Date : **15 Janvier 2015**

REGLES CONTRAIGNANTES D'ENTREPRISE DE ENGIE

Table des matières

1 Introduction

ENGIE SA[1] (« ENGIE SA ») et les entités de ENGIE[2] énumérées en Annexe 1 dans ses versions amendées successives (les « Filiales de ENGIE ») (collectivement dénommées « Groupe ENGIE ») doivent, dans le cadre de leurs activités, traiter des Données à caractère personnel concernant leurs employés et autres membres du personnel assimilés (comme les postulants, etc.) (les « Personnes Concernées »).

Conscient de l'importance de la Protection des Données, le Groupe ENGIE s'est engagé à protéger les Données à caractère personnel des Personnes Concernées et à garantir le respect des législations sur la Protection des Données à caractère personnel applicables dans les pays où le Groupe ENGIE est présent.

À cette fin, le Groupe ENGIE a déjà établi des normes de Protection des Données uniformes et adéquates pour les Traitement des Données à caractère personnel des Personnes Concernées, en adoptant la Politique Groupe de Protection des Données à caractère personnel (voir Annexe 2) le 20 janvier 2014.

Les présentes Règles Contraignantes d'Entreprise (ou Binding Corporate Rules « BCR ») ont pour objectif de compléter la Politique Groupe de Protection des Données à caractère personnel et la Charte Éthique afin de garantir un niveau de protection adéquat aux transferts et Traitements associés des Données à caractère personnel des Personnes Concernées au sein du Groupe ENGIE, et afin de faciliter les transferts des données dans tout le Groupe, conformément aux dispositions légales applicables, en particulier celles énoncées dans la Directive européenne 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Toutes les entités au sein du Groupe ENGIE et leurs directeurs, responsables et employés s'engagent à respecter en tout temps les présentes BCR lorsqu'ils collectent, utilisent, transmettent et traitent des données à caractère personnel se rapportant à une Personne Concernée.

Ces BCR sont communiquées à tous les employés du Groupe ENGIE [en particulier par l'Intranet et par note interne] et sont disponibles sur le site Web de ENGIE à l'adresse suivante : www.engie.com.

Pour toutes les questions relatives à ces BCR ou à vos droits dans le cadre des BCR, ou pour toute autre question en matière de Protection des Données à caractère personnel, veuillez contacter le Délégué Groupe aux Données Personnelles à l'adresse ci-dessous :

privacy@engie.com.

[1] « ENGIE SA », est la nouvelle dénomination sociale du Groupe GDF SUEZ SA
[2] ENGIE est le nouveau nom de GDF SUEZ

2 Définitions

Aux fins des présentes BCR, les termes et expressions commençant par une majuscule auront le sens qui leur est attribué ci-dessous, étant précisé que, indépendamment des définitions ci-dessous, les termes des présentes BCR seront en tout état de cause interprétés conformément à la législation européenne applicable, c'est-à-dire à la date d'exécution de ces BCR, à la Directive européenne 95/46/CE du 24 octobre 1995.

« **Autorité de Protection des Données** » désigne une autorité indépendante nationale notamment chargée de vérifier le respect des lois sur la Protection des Données applicables dans son pays. Une liste des Autorités de Protection des Données est disponible sur la page Web http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

« **Comité des Données à Caractère Personnel** » (« **Comité DCP** ») désigne le Comité créé en vertu de la Politique Groupe de Protection des Données à caractère personnel de ENGIE, qui a pour objectif de mener des activités visant à promouvoir et/ou garantir l'application de la Politique Groupe de Protection des Données à caractère personnel de ENGIE.

« **Délégué Groupe aux Données Personnelles** » désigne la personne nommée au sein de ENGIE SA, responsable de la Protection des Données à caractère personnel au niveau du Groupe ENGIE, afin de définir et transmettre les bonnes pratiques relatives à la Protection des Données à caractère personnel, et de garantir leur mise en œuvre.

« **Délégué à la Protection des Données personnelles**» (« **DPD »**) désigne la personne nommée par une Filiale de ENGIE ou une Branche de ENGIE comme la personne qui conseille le Responsable de Traitement et vérifie que les lois sur la Protection des Données sont respectées.

