réfère à tout outil informatique (i) comprenant des Données à Caractère Personnel (ii) non limité à un site, à une Unité Commerciale ou à un segment.

Par exemple

Un SIRH

Responsable de Traitement

« Responsable de Traitement » ou « Contrôleur » désigne la personne physique ou morale qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des Données à Caractère Personnel.

Sous-traitant

« Sous-traitant » désigne une personne morale qui traite les Données à Caractère Personnel pour le compte du Responsable de Traitement. Le terme « Sous-traitant » a la même signification que « Prestataire de Services » tel que communément utilisé au sein d'ArcelorMittal.

Sous-traitant ArcelorMittal

« Sous-traitant ArcelorMittal » désigne un Sous-traitant qui est une Filiale d'ArcelorMittal.

Europe (« UE »)

L'Europe désigne les 27 États membres de l'Union Européenne en novembre 2010 + les 3 membres de l'EEE :

Islande

Liechtenstein

Norvège

Allemagne

Autriche

Belgique

Bulgarie

Chypre

Danemark

Espagne

Estonie

Finlande

France

Grèce

Hongrie

Irlande

Italie

Lettonie

Lituanie

Luxembourg

Malte

Pays Bas

Pologne

Portugal  
République tchèque  
Roumanie  
Royaume-Uni  
Slovaquie  
Slovénie  
Suède

#### Exportateur de données

« Exportateur de données » désigne toute Filiale située en Europe et traitant des Données à Caractère Personnel en Europe, ces Données à Caractère Personnel étant ensuite transférées ou mises à disposition d'une Filiale en dehors de l'Europe.

#### Importateur de données

« Importateur de données » désigne toute Filiale située en dehors de l'Europe traitant des Données à Caractère Personnel, ces Données à Caractère Personnel ayant été transférées ou mises à disposition par une Filiale située en Europe.

Les termes de la présente Procédure seront interprétés conformément aux Directives européennes 95/46/CE et 2002/58/CE.

### **Article 1 – Statut de la Procédure**

La Direction Générale d'ArcelorMittal est globalement responsable de la mise en œuvre de la présente Procédure.

Tous les administrateurs, cadres et employés d'ArcelorMittal et de ses Filiales à travers le monde qui traitent des Données à Caractère Personnel doivent respecter la présente Procédure.

Tout contrevenant à la présente Procédure fera l'objet de mesures disciplinaires, conformément aux lois et politiques locales applicables.

ArcelorMittal reconnaît que certaines lois peuvent prescrire des normes plus strictes que celles décrites dans la présente Procédure. Dans un tel cas, les Filiales d'ArcelorMittal concernées traiteront les Données à Caractère Personnel conformément au droit local applicable du lieu dans lequel les Données à Caractère Personnel sont traitées. Si le droit local applicable prévoit un niveau de protection des Données à Caractère Personnel inférieur à celui établi par la présente Procédure, les prescriptions de la présente Procédure s'appliqueront.

Des politiques de confidentialité spécifiques ont été et seront développées pour régir l'utilisation de certains outils/bases de données particuliers. En cas de contradiction entre la présente Procédure et une politique de confidentialité spécifique, la politique de confidentialité spécifique prévaudra. Les outils et les bases de données qui ne sont pas couverts par une politique de confidentialité spécifique seront uniquement régis par la présente Procédure.

La présente Procédure a été adoptée dans le cadre de la Directive européenne 95/46, en tant que « Règles d'entreprise Contraignantes » d'ArcelorMittal.

Les questions concernant la conformité à la présente Procédure et/ou les politiques de confidentialité spécifiques peuvent être adressées au Correspondant à la Protection des Données compétent (Voir Annexe VI).

La date d'entrée en vigueur de la présente Procédure pour toute Filiale particulière est soumise à la signature du Formulaire de Signature par ladite Filiale.

## **Article 2 – Champ d'application de la Procédure**

La présente Procédure couvre :

(i) toute Donnée à Caractère Personnel traitée dans l'UE par ou pour le compte d'ArcelorMittal, notamment les Données à Caractère Personnel des employés, des clients et des fournisseurs d'ArcelorMittal

et

(ii) toute Donnée à Caractère Personnel traitée dans l'UE par ou pour le compte d'ArcelorMittal et ensuite transférée ou mise à disposition en dehors de l'UE, notamment les Données à Caractère Personnel des employés, des clients et des fournisseurs d'ArcelorMittal.

La présente Procédure couvre toute personne dont les données sont traitées, quelle que soit sa nationalité.

La présente Procédure ne couvre aucune donnée rendue anonyme. Les données sont rendues anonymes si les personnes physiques qui les concernent ne sont plus directement ou indirectement identifiables.

La présente Procédure ne couvre pas les données traitées ab initio localement en dehors de l'UE par une Filiale et qui ne sont pas ensuite transférées, en tout ou partie, vers un pays membre de l'UE. Ces Données à Caractère Personnel seront traitées conformément au droit local applicable dans le lieu dans lequel elles sont traitées.

Les traitements concernés par la Procédure sont décrits plus en détail dans l'Annexe VIII de la présente Procédure.

## **Article 3 – Principes de Traitement des Données à Caractère Personnel**

### 3.1. Critères de légitimité

Les Données à Caractère Personnel seront traitées sur la base des principes suivants :

- La Personne Concernée a explicitement donné son consentement ; ou

- Le Traitement est nécessaire à l'exécution d'un contrat auquel la Personne Concernée est partie ou à l'exécution de mesures prises à la demande de la Personne Concernée avant de conclure un contrat avec celle-ci ; ou

- Le traitement est nécessaire au respect d'une obligation légale à laquelle le Responsable de Traitement est soumis ; ou

- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la Personne Concernée ;  
ou

- Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le Responsable de Traitement ou le tiers auquel les données sont divulguées.

Les Données à Caractère Personnel peuvent également être traitées (i) si une Filiale d'ArcelorMittal est tenue de le faire par la loi ou du fait d'une procédure judiciaire (ii) pour le compte d'une autorité chargée de l'application des lois ou d'un agent du gouvernement sur la base d'une demande émanant d'une autorité gouvernementale ou en relation avec une enquête sur une activité illégale présumée ou avérée (iii) lorsque leur divulgation est nécessaire ou appropriée pour protéger les intérêts vitaux d'ArcelorMittal ou l'intégrité ou le bien-être physique ou mental de ses employés.

ou

- Le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le Responsable de Traitement ou par le(s) tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la Personne Concernée.

### 3.2. Règles relatives au traitement des Données à Caractère Personnel

Les Données à Caractère Personnel seront traitées loyalement et licitement.

Les Données à Caractère Personnel seront collectées pour des finalités spécifiques et légitimes et ne seront pas traitées ultérieurement de manière incompatible avec ces finalités.

Les Données à Caractère Personnel seront adéquates, pertinentes et ne seront pas excessives par rapport aux finalités pour lesquelles elles sont collectées et utilisées.

Les Données à Caractère Personnel seront exactes et, si nécessaire, mises à jour. Des mesures raisonnables seront prises pour corriger ou effacer les données inexactes ou incomplètes.

Les Données à caractère personnel ne seront conservées que dans la mesure nécessaire pour les finalités pour lesquelles elles ont été collectées et traitées, en prenant en compte les obligations légales de conservation des données.

Des Catégories Particulières de Données bénéficieront de protections supplémentaires prévues par l'Article 9 de la présente Procédure.

L'accès aux Données à Caractère Personnel est limité aux personnes qui ont besoin de les connaître et dont les fonctions requièrent la manipulation de ces Données à Caractère Personnel.

L'Annexe I comprend un questionnaire de contrôle permettant de vérifier le respect des règles qui précèdent.

L'Annexe II présente les procédures précises qui doivent être suivies lors de la création d'un nouveau système d'information afin d'assurer que les règles qui précèdent sont respectées.

### 3.3. Catégories Particulières de Données

Le Traitement des Données Spéciales est interdit sauf si :

- La Personne Concernée a donné son consentement explicite au Traitement de ces Données Spéciales, sauf dans le cas où la législation applicable interdit ce Traitement ; ou
- Le traitement est nécessaire au respect des obligations et des droits spécifiques du Responsable de Traitement en matière de droit du travail (par exemple en matière de lutte contre la discrimination), dans la mesure où ce traitement est autorisé par la législation nationale concernée et où cette législation prévoit des garanties adéquates ; ou
- Le traitement est nécessaire à la défense des intérêts vitaux de la Personne Concernée ou d'une autre personne dans le cas où la Personne Concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ; ou
- Le traitement est effectué dans le cadre d'activités légitimes et avec des garanties appropriées fournies par une fondation (telle que la Fondation ArcelorMittal), une association ou tout autre organisme à but non lucratif et à finalité de santé, de sécurité ou de responsabilité sociale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à ses finalités et que les données ne soient pas communiquées à des tiers sans le consentement des Personnes Concernées ; ou
- Le traitement porte sur des Données Spéciales manifestement rendues publiques par la Personne Concernée ; ou
- Le traitement de données sensibles est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ; ou
- Le traitement des données sensibles est nécessaire à des fins de médecine préventive, de diagnostics médicaux, d'administration de soins ou de traitements ou de gestion de services de santé, et le traitement de ces données sensibles est effectué par un professionnel de la santé soumis au secret professionnel par le droit national concerné ou par des réglementations arrêtées par les autorités nationales compétentes concernées ou par une autre personne également soumise à une obligation de confidentialité équivalente.

## **Article 4 - Sécurité et Confidentialité**

### 4.1. Contrôles de sécurité informatique de base d'ArcelorMittal

Des mesures techniques, physiques et organisationnelles appropriées seront prises pour empêcher l'accès non autorisé, le traitement illégal et la perte, la destruction ou la dégradation non autorisée ou accidentelle de données, tel que décrit de manière plus détaillée dans l'Annexe III jointe à la présente Procédure (Contrôles de sécurité informatique de base d'ArcelorMittal).

Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en œuvre, ces mesures assureront un niveau de sécurité adapté aux risques représentés par le traitement et la nature des données à protéger.

Tous les Outils globaux, tous les procédés spécifiques à chaque secteur et toutes les applications logicielles locales relevant du champ d'application de la présente Procédure doivent se soumettre aux Contrôles de sécurité informatique de base d'ArcelorMittal.

Afin d'assurer que tout futur outil ou procédé respecte cette norme, les Contrôles de sécurité informatique de base d'ArcelorMittal feront partie intégrante des spécifications (voir Annexe II). Tout consultant extérieur ayant accès aux systèmes et aux outils d'ArcelorMittal en tant qu'utilisateur doit s'engager à suivre les Contrôles de sécurité informatique de base d'ArcelorMittal.

Les Contrôles de sécurité informatique de base d'ArcelorMittal seront, au besoin, mis à jour par le Comité de Protection des Données.

Le niveau de protection et de sécurité ainsi défini constitue une norme minimale que toutes les Filiales d'ArcelorMittal doivent respecter. Il est recommandé aux Filiales d'ArcelorMittal d'adopter des mesures de sécurité supplémentaires lorsque cela est approprié.

Les questions concernant la conformité aux Contrôles de sécurité informatique de base d'ArcelorMittal (Annexe III) peuvent être adressées à l'Agent chargé de la Conformité et de la Sécurité Informatique compétent (« Agent chargé de la CSI », voir Annexe VI).

### 4.2. Atteintes à la sécurité

Le Correspondant à la Protection des Données et/ou l'Agent chargé de la CSI doivent immédiatement aviser le Comité de Protection des Données de toute atteinte à la sécurité supposée ou avérée ou de tout incident similaire ayant ou susceptible d'avoir compromis la confidentialité ou la sécurité de toute Donnée à Caractère Personnel.

La ou les Filiale(s) d'ArcelorMittal concernée(s) doivent prendre toutes les mesures nécessaires pour remédier à une telle atteinte à la sécurité supposée ou avérée et doivent faire en sorte que les prestataires extérieurs coopèrent pleinement, conformément aux instructions du Comité de Protection des Données. Tout Correspondant à la Protection des Données

désigné par le Comité de Protection des Données doit aider à détecter et identifier les atteintes à la sécurité.

La ou les Filiale(s) d'ArcelorMittal et le Correspondant à la Protection des Données concernés doivent pleinement coopérer avec les autorités civiles ou pénales dans toute enquête ou action se rapportant à cette atteinte ou à cette tentative d'atteinte à la sécurité.

L'atteinte à la sécurité doit ensuite être enregistrée par le Comité de Protection des Données pour diffuser les enseignements qui en sont tirés et modifier en conséquence les Contrôles de sécurité informatique de base d'ArcelorMittal (si nécessaire).

## **Article 5 – Droits des Personnes Concernées**

### 5.1. Responsable de Traitement

Chaque Filiale d'ArcelorMittal sera responsable de sa conformité à la présente Procédure.

Chaque Filiale d'ArcelorMittal est réputée Responsable de Traitement de ses Données RH, sauf disposition contraire prévue par une politique de confidentialité particulière ou approuvée par le Comité de Protection des Données.

(À titre d'information uniquement : pour les systèmes d'information non RH, l'entité juridique agissant en tant que « Propriétaire de l'activité » au sens des pratiques habituelles d'ArcelorMittal peut être considéré comme Responsable de Traitement).

### 5.2. Transparence et droit d'information

La présente Procédure doit être facilement accessible à chaque Personne Concernée. Une copie sera mise à disposition sur demande sous format papier ou par voie électronique.

La Personne Concernée sera informée du transfert et du traitement de ses Données à Caractère Personnel.

Avant le traitement de leurs données, les Personnes Concernées se verront communiquer les informations suivantes :

- L'identité du ou des Responsable(s) de Traitement et, le cas échéant, de son représentant ;
- Les finalités du Traitement auquel les données sont destinées ;
- Toute autre information telle que :
  - i) les destinataires ou les catégories de destinataires des données,
  - ii) l'existence d'un droit d'accès aux données le concernant et d'un droit de rectification de ces données.

Si les données n'ont pas été obtenues de la Personne Concernée, l'obligation d'informer la Personne Concernée ne s'applique pas si la communication des informations mentionnées ci-

dessus s'avère impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données concernées.

### 5.3. Droits d'accès à, de rectification, d'effacement et de verrouillage des données

Toute Personne Concernée a le droit d'obtenir, sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs, une copie de toutes les données la concernant qui sont traitées.

Pour lever toute ambiguïté, une Personne Concernée n'a pas le droit d'accéder à une Donnée à Caractère Personnel qui ne la concerne pas.

Toute Personne Concernée a le droit d'obtenir la rectification, l'effacement ou le verrouillage des données, notamment si ces données sont incomplètes ou inexactes.

Toute Personne Concernée a le droit de s'opposer à tout moment, pour des raisons impérieuses et légitimes relatives à sa situation particulière, au traitement des Données à Caractère Personnel la concernant, sauf si ce Traitement est exigé par la loi. En cas d'opposition justifiée, le traitement doit être arrêté.

Toute Personne Concernée a le droit de s'opposer, gratuitement en en faisant la demande, au traitement des Données à Caractère Personnel la concernant à des fins de prospection directe.

Les Personnes Concernées peuvent avoir accès à leurs Données à Caractère Personnel en présentant une demande dans ce sens au Responsable de Traitement concerné. Le Responsable de Traitement peut ne pas répondre aux demandes manifestement déraisonnables.

### 5.4. Décisions individuelles automatisées

Aucune évaluation ou décision liée à une Personne Concernée et qui a un effet significatif sur celle-ci ne sera prise sur le seul fondement d'un traitement automatisé des données de cette Personne concernée, sauf si cette décision :

- est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande préalable pour la conclusion ou l'exécution du contrat introduite par la Personne Concernée ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, aient été prises pour garantir la sauvegarde de ses intérêts légitimes ;

ou

- est autorisé par une loi qui prévoit également des mesures garantissant la sauvegarde des intérêts légitimes de la Personne Concernée.

## **Article 6 – Transferts de données**

Les Données à Caractère Personnel peuvent être traitées par des systèmes d'informations détenus et contrôlés par un Sous-traitant extérieur.

Avant de transmettre des Données à Caractère Personnel à un prestataire, la Filiale d'ArcelorMittal concernée doit choisir un prestataire apportant des garanties suffisantes concernant les mesures techniques de sécurité technique et les mesures organisationnelles relatives aux traitements à effectuer et doit veiller au respect de ces mesures.

#### 6.1. Transferts de Données à un Sous-traitant extérieur (« Fournisseur ») dans l'UE ou en dehors de l'UE

Règle d'Or #1 : Aucune Donnée à Caractère Personnel d'ArcelorMittal ne sera communiquée à/mise à la disposition d'un Sous-traitant extérieur sans contrat écrit et signé entre la Filiale d'ArcelorMittal concernée et ce Sous-traitant extérieur. Ce contrat comprendra la clause contractuelle type jointe à la présente Procédure (voir Annexe V).

Règle d'Or #2 : Aucune Donnée à Caractère Personnel d'ArcelorMittal ne sera communiquée à/mise à la disposition d'un Sous-traitant extérieur à moins ce Sous-traitant extérieur n'assure un niveau de protection équivalent à celui prévu par les Contrôles de sécurité informatique de base d'ArcelorMittal.

Règle d'Or #3 : En cas de transfert transfrontalier de l'Europe vers un pays situé en dehors de l'Europe, les clauses contractuelles types les plus récentes imposées par la législation européenne (ensemble de clauses contractuelles types pour le transfert transfrontalier de Données à Caractère Personnel du Responsable de Traitement au Sous-traitant) ou par toute législation nationale applicable seront également intégrées, le cas échéant, dans le Contrat signé entre la Filiale d'ArcelorMittal concernée et le Sous-traitant.

L'Évaluation de Sécurité décrite dans la présente Section sera effectuée avant la signature du contrat (ou le renouvellement du contrat) dans tous les cas où un Sous-traitant extérieur aura accès à des Données à Caractère Personnel.

L'objectif de l'Évaluation de Sécurité est de vérifier que le Sous-traitant extérieur assure le même niveau de protection pour les Données à Caractère Personnel d'ArcelorMittal que celui prévu par les Contrôles de sécurité informatique de base d'ArcelorMittal.

Avant de transmettre des Données à Caractère Personnel à un prestataire qui n'est pas une Filiale d'ArcelorMittal, les étapes suivantes doivent être suivies par la Filiale d'ArcelorMittal concernée en sa qualité de Responsable de Traitement :

→ Étape 1 : Évaluation de Sécurité

La Filiale d'ArcelorMittal concernée communiquera le Questionnaire d'Évaluation de Sécurité ci-joint (Annexe IV) au Fournisseur souhaitant fournir des services à ArcelorMittal.

La réponse du Fournisseur sera évaluée par l'Agent chargé de la Conformité et de la Sécurité Informatique afin d'évaluer si le niveau de protection proposé par le Fournisseur est équivalent à celui prévu par les Contrôles de sécurité informatique de base d'ArcelorMittal (Annexe III).

Dans le cadre de cette évaluation, la Filiale d'ArcelorMittal donnera à l'Agent chargé de la Conformité et de la Sécurité Informatique l'opportunité de discuter avec le Fournisseur, de suggérer des améliorations des mesures de sécurité du Fournisseur et d'inspecter ses systèmes afin de vérifier que le Fournisseur assure réellement un niveau de protection équivalent à celui prévu par les Contrôles de sécurité informatique de base d'ArcelorMittal.

Si le résultat de l'Évaluation est négatif du fait d'un problème majeur dans les politiques du Fournisseur, le processus de négociation sera bloqué et aucun contrat ne sera signé, sauf si le Fournisseur s'engage à résoudre le ou les problème(s) soulevé(s) par l'Agent chargé de la CSI dans un bref délai.