« **Données** » ou « **Données à caractère personnel** » désigne toute information relative à une personne identifiée ou identifiable. Une personne est réputée identifiable, directement ou indirectement, en particulier par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques à son identité physique, physiologique, psychique, économique, culturelle ou sociale. Les Données à caractère personnel soumises à ces BCR sont des « Données de RH » comme défini ci-dessous.

- « **Données de RH** » désigne toute Donnée à caractère personnel relative à des Personnes Concernées au sens de membres du personnel, à savoir les employés, les postulants, les stagiaires, les travailleurs temporaires ou les employés retraités de toute Filiale de ENGIE ;

« **Données Sensibles »** désigne toutes Données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat, ainsi que les Données relatives à la santé ou à la vie sexuelle.

« **EEE »** désigne l'Espace Économique Européen.

« Exportateur des données » ou « Exportateur » désigne le Responsable de Traitement établi dans l'EEE qui transfère des Données à caractère personnel.

« **Filiale(s) de ENGIE** » désigne les entités juridiques dans le périmètre de consolidation du Groupe (consolidation intégrale) comme indiqué en Annexe 1 jointe aux présentes dans ses versions amendées successives en vertu de l'Article 13 ci-dessous.

« **Groupe ENGIE »** désigne ENGIE SA et toutes les Filiales de ENGIE.

« Importateur des Données » ou « Importateur » désigne, si le contexte l'exige : (i) le Responsable de Traitement qui accepte de recevoir de l'Exportateur des Données des Données à caractère personnel en vue d'un Traitement ultérieur conformément aux clauses des présentes BCR ou (ii) le Sous-Traitant qui accepte de recevoir du l'Exportateur des Données, des Données à caractère personnel devant être traitées pour le compte de l'exportateur des données - après leur transfert - conformément à ses instructions et aux clauses des présentes BCR.

« **Personne Concernée** » désigne une personne identifiée ou identifiable dont les Données à caractère personnel font l'objet d'un Traitement, quelle que soit sa nationalité.

« **Politique Groupe de Protection des Données à caractère personnel de ENGIE** » désigne les principes et les objectifs, et l'organisation et le système de suivi qui ont été mis en œuvre,, ainsi que les rôles et responsabilités en matière de Protection des Données à caractère personnel, indiqués en Annexe 2.

« **Protection des Données** » ou « **Protection des Données à caractère personnel** » désigne l'ensemble des mesures, activités, méthodes, processus, organisations, etc. visant à protéger les Données à caractère personnel et à garantir le respect des lois et réglementations applicables en matière de Protection des Données à caractère personnel.

« **Responsable de Traitement des Données** » ou « **Responsable de Traitement** » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine seul ou conjointement avec d'autres personnes les finalités et les moyens de Traitement des Données à caractère personnel.

« Sous-Traitant des données » ou « Sous-Traitant » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des Données à caractère personnel pour le compte du Responsable de Traitement.

« **Tiers** » désigne toute personne physique ou morale qui n'est pas une Personne Concernée, y compris toute autorité publique, tout service ou tout organisme autre que ENGIE SA et les Filiales de ENGIE.

« **Traitement des Données** », « **Traitement** » ou « **Traité** » désigne toute opération ou ensemble d'opérations manuelles et/ou automatisées, effectuées ou non à l'aide de procédés automatiques, sur des Données à caractère personnel, comme la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition ou de transfert, l'alignement ou la combinaison, le verrouillage, l'effacement ou la suppression. Le Traitement des Données et ses finalités qui entrent dans le périmètre des présentes BCR sont définis plus en détail en Annexe 3.

3 Champ d'application des BCR et liens avec les lois nationales applicables

3.1 Les présentes BCR visent à garantir un niveau de protection adéquat et à fournir des garanties de protection appropriées au sens des Articles 25 et 26 de la Directive européenne 95/46/CE du 24 octobre 1995 (« la Directive européenne ») dans tout le Groupe ENGIE comme défini en Annexe 1, pour toutes les catégories de Données à caractère personnel et pour tous les transferts et Traitements associés spécifiés en Annexe 3 conformément aux finalités énoncées dans ladite Annexe.

3.2 Les présentes BCR s'appliquent par conséquent à tous les transferts et au Traitement des Données à caractère personnel des Personnes Concernées au sein du Groupe ENGIE qui sont ou ont été soumises à la Directive européenne et, plus précisément, à toutes les Données à caractère personnel des Personnes Concernées :

- qui sont collectées et Traitées dans l'Espace Économique Européen (EEE) par ENGIE SA et/ou l'une des Filiales de ENGIE ayant son siège social dans l'EEE ;

- qui sont Traitées par l'une des Filiales de ENGIE ayant son siège social dans l'EEE, dans la mesure où les Données à caractère personnel sont collectées et transférées ou mises à disposition ultérieurement par ENGIE SA et/ou l'une des Filiales de ENGIE ayant son siège social dans l'EEE ;

- qui sont collectées en dehors de l'EEE par l'une des Filiales de ENGIE ayant son siège social en dehors de l'EEE et qui sont transférées ou mises à disposition par le destinataire de la collecte à ENGIE SA et/ou l'une des Filiales de ENGIE ayant son siège social dans l'EEE à des fins de Traitement, que ce Traitement ayant lieu dans l'EEE implique ou non le transfert ultérieur des Données à caractère personnel au destinataire de la collecte dont le siège social se situe en dehors de l'EEE.

Les présentes BCR ne couvrent pas les Données à caractère personnel Traitées exclusivement en dehors de l'EEE. Le Traitement de Données à caractère personnel collectées en dehors de l'EEE par l'une des filiales de ENGIE ayant son siège social en dehors de l'EEE, qui ne sont pas transférées ultérieurement dans l'EEE, en tout ou partie, est soumis uniquement à la loi nationale sur la Protection des Données qui est applicable dans le pays où les données sont Traitées.

3.3 Chaque Exportateur et/ou Importateur des données dans le Groupe ENGIE doit s'assurer que les transferts et le Traitement des Données à caractère personnel des Personnes Concernées sont conformes aux présentes BCR et, en tout état de cause, à la législation en vigueur comme mentionné à l'Article 4 de la Directive européenne 95/46/CE du 24 octobre 1995 et à toute législation locale pertinente. Chaque Exportateur et/ou Importateur de Données s'engage, si les Données à caractère personnel comprennent des Données Sensibles, à prévoir des garanties supplémentaires similaires à celles prévues par la Directive européenne 95/46/CE du 24 octobre 1995, comme spécifié dans l'Article 4.1(c) ci-dessous.

3.4 Si la législation locale exige un plus haut niveau de Protection des Données à caractère personnel, la législation locale applicable prévaudra sur les BCR. Dans le cas inverse, si la législation locale prévoit un niveau de Protection des Données à caractère personnel plus faible que celui qui est prévu par les présentes BCR, les dispositions des BCR s'appliquent.

3.5 Si une Filiale de ENGIE a un motif raisonnable d'estimer que la législation locale applicable l'empêche d'exécuter ses obligations en vertu des présentes BCR et altérera les garanties prévues en vertu des présentes BCR à l'égard des Personnes Concernées, elle doit immédiatement en informer ENGIE SA et le Délégué Groupe aux Données Personnelles, sauf si une autorité chargée de l'exécution des lois l'interdit. Dans de tels cas, ENGIE SA et/ou le Délégué Groupe aux Données Personnelles décideront de l'action à entreprendre et consulteront, en cas de doute, l'Autorité de Protection des Données compétente.

3.6 Caractère contraignant des BCR à l'égard des entités et des employés :

Les présentes BCR s'appliquent à toutes les Entités du Groupe ENGIE qui ont signé l'Accord de Groupe prévoyant leur adhésion aux BCR et lient chacune desdites Entités ainsi que leurs employés respectifs. L'Annexe 1 présente la liste des Entités pour lesquelles l'approbation des BCR est requise.