#### → Étape 2 : Contrat

Si la réponse du Fournisseur au Questionnaire d'Évaluation de Sécurité est considérée comme satisfaisante par l'Agent chargé de la CSI, cette réponse sera intégrée dans le contrat signé entre la Filiale d'ArcelorMittal et le Fournisseur et en fera partie intégrante.

Le contrat signé entre la Filiale d'ArcelorMittal concernée et le Sous-traitant extérieur comprendra également les dispositions standards jointes à la présente Procédure (voir Annexe V). Toutefois, si et dans la mesure où les Lois applicables en matière de protection des données imposent des obligations plus strictes concernant un tel contrat, les Lois applicables en matière de protection des données prévaudront, de sorte que les clauses types visées à l'Annexe V contraires aux Lois applicables en matière de protection des données seront remplacées par de nouvelles clauses conformes aux Lois applicables en matière de protection des données.

En cas de transfert transfrontalier de l'Europe vers un pays situé en dehors de l'Europe, les clauses contractuelles types les plus récentes imposées par la législation européenne (ensemble de clauses contractuelles types pour le transfert transfrontalier de Données à Caractère Personnel du Responsable de Traitement au Sous-traitant) ou par toute législation nationale applicable seront également intégrées, le cas échéant, dans le Contrat signé entre la Filiale d'ArcelorMittal concernée et le Sous-traitant.

## 6.2. Transfert de données à un Sous-traitant d'ArcelorMittal

Tout Sous-traitant d'ArcelorMittal doit respecter les Contrôles de sécurité informatique de base d'ArcelorMittal.

Les Contrôles de sécurité informatique de base d'ArcelorMittal sont automatiquement intégrés à tout contrat signé entre un Sous-traitant d'ArcelorMittal et ses clients (c'est-à-dire les Responsables de Traitements de Données).

La finalité du Traitement de Données à Caractère Personnel par le Sous-traitant d'ArcelorMittal pour le compte de son client fera l'objet d'un accord écrit entre le Sous-traitant d'ArcelorMittal et son client ArcelorMittal. Le Sous-traitant d'ArcelorMittal ne traitera pas les Données à Caractère Personnel à toute autre fin. Le Sous-traitant d'ArcelorMittal ne transfèrera les Données à Caractère Personnel que conformément aux instructions écrites de son client.

S'il sous-traite une partie ou l'ensemble des services à un Sous-traitant extérieur, le Sous-traitant d'ArcelorMittal doit respecter la procédure décrite à la Section 6.1 ci-dessus.

### 6.3. Transferts de données à un Responsable de Traitement extérieur

Tous les transferts de Données à Caractère Personnel de l'Europe vers des Responsables de Traitements extérieurs situés en dehors de l'UE doivent respecter les règles européennes en matière de flux transfrontaliers de données (Articles 25 et 26 de la Directive 95/46/CE : par exemple par l'utilisation de clauses contractuelles types de l'UE approuvées par les décisions 2001/497/CE ou 2004/915/CE de la Commission européenne ou par tout autre moyen contractuel adéquat conformément aux Articles 25 et 26 de la Directive Européenne).

### 6.4. Transferts de données à une nouvelle Filiale d'ArcelorMittal

Aucune Donnée à Caractère Personnel ne sera transférée à une nouvelle Filiale d'ArcelorMittal avant (i) signature de la présente Procédure par cette nouvelle Filiale, et (ii) nomination d'un Correspondant à la Protection des Données s'il n'y a aucun Correspondant à la Protection des Données dans le pays / segment concerné.

## **Article 7 – Mise en œuvre de la présente Procédure et mécanismes d'application**

- Conformité au niveau local/régional (Correspondant à la Protection des Données et CSI)
- Comité de Protection des Données d'ArcelorMittal
- Programme de formation
- Procédure interne de traitement des plaintes
- Plan d'Audit
- Assistance réciproque et coopération avec les Autorités de Protection des Données
- Mesures à prendre si la législation nationale empêche de respecter la présente Procédure

### 7.1. Conformité au niveau local/régional (Correspondant à la Protection des Données et CSI)

Correspondant à la Protection des Données

Chaque Responsable Pays ou Responsable Segment d'ArcelorMittal désignera un ou plusieurs Correspondant(s) à la Protection des Données. Une zone géographique et/ou organisationnelle précise sera affectée à chaque Correspondant à la Protection des Données.

Le Correspondant à la Protection des Données coordonnera toutes les mesures nécessaires pour veiller à ce que les Filiales relevant de sa zone respectent leurs obligations au titre de la présente Procédure.

Le Correspondant en matière de Protection des Données agira également en tant que personne à contacter pour toute plainte relevant de sa zone tel que défini la Section 7.4 de la présente Procédure (« Procédure Interne de traitement des plaintes ») et pour toute atteinte à la sécurité visée à la Section 4.2 de la présente Procédure (« Atteintes à la Sécurité »).

Le Correspondant à la Protection des Données a le devoir de pleinement coopérer avec ses pairs pour toute question se rapportant à la bonne exécution de la présente Procédure, en particulier pour les questions impliquant ou ayant une incidence sur plusieurs Contrôleurs de Données dans différents pays/segments.

Le Correspondant à la Protection des Données tiendra le Comité de Protection des Données constamment informé de toute plainte ou de tout autre question/problème relevant du champ d'application de la présente Procédure.

Si le Correspondant à la Protection des Données ne s'acquitte pas des obligations qui lui incombent, il peut être révoqué par le Comité de Protection des Données. Dans ce cas, un nouveau Correspondant à la Protection des Données sera désigné par le Responsable Pays ou par la direction locale.

#### Équipe Conformité et Sécurité Informatique (CSI)

Les Agents chargés de la Conformité et de la Sécurité Informatique ont pour mission de définir, de mettre en œuvre et de surveiller le déploiement d'un système de contrôle interne au sein de l'informatique d'ArcelorMittal nécessaire pour atteindre les objectifs informatiques en matière de Conformité et de Sécurité.

Plus particulièrement, les Agents chargés de la Conformité et de la Sécurité Informatique mettront en œuvre et contrôleront le déploiement des Contrôles de sécurité informatique de base d'ArcelorMittal en interne et, en ce qui concerne les Sous-traitants extérieurs, vérifieront que leur niveau de sécurité minimal est satisfaisant au regard de la Section 6.1 de la présente Procédure.

#### 7.2. Comité de Protection des Données d'ArcelorMittal

Le Comité de Protection des Données demeurera en activité pendant la durée de la présente Procédure.

Le Comité de Protection des Données sera composé de trois (3) membres principaux,

- . Un (1) membre qui sera désigné par le Directeur Informatique du Groupe ArcelorMittal,
- . Un (1) membre qui sera désigné par le Vice-président des Ressources Humaines d'ArcelorMittal, et
- . un secrétaire général désigné par le Directeur Juridique du Groupe ArcelorMittal.

Les membres initiaux du Comité de Protection des Données sont identifiés à l'Annexe IX.

Le Comité de Protection des Données comprendra également l'ensemble ou certains des Correspondants à la Protection des Données si les membres principaux l'estime nécessaire pour couvrir de manière efficace les points à l'ordre du jour d'une réunion donnée.

Par ailleurs, le directeur de l'Assurance Interne d'ArcelorMittal peut à sa discrétion participer en personne ou désigner un représentant pour participer aux réunions du Comité de Protection des Données.

Chaque membre peut, à sa discrétion, inviter d'autres personnes ou des consultants à participer aux réunions du Comité de Protection des Données. Pour lever toute ambiguïté, tout consultant ainsi invité ne prendra pas part aux décisions et ne sera pas considéré comme un membre du Comité de Protection des Données d'ArcelorMittal.

Le Directeur informatique du Groupe, le Vice-président des Ressources Humaines et le Directeur Juridique du Groupe peuvent à tout moment révoquer la désignation du ou des membre(s) qu'ils ont désigné(s), et désigner un ou des remplaçant(s) (dont le mandat commencera immédiatement) moyennant notification de cette révocation et de ce remplacement aux autres membres.

Le Comité de Protection des Données se réunira à toutes dates et lieux dont les membres du Comité de Protection des Données conviendront de temps à autre, mais en aucun cas moins d'une (1) fois par trimestre.

L'ordre du jour de chaque réunion sera établi par le secrétaire général et communiqué aux autres membres du Comité de Protection des Données ainsi qu'aux Correspondants à la Protection des Données.

Dans les trois (3) jours ouvrables suivant chaque réunion du Comité de Protection des Données, le secrétaire général du Comité de Protection des Données préparera et enverra aux autres membres de ce Comité un rapport écrit détaillé des décisions adoptées lors de la réunion.

Ce Rapport sera également communiqué aux Correspondants à la Protection des Données.