À cette fin, chaque Entité doit garantir l'application de ces BCR, en respectant la Charte Ethique du Groupe et, le cas échéant, le ou les dispositifs suivants qui doivent être mis en œuvre conformément au droit du travail applicable :

- le règlement interne,
- toute disposition du contrat de travail,

- toute autre disposition visant à rendre les BCR applicables à ses employés.

4 Principes régissant la Sous-Traitance et les transferts de Données à caractère personnel

4.1 Pour garantir aux Personnes Concernées un niveau de protection adéquat et équivalent dans tout le Groupe ENGIE au sens des Articles 25 et 26 de la Directive européenne 95/46/CE du 24 octobre 1995, ENGIE SA et les Filiales de ENGIE s'engagent à appliquer et à respecter de manière stricte, et doivent s'assurer que les directeurs, responsables et employés respectifs appliquent et respectent de manière stricte les principes énoncés ci-dessous lors du Traitement et du transfert de Données à caractère personnel comme défini ci-dessus et en Annexe 3 à titre indicatif.

(a) Caractère légal et loyal du Traitement et légitimité des finalités du Traitement

Les Données à caractère personnel doivent être collectées, transférées et Traitées de manière loyale et licite, à savoir d'une manière transparente et à des fins déterminées, explicites et légitimes. Les Données à caractère personnel ne doivent pas être utilisées, transférées ou Traitées ultérieurement, y compris par des Importateurs de Données agissant en tant que Responsables de Traitement, d'une manière incompatible avec les finalités initiales.

En conséquence :

(i) la Personne Concernée doit recevoir toutes les informations requises en vertu de la législation nationale applicable en matière de Protection des Données en ce qui concerne le Traitement de ses Données à caractère personnel, comme spécifié dans l'Article 5.1 ci-dessous ;

(ii) le cas échéant, en vertu de la loi locale applicable sur la Protection des Données, le Traitement doit être notifié à l'Autorité de Protection des Données compétente ; et

(iii) le Traitement des Données à caractère personnel doit reposer sur l'un des motifs légaux suivants :

- le consentement explicite de la Personne Concernée par le Traitement ; ou
- le respect d'une obligation légale à laquelle est soumis le Responsable de Traitement; ou
- l'exécution d'un contrat auquel la Personne Concernée est partie ou avant la conclusion d'un contrat à la demande de la Personne Concernée ; ou
- la protection des intérêts vitaux de la Personne Concernée ; ou

- l'exécution d'une mission d''intérêt public ou relevant de l'exercice d'une autorité publique dont est investi le Responsable de Traitement ou le(s) destinataire(s) des Données à caractère personnel ; ou

- la réalisation de l'intérêt légitime du Responsable de Traitement ou du destinataire des Données, à condition qu'elle ne soit pas incompatible avec les intérêts ou les droits et libertés individuels fondamentaux de la Personne Concernée..

(b) Pertinence et proportionnalité des Données à caractère personnel Traitées

Les Données à caractère personnel collectées, transférées ou Traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs Traitements ultérieurs. Les Données à caractère personnel doivent être exactes, complètes et actualisées si nécessaire.

La durée de conservation des Données à caractère personnel Traitées doit être définie selon la finalité prévue de la collecte, du transfert et du Traitement des Données à caractère personnel. Les Données à caractère personnel doivent être conservées sous une forme permettant l'identification des Personnes Concernées pendant une durée qui n'excède pas la période nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et Traitées ultérieurement.

Si les Données à caractère personnel collectées ne sont plus nécessaires aux fins de leur Traitement, lesdites Données doivent être effacées ou rendues anonymes, comme requis par la législation locale applicable en matière de Protection des Données.