Le Comité de Protection des Données :

- (i) maintiendra et tiendra à jour la liste des Filiales d'ArcelorMittal liées par la présente Procédure ;
- (ii) maintiendra et tiendra à jour la liste des Correspondants à la Protection des Données, conformément aux demandes des Responsables d'ArcelorMittal au niveau local/régional (voir la liste initiale à l'Annexe VI) ;
- (iii) surveillera la mise en œuvre de la présente Procédure et son exécution par les Filiales, y compris les futures Filiales d'ArcelorMittal ;
- (iv) résoudra toute question / tout problème majeur(e) pouvant survenir ;

- (v) lancera, validera et mettra à jour les politiques spécifiques pour les Outils Globaux (aucune politique de ce type ne sera applicable sans l'autorisation préalable du Comité de Protection des Données) ;
- (vi) mettra à jour l'Annexe II et les Annexes III, IV, V, VI, VII et VIII avec pleine autorité. Ces modifications seront notifiées au Correspondants à la Protection des Données ainsi qu'aux Agents chargés de la CSI et deviendront contraignantes à la date mentionnée dans la notification. À titre d'exemple, il est possible que la clause type pour les prestataires de services externes à l'Annexe V doive être adaptée aux lois nationales et à toute évolution de ces dernières, pays par pays.
- (vii) modifiera la présente Procédure si nécessaire, par exemple, pour respecter toute modification de la législation, des règles ou des pratiques et procédures d'ArcelorMittal, de la structure sociale d'ArcelorMittal ou des prescriptions imposées par les autorités en matière de protection des données. Les modifications de ce document de base seront notifiées aux Filiales d'ArcelorMittal et seront réputées acceptées par chacune d'elles après un délai de deux (2) mois, sauf refus spécifique écrit d'une Filiale.
- (viii) s'assurera que les modifications de ce document de base et les modifications de la liste des Filiales d'ArcelorMittal liées par la présente Procédure seront notifiées aux Autorités de Protection des Données accordant les autorisations nécessaires accompagnées d'une brève explication des motifs de ces modifications.
- (ix) assurera un suivi de toutes les versions de la présente Procédure.

### 7.3 Programme de formation

Une formation appropriée concernant la présente Procédure sera fournie aux membres du personnel ayant accès de manière permanente ou régulière à des Données à Caractère Personnel et à ceux qui participent à la collecte de Données à Caractère Personnel ou au développement d'outils utilisés pour traiter les Données à Caractère Personnel.

Le Correspondant à la Protection des Données sera chargé de ce programme de formation, qui pourra être mené sous forme de programme de formation en ligne.

### 7.4 Procédure interne de traitement des plaintes

Toute Personne Concernée peut porter plainte si un Responsable de Traitement d'ArcelorMittal ne respecte pas la présente Procédure.

Le Correspondant à la Protection des Données du Responsable de Traitement d'ArcelorMittal concerné sera chargé de gérer cette plainte dans un délai raisonnable. Un premier retour sera communiqué au demandeur dans un délai d'un (1) mois suivant la plainte. Le Correspondant à

la Protection des Données mettra ensuite tout en œuvre pour traiter la plainte dans les plus brefs délais en tenant compte de la complexité et de la portée de celle-ci. Il est prévu qu'une enquête pour plainte dure entre un (1) et six (6) mois, sauf circonstances inhabituelles et exceptionnelles.

Si une question ne peut pas être résolue par le Correspondant à la Protection des Données, elle sera transmise par ce dernier au Comité de Protection des Données d'ArcelorMittal.

La Personne Concernée peut à tout moment déposer une plainte auprès de l'Autorité de Protection des Données compétente ou engager une procédure auprès du tribunal de l'Exportateur de Données situé dans l'UE.

## 7.5 Plan d'Audit

La conformité du groupe à la présente Procédure sera régulièrement vérifiée par le Département Assurance Interne. La fréquence des vérifications sera d'au moins deux fois par an. Le Département Assurance Interne peut être aidé par un membre du Comité de Protection des Données. Une équipe extérieure peut également être nommée.

Cette vérification peut couvrir tous les aspects de la présente Procédure, à la fois en Europe et en dehors de l'Europe.

Chaque vérification sera suivie d'un rapport détaillant si nécessaire les mesures correctives à prendre (Phase 1). Ces mesures seront prises par la ou les Filiale(s) d'ArcelorMittal concernée(s) dans un délai spécifique stipulé dans le rapport. Une seconde visite sera alors faite pour s'assurer de la mise en œuvre de toutes les mesures correctives (Phase 2).

Le Département Assurance Interne et le Comité de Protection des Données établiront un Plan d'Audit annuel.

Une copie de tous les rapports d'audit sera communiquée (i) au(x) Correspondant(s) à la Protection des Données concerné(s), (ii) au Comité de Protection des Données, (iii) au Vice-président des Ressources Humaines, au Directeur Informatique du Groupe et au Directeur Juridique du Groupe et (iv) à la direction de la Filiale ou des Filiales concernées.

Les Autorités de Protection des Données pourront avoir accès aux rapports d'audit sur demande.

Les rapports d'audit ne seront communiqués d'aucune manière que ce soit à aucun organisme ou personne non visé(e) à la présente Section 7.5 (« Plan d'Audit »).

## 7.6. Assistance réciproque et coopération avec les Autorités de Protection des Données

- Les Filiales coopéreront et se prêteront mutuellement assistance pour traiter toute requête ou plainte émanant d'une Personne Concernée ou toute enquête ou question des Autorités de Protection des Données.

- En cas de violation de la présente Procédure en dehors de l'Europe, l'Autorité de Protection des Données du pays de situation de l'Exportateur de Données peut demander qu'il soit procédé à un audit par le Département Assurance Interne d'ArcelorMittal. Cet audit sera réalisé conformément à la Section 7.5 de la présente Procédure.

- Les Filiales se soumettront à l'avis des Autorités de Protection des Données pour toute question relative à l'interprétation de la présente Procédure.

#### 7.7 Mesures à prendre si la législation nationale empêche le respect de la présente Procédure

Si une Filiale a des raisons de croire que la législation qui lui est applicable empêche le Responsable de Traitement de satisfaire ses obligations en vertu de la présente Procédure et a un effet significatif sur les garanties prévues par la présente Procédure, elle en informera rapidement le Comité de Protection des Données (sauf si une autorité chargée de l'application de la loi l'interdit, comme en cas d'interdiction de divulgation soumise au droit pénal afin de protéger la confidentialité d'une enquête pénale).

Par ailleurs, en cas de conflit entre une législation nationale et les engagements de la présente Procédure, le Comité de Protection des Données prendra une décision responsable sur les mesures à prendre et consultera les Autorités de Protection des Données compétentes en cas de doute.

### **Article 8 - Responsabilité**

Toute Personne Concernée peut demander le respect des principes suivants, en tant que droits, auprès de l'Autorité de Protection des Données compétente ou du tribunal compétent pour exercer des recours et obtenir réparation si l'une des Filiales ne respecte pas ces principes :

- o Législation nationale empêchant le respect de la présente Procédure, telle que décrite à la Section 7.7 de la présente Procédure,
- o Droit de déposer une plainte via la procédure interne de traitement des plaintes décrite à la Section 7.4,
- o Obligations de coopération avec l'Autorité de Protection des Données comme décrit à la Section 7.6,
- o Dispositions relatives à la responsabilité et à la compétence juridique telles que décrites à la Section suivante et à la Section 7.4.
- o Limitation de finalité telle que définie à la Section 3.2,
- o Qualité et proportionnalité des données telles que définies à la Section 3.2,
- o Critères de légitimité du traitement de données, tels qu'énoncés à la Section 3.1,
- o Transparence et facilité d'accès à la présente Procédure, telles que décrites à la Section 5.2,
- o Droits d'accès aux données, de rectification, d'effacement, de verrouillage des données et d'opposition à leur traitement, tels que décrits dans la Section 5.3,
- o Droits en cas de décisions individuelles automatisées, tels que définis à la Section 5.4,
- o Sécurité et confidentialité, telles que définies à la Section 4,
- o Limitations sur les transferts en dehors du groupe de sociétés, telles qu'énoncées aux Sections 6.1 et 6.3.

Chaque Filiale d'ArcelorMittal accepte d'être responsable de toute violation de la présente Procédure, nonobstant le mécanisme de responsabilité solidaire en cas de violation visé à la Section 8.2.

La Personne Concernée peut à tout moment déposer plainte auprès de l'Autorité de Protection des Données compétente ou engager une procédure dans la juridiction de l'Exportateur de Données situé dans l'UE, comme décrit dans la Section 7.4.

Ces droits ne s'étendent pas aux éléments de la présente Procédure relatifs aux mécanismes internes mis en œuvre au sein des Filiales, tels que les détails de la formation, des programmes d'audit, du réseau de conformité et du mécanisme de mise à jour des règles.

### 8.1. Obligation de remédier aux violations

Si une Filiale d'ArcelorMittal viole la présente Procédure, cette Filiale d'ArcelorMittal défaillante doit remédier à ce problème et prendre les mesures nécessaires pour se conformer à la présente Procédure.

Les Filiales conviennent qu'elles doivent remédier aux violations, aux défaillances ou à toute non-conformité avec la présente Procédure pour empêcher que ce problème ne se reproduise dans le futur.

### 8.2. Obligation de verser des dommages et intérêts à la Personne Concernée

Par ailleurs, toute Personne Concernée ayant subi un préjudice du fait d'une violation des huit (8) droits énoncés ci-dessus est en droit de recevoir un dédommagement pour le préjudice subi.

Si la Filiale défaillante n'est pas située en Europe, les règles suivantes s'appliqueront :

- o Cette Filiale défaillante et l'Exportateur de Données seront conjointement et solidairement responsables du préjudice subi par la Personne Concernée suite à une violation des dispositions de la présente Procédure.
- o La Filiale défaillante indemniserà l'Exportateur de Données de tous frais, charges, dommages, dépenses ou pertes qu'il aura subis.
- o Si l'Exportateur de Données peut démontrer que le membre situé en dehors de l'Europe n'est pas responsable du manquement, il peut se décharger de toute responsabilité.

## ANNEXE I

### PRINCIPES DE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

#### LISTE DE VÉRIFICATION

La présente liste de vérification vise à illustrer la manière dont les principes de protection des données doivent être compris.

*« Les Données Personnelles seront traitées loyalement et licitement ».*

- Existe-il un besoin commercial clair de traiter ces informations ?
- Les personnes dont je détiens les informations savent-elles que je détiens ces informations et peuvent-elles comprendre la finalité de leur utilisation ?
- Dois-je en informer l'Autorité de Protection des Données et, dans l'affirmative, ma notification est-elle à jour ?