(c) Garanties supplémentaires applicables aux Données Sensibles

Les Données Sensibles ne doivent pas être collectées, transférées et/ou Traitées, sauf si ce Traitement repose sur un motif légal, notamment :

(i) si la Personne Concernée a donné son consentement exprès et explicite (excepté si la loi locale applicable l'interdit) ; ou

(ii) si la loi locale applicable autorise spécifiquement les circonstances dans lesquelles les Données Sensibles doivent être collectées, transférées et/ou Traitées, notamment dans les cas suivants :

- si le Traitement est nécessaire aux fins d'exécution des obligations et des droits spécifiques du Responsable de Traitement en matière de droit du travail, dans la mesure où la loi locale l'autorise en prévoyant des garanties adéquates ;

- si le Traitement est nécessaire à la protection des intérêts vitaux de la Personne Concernée ou d'une autre personne si la Personne Concernée est dans l'incapacité physique ou légale de donner son consentement ; ou

- si le Traitement concerne des Données à caractère personnel qui sont manifestement rendues publiques par la Personne Concernée ;

- si le Traitement est nécessaire à l'introduction, l'exécution ou la défense d'une action légale ; ou

- si le Traitement est effectué dans le cadre d'activités légitimes par une fondation, une association ou tout autre organisme à but non lucratif dont l'objet est politique, philosophique, religieux ou syndical, sous réserve de garanties appropriées fournies à cette fin et à condition que le Traitement concerne uniquement les membres ou les personnes ayant des contacts réguliers avec cet organisme et que les Données à caractère personnel ne soient pas divulguées à un tiers sans le consentement explicite de la Personne Concernée ; ou

- si le Traitement des Données Sensibles est nécessaire aux fins de la médecine préventive, du diagnostic médical, de l'administration de soins ou de traitements ou de la fourniture de services de santé, et doit être effectué dans des lieux où lesdites Données Sensibles sont traitées par un professionnel de la santé ou toute autre personne tenue au secret professionnel ou soumise à une obligation de secret équivalente en vertu du droit ou de la réglementation émanant d'autorités compétentes.

(d) Règles spécifiques applicables aux décisions individuelles automatisées

Une évaluation ou une décision concernant les Personnes Concernées ayant des conséquences significatives sur celles-ci ne peut en aucun cas être basée uniquement sur le Traitement automatisé de leurs Données à caractère personnel, sauf si cette décision :

(i) est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat présentée par la Personne Concernée ait été satisfaite ou à condition que les mesures appropriées, comme des dispositions lui permettant de présenter ses observations, soient prises afin de préserver ses intérêts légitimes ; ou

(ii) est autorisée par une loi qui fixe également des mesures de sauvegarde des intérêts légitimes de la Personne Concernée.

(e) Obligations de sécurité et de confidentialité

Le Groupe ENGIE doit protéger les Données à caractère personnel des Personnes Concernées contre tout accès non autorisé et accidentel, tout Traitement illégal, toute divulgation involontaire ou illégale, toute perte, toute destruction ou tout dommage. Par conséquent, le Groupe ENGIE s'engage à mettre en œuvre des mesures de protection et, en particulier, des mesures de sécurité physiques, techniques et organisationnelles visant à garantir de manière adéquate la sécurité et la confidentialité des Données à caractère personnel des Personnes Concernées.

Ces mesures dépendent du risque existant, des conséquences potentielles sur la Personne Concernée, du niveau de sensibilité des Données à caractère personnel, de la technologie disponible et de l'état de la technique dans les pays où ENGIE SA ou l'une des Filiales de ENGIE est établie.

Les mesures de sécurité mises en œuvre au niveau du Groupe ENGIE sont notamment définies dans les politiques et les normes de sécurité relatives aux Systèmes d'Information énoncées en Annexe 4.

Les incidents de sécurité doivent être gérés conformément aux règles indiquées dans la Politique de Protection des Données à caractère personnel.

(f) Transferts de données aux Sous-Traitant

Dès que ENGIE ou l'une des Filiales de ENGIE, agissant en tant que Responsable de Traitement, a recours à un Sous-Traitant pour le Traitement des Données à caractère personnel de Personnes Concernées, dans ou hors du périmètre du groupe ENGIE, ladite Filiale de ENGIE doit s'assurer que, avant le transfert des Données à caractère personnel à tout Sous-Traitant, celui-ci fournit des garanties suffisantes quant aux mesures de sécurité techniques et organisationnelles régissant le Traitement, et doit s'assurer que le Sous-Traitant sélectionné respecte ces mesures.