*« Les Données à Caractère Personnel seront collectées pour des finalités spécifiques et légitimes et ne seront pas traitées ultérieurement de manière incompatible avec ces finalités. »*

- Est-ce que je sais ce que je vais faire de ces Données à Caractère Personnel ?
- Si on me demande de communiquer des Données à Caractère Personnel, est-ce que les personnes concernées par les informations que je détiens s'attendent à ce que je le fasse ?

*« Les Données à Caractère Personnel seront adéquates, pertinentes et ne seront pas excessives par rapport aux finalités pour lesquelles elles sont collectées et utilisées. »*

- Ai-je vraiment besoin de ces informations concernant une personne ?

*« Les Données à Caractère Personnel seront exactes et, si nécessaire, mises à jour. Des mesures raisonnables seront prises pour corriger ou effacer les données inexactes ou incomplètes. »*

- Suis-je sûr que les données personnelles sont exactes et mises à jour ?

*« Les Données à Caractère Personnel ne seront conservées que dans la mesure nécessaire pour les finalités pour lesquelles elles ont été collectées et traitées, en prenant en compte les obligations légales de conservation des données. »*

- Est-ce que je supprime ou est-ce que je détruis les informations à caractère personnel dès que je n'en ai plus besoin ?

*« Les données sensibles bénéficieront de protections supplémentaires prévues par la Directive européenne 95/46/CE »*

- Est-ce que j'ai formé mon personnel concernant leurs obligations et responsabilités au titre de la Procédure de Protection des Données d'ArcelorMittal, et s'acquittent-ils de ces obligations et responsabilités ?

*« L'accès aux Données à Caractère Personnel est limité aux personnes qui ont besoin de les connaître et dont les fonctions requièrent la manipulation de ces Données à Caractère Personnel. »*

- L'accès aux Données à Caractère Personnel est-il strictement limité à ceux qui ont besoin de les connaître ?
- Est-ce que je suis sûr que les informations sont conservées de manière sécurisée ?

## ANNEXE II

### PROCÉDURE DE VÉRIFICATION DE LA PROTECTION DES DONNÉES AVANT DE TERMINER LA PHASE DE CONCEPTION D'UN PROJET

La phase de conception d'un projet est cruciale pour veiller à ce que la procédure/l'application en résultant est conforme à la présente Procédure. La « phase de conception » désigne la phase pendant laquelle l'architecture, les spécifications et les fonctionnalités d'un nouveau système sont définies par l'équipe du projet, pour le compte du ou des Responsable de Traitement(s).

Les principes énoncés dans la présente Procédure doivent être intégrés dans tout nouveau système d'information ou toute évolution substantielle de ce dernier, dès la phase de conception.

La présente ANNEXE décrit la manière dont cet objectif sera atteint.

À titre de remarque préliminaire, il est important de noter que la présente Procédure est neutre sur le plan technologique. Si un système existant est simplement redéveloppé sur la base d'une nouvelle technologie, tout en conservant les mêmes procédés, les mêmes données, les mêmes mesures d'organisation et de sécurité, les recommandations émises à la date de conception du système existant devront être suivies, mais aucune nouvelle procédure de vérification de la Protection des Données ne sera nécessaire pour ledit redéveloppement.

La présente ANNEXE est applicable à tout nouveau système d'information relevant du champ d'application de la présente Procédure, ou à toute évolution de ce dernier (à la condition toutefois que la méthode de traitement des Données à Caractère Personnel soit modifiée).

#### ➤ Nouvel Outil Global

Le Comité de Protection des Données doit être consulté par l'équipe du projet avant la validation de la conception d'un nouvel Outil Global.

Le Comité de Protection des Données conseillera et aidera l'équipe du projet à s'assurer que la conception du système est conforme à la présente Procédure.

En tout état de cause, les Contrôles de sécurité informatique de base (voir ANNEXE III) seront intégrés aux spécifications.

#### ➤ Processus spécifique à un segment

Les Correspondants à la Protection des Données des pays concernés doivent être consultés par l'équipe du projet avant toute validation de la conception d'une nouvelle procédure spécifique à un segment.

Les Correspondants à la Protection des Données conseilleront et aideront l'équipe du projet à s'assurer que la conception du système est conforme à la présente Procédure.

En tout état de cause, les Contrôles de sécurité informatique de base (voir ANNEXE III) seront intégrés aux spécifications.

Si le nouveau système est censé utiliser des Données à Caractère Personnel extraites d'un outil ou d'un procédé déjà existant, l'équipe du projet doit également consulter le Comité de Protection des Données.

#### ➤ Applications logicielles locales

Le Correspondant à la Protection des Données du pays concerné doit être consulté avant toute validation de la conception du système.

Les Correspondants à la Protection des Données conseilleront et aideront l'équipe du projet à s'assurer que la conception du système est conforme à la présente Procédure.

En tout état de cause, les Contrôles de sécurité informatique de base (voir ANNEXE III) seront intégrés aux spécifications.

Si la nouvelle application logicielle est censée utiliser des Données à Caractère Personnel extraites d'un système déjà existant, l'équipe du projet doit également consulter le Comité de Protection des Données.

La présente procédure peut impliquer la prise de différentes mesures selon le cas ou l'application particulière. Par exemple, dans certains cas, elle peut imposer l'élimination/la réduction des Données à Caractère Personnel, la prévention de tout traitement inutile ou l'amélioration des mesures de sécurité afin de respecter les Contrôles de sécurité informatique de base.

Le ou les Responsable de Traitements seront chargés d'intégrer les recommandations du Correspondant à la Protection des Données au système concerné.

Dernière version mise à jour des Règles relatives à la création d'un nouveau système d'information : <http://www.....> Intranet d'ArcelorMittal

## **ANNEXE III**

### **CONTRÔLES DE SÉCURITÉ INFORMATIQUE DE BASE**

Dernière version mise à jour des Contrôles : <http://www.....> Intranet d'Arcelormittal

**ANNEXE IV**

**QUESTIONNAIRE D'ÉVALUATION DE SÉCURITÉ (« QES »)**

Dernière version mise à jour du Questionnaire : <http://www.....> Intranet d'Arcelormittal

## ANNEXE V

Clause contractuelle type pour les Sous-traitants extérieurs d'ArcelorMittal

Cette clause doit être intégrée et est OBLIGATOIRE dans tous les contrats entre une Filiale d'ArcelorMittal agissant en tant que Responsable de Traitement et un Sous-traitant extérieur agissant en tant que prestataire et auquel la Filiale d'ArcelorMittal divulguera des Données à Caractère Personnel relevant du champ d'application de la présente Procédure par voie de flux structurés de Données à Caractère Personnel européennes de la Filiale d'ArcelorMittal au Sous-traitant extérieur en vue de promouvoir l'objet du contrat.

. Il est prévu que l'Accord Commercial dans lequel cette clause sera intégrée comprenne déjà une claire description (i) de l'objet global du contrat, (ii) des services à exécuter, et (iii) des données à transférer à ou à mettre à disposition du Sous-traitant.

La présente Annexe comprend également une version spécifique pour l'Allemagne (voir ci-après).

### Protection des Données

« Donnée à Caractère Personnel » désigne toute donnée se rapportant à une personne identifiée ou identifiable (i) communiquée par ArcelorMittal ou par une Filiale d'ArcelorMittal et parvenant à la connaissance du Fournisseur ou de toute filiale du Fournisseur conformément au présent Accord, (ii) créée dans le cadre ou découlant de données fournies par ArcelorMittal ou toute Filiale d'ArcelorMittal conformément au présent Accord, et (iii) automatiquement générée par les services fournis à ArcelorMittal par le Fournisseur.

*[ArcelorMittal est et restera le Responsable de Traitement et le Fournisseur n'agira qu'en qualité de Sous-traitant des Données à Caractère Personnel] (\*)*. Le Fournisseur ne traitera pas de Données à Caractère Personnel (notamment les Données à Caractère Personnel initialement traitées par ArcelorMittal), à moins qu'il n'agisse pour fournir les services décrits dans le présent Accord. Le Fournisseur mettra tout en œuvre pour veiller à la fiabilité des membres de son personnel ayant accès à ou étant chargés du traitement des Données à Caractère Personnel.

À la résiliation ou à l'expiration du présent Accord ou sur demande écrite d'ArcelorMittal, le Fournisseur : (i) cessera immédiatement de traiter les Données à Caractère Personnel ; et (ii) restituera à ArcelorMittal ou, au choix d'ArcelorMittal, détruira les Données à Caractère Personnel et toutes les copies, notes ou extraits de ces dernières, dans les sept (7) jours ouvrables suivant la date de résiliation ou d'expiration du présent Accord ou à la réception de la demande. À la demande d'ArcelorMittal, le Fournisseur confirmera également par écrit avoir respecté les obligations énoncées dans la présente clause.

Le Fournisseur respectera à tout moment les politiques en matière de sécurité informatique (\*\*\*) jointes au présent Accord et toutes les lois et règles pertinentes se rapportant à la protection des données (« Lois sur la Protection des Données »). Si et dans la mesure où les Lois sur la Protection des Données imposent des obligations, notamment des mesures de sécurité, plus strictes au Fournisseur que dans le cadre du présent Accord, les Lois sur la Protection des Données prévaudront.

Le Fournisseur ne communiquera pas ni ne transférera de quelque manière que ce soit de Données à Caractère Personnel à un tiers, notamment à une filiale ou à un sous-traitant du Fournisseur (« Sous-Sous-traitant ultérieur ») sans le consentement écrit et préalable d'ArcelorMittal, lequel consentement pourra être refusé avec ou sans motif valable, à la seule discrétion d'ArcelorMittal. Avant de demander le consentement d'ArcelorMittal, le Fournisseur communiquera à ce dernier toutes les informations concernant le rôle du Sous-Sous-traitant ultérieur proposé, notamment l'identité du Sous-Sous-traitant ultérieur, son historique de sécurité des données, le lieu de ses installations de traitement, une description du projet d'accès aux données d'ArcelorMittal et toutes autres informations qu'ArcelorMittal peut raisonnablement demander pour évaluer les risques liés au fait de permettre au Sous-Sous-traitant ultérieur de traiter des Données à Caractère Personnel. ArcelorMittal peut, à titre de condition de son approbation d'un Sous-Sous-traitant proposé, demander au Fournisseur de conclure un accord écrit avec le Sous-Sous-traitant ultérieur contenant des termes équivalents au présent Accord (à la condition que le Fournisseur n'ait pas le droit d'autoriser le Sous-Sous-traitant ultérieur à sous-traiter à nouveau ou à autrement déléguer tout ou partie du traitement effectué par le Sous-Sous-traitant ultérieur sans le consentement écrit et préalable d'ArcelorMittal, qui sera donné à la seule discrétion d'ArcelorMittal). En tout état de cause, le Fournisseur fera en sorte que son Sous-Sous-traitant autorisé respecte à tous égards les obligations en matière de protection des données stipulées dans le présent Accord et l'ensemble des lois pertinentes se rapportant à la protection des données.

Le cas échéant, conformément à la Directive européenne 95/46, ArcelorMittal peut imposer au Fournisseur de signer toutes conditions supplémentaires, y compris, sans s'y limiter, les clauses contractuelles types pour le transfert d'Informations à Caractère Personnel à des pays tiers selon la Directive 95/46/CE, et le Fournisseur se soumettra à ces clauses.

Le Fournisseur communiquera à ArcelorMittal tous les rapports d'audit publiés par le Département d'Audit Interne du Fournisseur se rapportant en tout ou partie aux services fournis à ArcelorMittal.

Par ailleurs, le Fournisseur notifiera par écrit à l'Agent chargé de la Conformité et de la Sécurité Informatique d'ArcelorMittal toute atteinte à la sécurité suspectée ou avérée ayant compromis ou étant susceptible d'avoir compromis la confidentialité ou la sécurité de données d'ArcelorMittal (notamment de Données à Caractère Personnel) dans les vingt-quatre (24) heures suivant cette atteinte suspectée ou avérée. Cette notification comprendra une description de toutes les mesures déjà prises et à prendre par le Fournisseur en vue de remédier à l'atteinte suspectée ou avérée.

Le Fournisseur portera pleinement assistance à ArcelorMittal pour répondre à toute demande d'une Personne Concernée d'accéder à ses Données à Caractère Personnel. Si une Personne Concernée demande directement au Fournisseur de communiquer des informations concernant ses Données à Caractère Personnel, le Fournisseur devra immédiatement transmettre cette demande à ArcelorMittal et ne

devra pas répondre à la Personne Concernée sans qu'ArcelorMittal ne le lui demande.

Le Fournisseur aidera ArcelorMittal à procéder à l'enregistrement ou à répondre à toute autre exigence applicable dans le cadre des Lois sur la Protection des Données ou des lois en matière de confidentialité, y compris, sans s'y limiter, à fournir les informations requises, à s'enregistrer auprès des Autorités de Protection des Données ou à participer à des programmes d'autorégulation à la demande d'ArcelorMittal.

Commentaires :

Dans la disposition contractuelle qui précède, « Fournisseur » désigne le Sous-traitant et « ArcelorMittal » désigne la Filiale d'ArcelorMittal concernée. Si nécessaire, la formulation de la clause ci-dessus peut être adaptée à la formulation de l'Accord sans influencer sur le niveau d'engagement du Sous-traitant extérieur.

Tout contrat signé entre la Filiale d'ArcelorMittal et le Sous-traitant extérieur doit également inclure une clause « Droit d'Audit ». Conformément à cette clause, la Filiale d'ArcelorMittal aura le droit pendant toute la durée du contrat de vérifier que le Fournisseur se conforme aux Contrôles de sécurité informatique de base d'ArcelorMittal.

(\*) Cette *[disposition]* ne doit être intégrée que si l'entité juridique d'ArcelorMittal signant l'accord est située en Europe. Cette disposition n'est valable qu'en droit européen.

(\*\*) Les Politiques de Sécurité Informatique visées au troisième paragraphe découlent de l'Évaluation de Sécurité. Dans la plupart des cas, elle prendra la forme des Politiques de Sécurité du Fournisseur, éventuellement modifiées afin de respecter les Contrôles de sécurité informatique de base d'ArcelorMittal.

Dernière version mise à jour des clauses : <http://www.....> Intranet d'Arcelormittal

ALLEMAGNE

Ci-après une version spécifique pour l'Allemagne

<b>Agreement on Data Processing Agency</b>	<b>Contrat d'Agence pour le Traitement de Données</b>
<p><b>2. Scope of Application</b></p> <p>Rendering the services pursuant to the Framework Contract <b>dating from ...</b> 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><b>2. Champ d'Application</b></p> <p>Dans le cadre de la prestation de services conformément au Contrat Cadre <b>en date du ...</b>, y compris ses annexes, (ci-après généralement dénommé « le Contrat Cadre »), l'Agent doit avoir accès aux données à caractère personnel du Commettant ou d'autres tiers (ci-après généralement désignées par « Données d'AM »). Le présent contrat définira clairement les droits et les obligations des parties en lien avec la législation sur la protection et la confidentialité des données lors de l'exécution du Contrat Cadre.</p>
<p><b>2. Commissioned Data Processing</b></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</p>	<p><b>2. Traitement de Données par mandat</b></p> <p>2.1 L'Agent collectera, traitera et/ou utilisera les Données d'AM exclusivement au nom et conformément aux instructions du Commettant au sens de la Sec. 11 de la Loi Fédérale Allemande sur la Protection des Données (Traitement des Données par mandat). Le Commettant restera l'entité responsable en matière de protection des données (« Responsable de Traitement ») et est responsable de la légalité de la collecte, du traitement et/ou de l'utilisation des Données d'AM conformément à ses instructions.</p> <p>2.2 La collecte, le traitement et/ou l'utilisation des Données d'AM se produiront exclusivement et intégralement dans la République Fédérale d'Allemagne (RFA) et de la manière, dans la mesure et à la finalité exclusivement définies dans l'Annexe 1 du présent contrat. La collecte, le</p>

<p>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> <p>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).</p>	<p>traitement et/ou l'utilisation des Données d'AM comprennent le type de Données d'AM et le cercle des personnes concernées tels qu'exclusivement définis dans l'Annexe 1 du présent contrat.</p> <p>2.3 L'Agent n'acquerra aucun droit sur les Données d'AM et sera tenu de restituer les Données d'AM à tout moment à la demande du Commettant. Tout droit de rétention se rapportant aux Données d'AM est exclu.</p> <p>2.4 L'Agent, à la demande du Commettant et dans un délai raisonnable, communiquera des informations complètes au Commettant si ces informations sont exigées pour mettre en place ou pour mettre à jour le contrôle interne par le Commettant du traitement des données à caractère personnel (Sec. 4g para. 2 de la Loi Fédérale Allemande sur la Protection des Données).</p> <p>2.5 En règle générale, si l'Agent déploie au moins dix (10) personnes pour procéder au traitement automatisé de données à caractère personnel, l'Agent sera tenu de nommer par écrit un détaché à la protection des données (Sec. 4f para. 1 phrases 1- 4 de la Loi Fédérale Allemande sur la Protection des Données).</p>
<p><b>3. Instructions by the Principal</b></p> <p>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.</p> <p>3.2 Instructions issued in individual cases</p>	<p><b>3. Instructions du Commettant</b></p> <p>3.1 Concernant l'utilisation des Données d'AM, l'Agent sera tenu de se conformer entièrement aux instructions découlant du Contrat Cadre ainsi qu'aux instructions émanant du Commettant. Le Commettant se réserve le droit de donner des instructions à l'Agent concernant la méthode, l'étendue et la pratique du traitement des données et de l'utilisation des données.</p> <p>3.2 Les instructions données dans des</p>

<p>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.</p> <p>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 :</p> <p style="text-align: center;">Persons Authorized to Issue Instructions:</p> <p style="text-align: center;">_____</p> <p style="text-align: center;">_____</p> <p style="text-align: center;">Representative:</p> <p style="text-align: center;">_____</p> <p style="text-align: center;">_____</p> <p>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.</p> <p>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 undue delay. The Agent shall be entitled to refrain from the execution of such instruction unless the Principal confirms its instruction.</p>	<p>cas individuels le seront par écrit ou par email. Dans des cas justifiés et individuels, les instructions peuvent également être données par oral ; toutefois, le Commettant fera confirmer ultérieurement ces instructions, par écrit ou par email et dans les plus brefs délais, par la personne habilitée conformément à la clause 3.3 du présent contrat.</p> <p>3.3 Les instructions ne peuvent être données que par des personnes habilitées à donner des instructions et leurs représentants. Les parties conviennent des personnes suivantes qui donneront des instructions pour le compte du Commettant :</p> <p style="text-align: center;">Personnes Autorisées à donner des Instructions :</p> <p style="text-align: center;">_____</p> <p style="text-align: center;">_____</p> <p style="text-align: center;">Représentants :</p> <p style="text-align: center;">_____</p> <p style="text-align: center;">_____</p> <p>3.4 Chaque partie informera immédiatement par écrit l'autre partie si les personnes responsables sont remplacées ou se trouvent dans l'incapacité d'agir et nommera si nécessaire un remplaçant.</p> <p>3.5 Si l'Agent estime qu'une instruction est contraire à une réglementation statutaire et/ou à une disposition du Contrat Cadre, il sera tenu d'en informer le Commettant dans les meilleurs délais. L'Agent sera en droit de s'abstenir d'exécuter cette instruction, à moins que le Commettant ne confirme son instruction.</p>
<p><b>4. Obligations of the Principal</b></p> <p>4.1 The Agent acknowledges that the Principal remains responsible for the legality of the processing of AM Data and</p>	<p><b>4. Obligations du Commettant</b></p> <p>4.1 L'Agent reconnaît que le Commettant reste responsable de la légalité du traitement des Données d'AM et que le</p>