Par conséquent, le contrat devant être conclu avec le Sous-Traitant sélectionné comprendra une clause similaire à la clause type prévue en Annexe 5 qui stipule que le Sous-Traitant doit agir uniquement sur les instructions du Responsable de Traitement et doit appliquer les règles permettant de garantir la sécurité et la confidentialité qui incombent au Sous-Traitant.

Si le Sous-Traitant a son siège social en dehors de l'EEE et n'est pas une Filiale de ENGIE, le contrat avec ledit Sous-Traitant doit inclure les dernières clauses contractuelles types approuvées par la Commission européenne, qui régissent les transferts de Données à caractère personnel par un Responsable de Traitement vers un Sous-Traitant, sauf si le transfert fait l'objet d'une dérogation accordée en vertu de la loi

locale applicable sur la Protection des Données ou si le transfert est effectué vers un Sous-Traitant ayant la certification américaine Safe Harbor en matière de transfert de Données à caractère personnel ou ayant son siège social dans un pays offrant un niveau de protection approprié selon l'avis de la Commission européenne. Dans tous les cas, ces transferts doivent respecter la Directive européenne 95/46/CE du 24 octobre 1995, en particulier ses articles 25 et 26 sur les flux transfrontaliers de données.

(g) Restrictions concernant les transferts et les transferts ultérieurs à un Responsable de Traitement n'appartenant pas au Groupe ENGIE

Dans tous les transferts et les transferts ultérieurs de Données à caractère personnel à un Tiers agissant en tant que Responsable de Traitement ayant son siège social en dehors de l'EEE, le contrat avec ledit Responsable de Traitement doit inclure les dernières clauses contractuelles types approuvées par la Commission européenne, qui régissent les transferts de Données à caractère personnel par un Responsable de Traitement à un autre Responsable de Traitement, et doit être signé par toutes les parties concernées, sauf si le transfert fait l'objet d'une dérogation accordée en vertu de la loi locale applicable sur la Protection des Données ou si le transfert est destiné à un Responsable de Traitement ayant la certification américaine Safe Harbor en matière de transfert de Données à caractère personnel ou ayant son siège social dans un pays offrant un niveau de protection approprié selon l'avis de la Commission européenne. Dans tous les cas, ces transferts doivent respecter la Directive européenne 95/46/CE du 24 octobre 1995, en particulier ses articles 25 et 26 sur les flux transfrontaliers de données.

5 Information et droits des Personnes Concernées

5.1 Information des Personnes Concernées

(a) Pour que toutes les Personnes Concernées impliquées soient informées de l'existence et du contenu des présentes BCR et en complément des sessions de formation qui seront fournies aux employés du Groupe ENGIE comme indiqué dans l'Article 7 ci-dessous, chaque entité du Groupe ENGIE s'engage :

(i) à communiquer ces BCR, y compris toute version actualisée, à tous les employés de leur Business Unit (BU) en particulier par l'Intranet et par note interne, et

(ii) à mettre à disposition ces BCR au moins sur le site Web de ENGIE à l'adresse suivante : www.engie.com.

(b) Chaque entité du Groupe ENGIE s'engage également à fournir aux Personnes Concernées, avant tout Traitement de leurs Données à caractère personnel, toute

information pouvant être nécessaire en vertu de la loi locale applicable sur la Protection des Données et, dans tous les cas, au moins l'ensemble des informations suivantes :

(i) l'identité du (des) Responsable(s) de Traitement et de son (ses) représentant(s) le cas échéant ;

(ii) les finalités prévues du Traitement des Données à caractère personnel ; et

(iii) dans la mesure où ces informations sont nécessaires, compte tenu des circonstances particulières nécessitant la collecte de Données à caractère personnel, la garantie d'un traitement loyal à l'égard de la Personne Concernée, et toute autre information suivante :

- les destinataires ou catégories de destinataires auxquels sont adressées les Données à caractère personnel,

- l'existence d'un droit d'accès à et d'un droit de modification de ses Données à caractère personnel comme spécifié dans l'Article 5.2 ci-dessous.