<p>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>Commettant est seul responsable de la protection des droits des Personnes Concernées en application des Règles en matière de Protection des Données.</p> <p>4.2 Le Commettant est le propriétaire des Données d'AM et détient tous les droits se rapportant aux Données d'AM.</p>
<p><b>5. Obligations of the Agent</b></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>5.5 The Agent shall be obliged to correct,</p>	<p><b>5. Obligations de l'Agent</b></p> <p>5.1 Le Sous-traitant s'engage à traiter et à utiliser les Données d'AM, conformément au Contrat Cadre, aux Règles en vigueur en matière de Protection des Données (en particulier celles de la Loi Fédérale Allemande sur la Protection des Données), aux instructions du Commettant et aux dispositions du présent Accord.</p> <p>5.2 L'Agent convient et garantit que les Données d'AM seront sauvegardées et traitées séparément des autres Données conservées sur ses serveurs (en particulier des données à caractère personnel traitées pour d'autres commettants).</p> <p>5.3 Le Sous-traitant n'est pas autorisé à copier ou dupliquer les Données d'AM sans le consentement écrit et préalable du Contrôleur, sauf si ces copies ou duplicatas sont nécessaires ou habituels pour garantir le bon traitement des données conformément aux dispositions du Contrat Cadre ou pour respecter des dispositions statutaires en matière de conservation des données.</p> <p>5.4 L'Agent apposera une marque spéciale sur tous les supports de données appartenant au Commettant ou utilisés pour le compte du Commettant. Les supports entrants et sortants seront soumis à contrôle constant qui sera documenté.</p> <p>5.5 L'Agent sera tenu de corriger,</p>

<p>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>d'effacer et/ou de verrouiller les Données d'AM conformément aux instructions du Commettant dans les plus brefs délais (Sec. 35 de la Loi Fédérale Allemande sur la Protection des Données).</p> <p>5.6 À la demande du Commettant, l'Agent sera tenu de communiquer au Commettant, dans les plus brefs délais, un résumé de toutes les informations visées à la Sec. 4e phrase 2 de la Loi Fédérale Allemande sur la Protection des Données ainsi qu'une liste des personnes ayant accès à ces données (Sect. 4g para. 2 phrase 1 de la Loi Fédérale Allemande sur la Protection des Données).</p> <p>5.7 À la demande du Commettant, l'Agent sera tenu d'accepter les modifications des dispositions de l'Annexe 1 du présent contrat si et dans la mesure où l'Agent n'a pas de raison factuelle pour refuser de les accepter.</p>
<p><b>6. Data Secrecy</b></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><b>6. Confidentialité des Données</b></p> <p>L'Agent est tenu de faire en sorte que les personnes employées à la collecte, au traitement et/ou à l'utilisation des Données d'AM s'engagent par écrit à protéger la confidentialité de ces données, conformément à la Sect. 5 de la Loi Fédérale Allemande sur la Protection des Données. L'Agent est également tenu de faire en sorte que ses employés s'engagent par écrit à respecter les dispositions statutaires en matière de protection des données, engagement qui doit être conservé dans les registres. À la demande du Commettant, l'Agent est tenu de fournir des preuves suffisantes de la satisfaction de ces obligations.</p>
<p><b>7. Technical and organizational measures</b></p>	<p><b>7. Mesures techniques et organisationnelles</b></p>

<p>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. This technical and organizational measures may be adjusted to technological developments. Any adjustments require the written consent of the Principal.</p>	<p>7.1 L'Agent s'engage à prendre (dans la mesure et dans les cadre des responsabilités qui lui sont attribuées par le Contrat Cadre) les mesures techniques et organisationnelles pour s'assurer du respect des dispositions applicables en matière de protection des données, en particulier des dispositions du présent contrat et des dispositions statutaires. Dans le cadre du traitement automatisé des Données d'AM, l'Agent s'engage, sous réserve d'autres instructions du Commettant, à prendre les mesures techniques et organisationnelles listées dans les Mesures de Contrôle de Sécurité de Base d'AM visées au présent contrat afin d'assurer le respect des prescriptions de la Sec. 9 de la Loi Fédérale Allemande sur la Protection des Données et de l'annexe de la Sec. 9 de la Loi Fédérale Allemande sur la Protection des Données. Ces mesures techniques et organisationnelles peuvent être adaptées aux évolutions technologiques. Toute révision de ces mesures requiert le consentement écrit du Commettant.</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 &amp; 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>7.2 En cas d'écart réel ou suspecté par rapport aux dispositions visées à la clause 7.1, en particulier pour toute violation de dispositions statutaires en matière de protection des données, ou en cas de défaillance, de problème ou de dysfonctionnements lors du traitement des Données d'AM ou encore en cas de perte, de vol ou de transfert illégal à des tiers, ainsi qu'en cas de divulgation illégale à des tiers, l'Agent sera tenu d'informer par écrit l'Agent chargé de la Conformité et de la Sécurité informatique du Commettant des détails de l'incident concerné (en particulier de la cause, de la date précise ainsi que de l'étendue de l'écart, des mesures déjà prises et des mesures encore à prendre, etc.) dans les plus brefs délais (c'est-à-dire dans les 24 heures suivant l'écart).</p>
<p>7.3 In cases of incidents in terms of</p>	<p>7.3 En cas d'incidents au sens de</p>

<p>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>l'article 7.2 du présent contrat, l'Agent prendra, dans les plus brefs délais, toute mesure nécessaire pour exclure et minimiser tout risque potentiel concernant l'intégralité et la confidentialité des Données d'AM, pour sauvegarder les Données d'AM et atténuer tout préjudice potentiel aux personnes concernées. L'Agent sera tenu de se coordonner avec le Commettant.</p> <p>7.4 Dans la mesure où le Commettant a des obligations au titre de la Sec. 42a de la Loi Fédérale Allemande sur la Protection des Données, à la première demande du Commettant, l'Agent aidera gratuitement le Commettant dans une mesure raisonnable.</p>
<p><b>8. Right of Control</b></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 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</p>	<p><b>8. Droit de Contrôle</b></p> <p>8.1 Le Commettant aura à tout moment un droit d'accès aux locaux commerciaux de l'Agent et sera affranchi de conditions de temps ou d'espace pour inspecter les mesures techniques et organisationnelles mises en place et le déroulement du traitement des données dans la société du Sous-traitant ainsi que pour vérifier la conformité de l'Agent aux dispositions statutaires et contractuelles applicables en matière de protection des données.</p> <p>8.2 L'Agent conférera au Commettant et à tout tiers désigné par le Commettant les droits d'accès, d'information et d'inspection nécessaires à l'audit susmentionné. Par conséquent, l'Agent donnera au Commettant ou aux tiers mandatés par le Commettant un accès illimité à toutes les installations de traitement des données, à tous les fichiers de données et à tous autres documents en vue de permettre l'inspection et l'examen de toutes les installations de traitement de données et de tous les fichiers de données et autres documents requis pour le traitement des</p>

<p>necessary for the review.</p> <p>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.</p> <p>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.</p>	<p>Données d'AM. L'Agent communiquera au Commettant et aux tiers mandatés par le Commettant toutes les informations nécessaires à cet audit.</p> <p>8.3 Le Commettant et l'Agent peuvent être soumis à un contrôle par des autorités publiques chargées de la protection des données, conformément aux dispositions de la Loi Fédérale Allemande sur la Protection des Données. À la demande du Commettant, l'Agent communiquera aux autorités publiques chargées de la protection des données toutes les informations souhaitées et autorisera des inspections de la même façon que les autorités publiques chargées de la protection des données sont autorisées à inspecter le Commettant. Ces inspections comprennent des inspections des locaux de l'Agent par les autorités publiques chargées de la protection des données ou par des personnes mandatées par ces dernières. Par conséquent, l'Agent confèrera aux autorités publiques chargées de la protection des données les droits d'accès, d'information et d'inspection nécessaires à ces inspections.</p> <p>8.4 En cas d'inspection ou de mesures prises par les autorités chargées de la protection des données conformément à la Sec. 38 de la Loi Fédérale Allemande sur la Protection des Données ou en cas d'enquêtes menées dans les locaux de l'Agent par les autorités chargées de la protection des données compétentes conformément aux Sec. 43 et 44 de la Loi Fédérale Allemande sur la Protection des Données, l'Agent en informera le Commettant dans les plus brefs délais.</p>
--	--

<p><b>9. Subcontracting to Third Parties</b></p> <p>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.</p> <p>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 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><b>9. Sous-traitance à un Tiers</b></p> <p>9.1 L'Agent ne pourra pas sous-traiter à un tiers le traitement ou l'utilisation de Données d'AM sauf si le Commettant a préalablement donné son consentement écrit. Ceci ne s'applique pas aux sociétés associées à l'Agent au sens des Sect. 15 et suivantes de la Loi Allemande sur les Sociétés par actions.</p> <p>9.2 Aux fins d'évaluer ce consentement et par conséquent pour le besoin d'information concernant la sous-traitance dans le cas d'une société associée à l'Agent, cette dernière doit communiquer au Commettant une copie du contrat de sous-traitance du traitement des données mandaté entre l'Agent et le tiers. En vertu de ce contrat, l'Agent soumettra par écrit le tiers aux mêmes obligations auxquelles l'Agent est soumis vis-à-vis du Commettant, conformément au contrat. Toutefois, le Commettant ne sera soumis à aucune obligation (si le consentement est nécessaire) de donner un tel consentement.</p> <p>9.3 L'Agent contrôlera régulièrement (au moins une fois par an) si un tiers sous-traité respecte les obligations qui lui incombent aux termes du contrat conclu entre l'Agent et le tiers, et communiquera au Commettant le rapport d'inspection écrit pertinent dans les plus brefs délais, après l'inspection en question du sous-traitant.</p>
<p><b>10. Rights of data subjects (persons affected)</b></p> <p>10.1 Data subjects affected by the data processing may exercise their rights vis-à-vis the Principal only.</p>	<p><b>10. Droits des personnes concernées</b></p> <p>10.1 Les personnes concernées par le traitement des données ne peuvent exercer leurs droits que vis-à-vis du Commettant.</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>10.2 Si les personnes concernées contactent l'Agent pour exercer leurs droits à l'information sur, à la correction, à l'effacement ou au verrouillage des données à caractère personnel les concernant, l'Agent transférera ces demandes au Commettant dans les plus brefs délais.</p> <p>10.3 Si une personne concernée exerce ses droits à l'information sur, à la correction, à l'effacement ou au verrouillage des Données d'AM ainsi que ses droits à l'information sur les Données d'AM conservées, sur la finalité de la conservation et sur les personnes et lieux auxquels les Données d'AM sont régulièrement transférées, l'Agent est tenu d'aider le Commettant à remplir ses obligations.</p>
<p><b>11. Information of Third Persons</b></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>	<p><b>11. Information de Tiers</b></p> <p>11.1 Si et dans la mesure où l'Agent est tenu de communiquer des informations concernant les Données d'AM à un tiers du fait d'une disposition statutaire impérative, l'Agent est, avant la communication d'une telle information, tenu d'informer le Commettant par écrit de l'identité du tiers, de la date de la communication et des informations spécifiques devant être communiquées.</p> <p>11.2 À l'exception du cas visé à l'article 11.1, l'Agent ne peut communiquer des informations sur les Données d'AM à des tiers qu'avec le consentement écrit et préalable du Commettant.</p>
<p><b>12. Return and Deletion of Data</b></p> <p>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</p>	<p><b>12. Restitution et Effacement des Données</b></p> <p>12.1 L'Agent doit complètement et irrévocablement effacer ou détruire toutes les Données d'AM rendues au Commettant, toutes les Données d'AM collectées ultérieurement,</p>

<p>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.</p> <p>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.</p> <p>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.</p>	<p>toutes les données résultant du traitement et de l'utilisation des Données d'AM, ainsi que toutes les données associées au contrat dès que la connaissance de ces données n'est plus requise pour l'atteinte de l'objectif poursuivi par leur conservation et au plus tard après l'exécution du ou des service(s) couvert(s) par le Contrat Cadre (en particulier après l'annulation ou toute autre résiliation du Contrat Cadre). La présente clause s'applique également à toute duplication des Données d'AM (notamment aux sauvegardes aux fins d'archivage et de sécurité) sur l'un des systèmes de l'Agent ainsi qu'aux données de test, aux données jetées, aux notifications, aux notes, aux projets et aux copies.</p> <p>12.2 À la demande du Commettant, l'Agent sera tenu de mettre à disposition de ce dernier, dans les plus brefs délais, le protocole relatif à l'effacement ou à la suppression des Données d'AM.</p> <p>12.3 La documentation requise pour prouver le traitement des données conformément aux dispositions contractuelles et légales sera conservée par l'Agent après l'exécution du présent contrat pour la durée de la période de conservation spécifique prévue.</p>
---	--

<p><b>13. Final provisions</b></p> <p>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>	<p><b>13. Dispositions finales</b></p> <p>La durée du Traitement des Données Mandaté dépendra des dispositions relatives à la durée du Contrat Cadre. Toute modification, tout avenant à et toute résiliation du présent contrat seront faits par écrit. Ceci s'applique également à toute modification de la présente disposition. Si une disposition du présent contrat était ou devenait nulle ou incomplète, la validité des autres dispositions du présent Contrat n'en serait pas affectée. Les parties s'engagent à adopter en lieu et place de la disposition nulle une disposition juridiquement contraignante dont la finalité commerciale sera la plus proche possible de celle de la disposition partiellement nulle ou incomplète.</p>
---	---

\_\_\_\_\_  
Place, Date / Lieu, Date

\_\_\_\_\_  
Place, Date / Lieu, Date

\_\_\_\_\_  
Signature (Commettant)

\_\_\_\_\_  
Signature (Commettant)

**Annexe 1: Finalité, type et étendue du traitement des données, type de données et personnes concernées / Appendix 1: Purpose, type and extent of data processing, type of data and affected persons**

<b>1. Finalité du Traitement de Données / Purpose of Data Processing</b>
<b>2. Type et étendue du Traitement de Données / Type and Extent of Data Processing</b>
<b>3. Type de Données / Type of Data</b>
<b>4. Personnes Concernées / Affected Individuals</b>

## **ANNEXE VI**

NB : Pour des raisons de sécurité, la présente ANNEXE VI sera laissée en blanc dans la version publiée à l'extérieur d'ArcelorMittal. Cette ANNEXE VI sera incluse dans la copie de la Procédure postée sur l'Intranet.

Correspondants à la Protection des Données

Dernière version mise à jour de cette liste : <http://www.....> Intranet d'Arcelormittal

Agents chargés de la CSI

Dernière version mise à jour de cette liste : <http://www.....> Intranet d'Arcelormittal

## **ANNEXE VII**

Questionnaire d'Audit

### **Audit de Conformité de la Protection des Données**

#### **Liste de vérification**

Nom de l'Application Logicielle/de la Base de Données

Finalité(s) de l'Application

Nom/Département de la personne responsable de cette Application

- . aspects informatiques
- . aspects fonctionnels

Qui sont les Personnes Concernées ?

(tous les employés d'AM ? ou une catégorie particulière des employés d'AM ? des clients d'AM ?...)

Combien de Personnes Concernées comprend cette procédure ?  
(approximativement)

Quelles Données à Caractère Personnel comprend cette procédure ?  
(captures d'écran)

Y-a-t-il des données sensibles ?

D'où proviennent les données ?

(En d'autres termes, quelle(s) est (sont) la (les) source(s) des données ?) Directement des Personnes Concernées ? ou d'autres sources ?

Pendant combien de temps les données vont-elles être conservées ?

Qui a accès aux données ?

- . au sein d'AM
- . en dehors d'AM

Accès aux données : D'où ? Existe-t-il un transfert transfrontalier de données ?

Les données sont-elles migrées vers/utilisées par une autre Application ?

Si oui : quelle Application ?

Droit d'accès des Personnes Concernées à leurs données : comment informez-vous les Personnes Concernées de leur droit d'accès ?

Est-ce qu'un tiers (au sein d'AM ou en dehors d'AM) participe à la procédure ?

Si oui : à quelle fin (par exemple aux fins d'hébergement de données...) ?

L'Application a-t-elle été notifiée (le cas échéant) ?

Quelles mesures de sécurité sont en place ?

Dernière version mise à jour de ce Questionnaire : <http://www.....> Intranet d'Arcelormittal

## **ANNEXE VIII**

### **Description du Traitement des Données**

#### **Catégories de Données**

Données RH

Données Commerciales

Données Informatiques

Données en matière de Responsabilité Sociale

Données en matière de Santé et de Sécurité

#### **Personnes Concernées**

La majorité des Personnes Concernées dont les données sont traitées sont des employés d'ArcelorMittal.

En dehors des employés d'ArcelorMittal, les Personnes Concernées dont les données sont traitées par ArcelorMittal sont :

- . des représentants de clients (ArcelorMittal participe à des activités de « B2B » (commerce interentreprises) sans particulier dans son portefeuille de clients)
- . des représentants de fournisseurs
- . des prestataires travaillant pour le compte d'ArcelorMittal
- . des parties prenantes locales

#### **Données RH**

Finalités du transfert/ traitement

Ressources Humaines et Gestion de Personnel, y compris le recrutement, les services de paie, la gestion des carrières et des compétences, la formation (e-learning), la gestion des avantages sociaux des employés, l'évaluation de la performance des employés, la tenue des annuaires des employés et le respect des prescriptions légales en vigueur.

**Données Commerciales** (les Données à Caractère Personnel liées aux Clients, aux Fournisseurs ou aux partenaires commerciaux de toute nature).

Les personnes sont identifiées en tant que contacts d'ArcelorMittal au sein d'une société, représentant cette société.

#### Finalités du transfert/traitement

Exécution et Gestion de Procédés Commerciaux, notamment les activités commerciales, les activités d'achat, la comptabilité et le contrôle, la gestion d'actifs de sociétés, dans le respect des prescriptions légales en vigueur.

**Gestion d'infrastructures informatique**, notamment les e-mails, l'accès à l'Intranet d'ArcelorMittal, l'utilisation d'outils collaboratifs et, de manière plus générale, la gestion des accès des utilisateurs aux applications informatiques ;

#### **Données en matière de Responsabilité Sociale**

##### Finalité du transfert/traitement

Responsabilité Sociale, notamment avoir une compréhension de notre environnement opérationnel et des préoccupations des parties prenantes concernées, gérer le programme continu d'engagement vis-à-vis des communautés locales d'ArcelorMittal.

#### **Données en matière de Santé et de Sécurité**

##### Objet du transfert/traitement

Les procédures en matière de santé et de sécurité sont des activités visant à assurer la sécurité et la protection des travailleurs et des ressources d'ArcelorMittal. Ces activités incluent la protection de la santé et de la sécurité au travail et l'authentification du statut des travailleurs pour leur autoriser l'accès aux ressources et aux installations d'ArcelorMittal.

## **ANNEXE IX**

NB : Pour des raisons de sécurité, la présente ANNEXE IX sera laissée en blanc dans la version publiée à l'extérieur d'ArcelorMittal. Cette ANNEXE IX sera incluse dans la copie de la Procédure postée sur l'Intranet.

### **Comité de Protection des Données**

Les membres initiaux du Comité de Protection des Données désignés par le Directeur Juridique du Groupe sont

. [En nommer 2]

Les membres initiaux du Comité de Protection des Données désignés par le Vice-président des Ressources Humaines sont

. [En nommer 2]

Le secrétaire général initial est : Emmanuel CAUVIN