(c) Ces informations peuvent être mises à la disposition de la Personne Concernée sur le site Web de ENGIE et/ou sur le site Web de toute Filiale de ENGIE concernée, et/ou dans les politiques et chartes appropriées, et/ou dans les contrats conclus avec la Personne Concernée impliquée dans le Traitement des Données à caractère personnel de la Personne Concernée et/ou par tout autre moyen approprié (correspondance, note d'information, etc.).

(d) Si les Données à caractère personnel ne sont pas fournies directement par la Personne Concernée en question, l'obligation d'informer la Personne Concernée ne s'appliquera pas dans la mesure où l'information se révèle impossible ou implique des efforts disproportionnés à cet égard, ou si l'enregistrement ou la communication des données est expressément autorisée par la (les) loi(s) applicable(s).

5.2 **Droit d'accès, de rectification, de d'effacement, de verrouillage des Données à caractère personnel et droit d'opposition au traitement des Données à caractère personnel**

Chaque entité du Groupe ENGIE reconnaît aux Personnes Concernées les droits suivants :

(a) le droit d'obtenir sans limitations, à intervalles raisonnables, et sans délai ou frais excessifs, une copie de leurs Données à caractère personnel Traitées ;

(b) le droit d'obtenir la rectification, l'effacement ou le verrouillage de leurs Données à caractère personnel, en particulier si leurs Données sont incomplètes ou inexactes ;

(c) le droit de s'opposer, à tout moment et pour des motifs impérieux légitimes et pertinents, au Traitement de leurs Données à caractère personnel, sauf si ledit Traitement est exigé par la loi. Si l'objection est justifiée, le Traitement doit être arrêté ;

(d) le droit de s'opposer, sur demande et gratuitement, au Traitement de leurs Données à caractère personnel à des fins de prospection.

Les droits susmentionnés peuvent être exercés par les Personnes Concernées conformément à la procédure prévue dans la note d'information transmise par ENGIE SA ou par toute Filiale de ENGIE concernée qui est impliquée dans le Traitement.

6 Droits des Tiers bénéficiaires

Les Personnes Concernées ayant subi un préjudice suite à une violation des présentes BCR peuvent, en tant que Tiers bénéficiaires de ces BCR, exercer leurs droits en vertu des présentes règles et présenter leur dossier à l'Autorité de Protection des Données compétente ou au tribunal dont dépend le siège social de la Filiale Exportatrice des données dans l'EEE conformément à l'Article 10 ci-dessous.

Les principes que les Personnes Concernées peuvent faire appliquer sont les suivants :

- Légalité et loyauté du Traitement et légitimité des finalités du Traitement (voir article 4(a) ci-dessus) ;
- Pertinence et proportionnalité des Données à caractère personnel Traitées (voir article 4(b) ci-dessus) ;
- Garanties supplémentaires applicables aux Données Sensibles (voir article 4(c) ci-dessus) ;
- Règles spécifiques applicables aux décisions individuelles automatisées (voir article 4(d) ci-dessus) ;
- Obligations de sécurité et de confidentialité (voir article 4(e) ci-dessus) ;
- Règles spécifiques applicables aux transferts de Données aux Sous-Traitant ou aux transferts et transferts ultérieurs à un Responsable de Traitement n'appartenant pas au Groupe ENGIE (voir article 4(g) et 4(f) ci-dessus) ;
- Transparence et facilité d'accès aux BCR (voir article 5.1 des BCR GDF) ;

- Droits d'accès, de rectification, d'effacement, de verrouillage des données et d'opposition au traitement (voir article 5.2) ;

- Règles dans le cas où une législation nationale empêche l'application des BCR (voir article 3.5) ;

- Droit de réclamation au moyen du mécanisme de réclamation interne (voir article 9) ;

- Obligation de coopérer avec les Autorités de Protection des Données (voir articles 8.2(a)(v) ; 8.2(b)(iv) ; 8.2(c) et 12) ;

- Principes de responsabilité et droits des tiers bénéficiaires (voir articles 6 et 10).

7 Formation

7.1 Tout le personnel au sein du Groupe ENGIE et, plus particulièrement, les employés qui ont accès aux Données à caractère personnel en permanence ou régulièrement, ou qui sont impliqués dans la collecte de Données à caractère personnel, dans le développement ou l'acquisition d'outils utilisés pour traiter les Données, doivent être formellement informés du contenu des présentes BCR et, plus généralement, des sujets abordés, à savoir les questions juridiques et de sécurité.

7.2 Des campagnes mondiales de sensibilisation et des sessions de formation appropriées (sur site ou par des séminaires Web) seront réalisées par ENGIE SA au niveau du Groupe ENGIE. Des actions locales seront également menées par les Filiales de ENGIE en complément de ces campagnes et sessions de formation.

7.3 Une formation spécifique des Délégués à la Protection des Données (DPD) sera réalisée selon les mêmes principes.

7.4 Toutes ces actions, au niveau du Groupe ou au niveau local, doivent être coordonnées par le Délégué Groupe aux Données Personnelles et le(s) Délégué(s) local (locaux) aux Données Personnelles.

8 Contrôle de l'application des BCR

8.1 Gouvernance

(a) Au niveau du Groupe ENGIE

Le pilotage stratégique des présentes BCR est placé sous la responsabilité du Comité de Direction Générale de ENGIE qui en délègue la coordination et le pilotage opérationnel à

son Secrétaire Général. Ce dernier délègue cette responsabilité au Délégué Groupe aux Données Personnelles qui porte pour la France la fonction de Correspondant Informatique et Libertés.

Toute difficulté d'exécution des présentes BCR doit être signalée au Délégué Groupe aux Données Personnelles.

(i) Le Délégué Groupe aux Données Personnelles

Le Délégué Groupe aux Données Personnelles a principalement les responsabilités suivantes :

- vérification du respect des présentes BCR et de toute politique obligatoire applicable, y compris la Politique de Protection des Données à caractère personnel, et conseil/avertissement du Conseil d'administration concernant les risques associés ;
- réception de notifications des DPD concernant les réclamations de Personnes Concernées et le traitement de problèmes majeurs en matière de Protection des Données à caractère personnel ;
- transmission de comptes rendus annuels sur le respect des présentes BCR au Comité des Données à Caractère Personnel ;
- représentation du Groupe ENGIE dans ce domaine avec les parties intéressées et organisations externes, y compris dans le cadre d'investigations par des Autorités de Protection des Données ;
- coordination de la gestion et du traitement d'incidents relatifs à la Protection des Données conformément aux règles prévues par la Politique de Protection des Données à caractère personnel.

(ii) Le Comité des Données à Caractère Personnel

Le Comité des Données à Caractère Personnel (Comité DCP) défini en Annexe 2 – Politique de Protection des Données à caractère personnel de ENGIE - doit se réunir deux fois par an pour examiner les questions relatives aux BCR.

Le Comité DCP décide des actions locales ou transversales et les soumet pour approbation aux instances compétentes du Groupe, et/ou au Comité de Direction Générale de ENGIE le cas échéant.

Une fois par an, le Comité DCP établit le bilan de ses activités (dont un point de situation sur l'application des présentes BCR et de la Politique de Protection des

Données à caractère personnel) qu'il présente aux instances du Groupe concernées.

(b) Au niveau des Branches et des Business Units

Chaque Branche (et le cas échéant, Business Unit) désigne un Délégué à la Protection des Données personnelles (DPD) qui coordonne les activités relatives à la Protection des Données dans son domaine de compétence.

Le DPD doit effectuer les missions suivantes :

- effectuer le suivi de la mise en œuvre et du respect des BCR et de la Politique de Protection des Données à caractère personnel dans la Branche (ou Entité) ;
- informer, conseiller et avertir les Responsables de Traitement concernant les problèmes de Protection des Données ;
- représenter sa Branche ou sa Business Unit dans ce domaine avec les parties intéressées et organisations externes, y compris dans le cadre d'investigations par des Autorités de Protection des Données ;
- traiter les réclamations locales faites par des Personnes Concernées conformément à l'Article 9 ci-dessous et les transmettre au Délégué Groupe aux Données Personnelles ;
- participer aux campagnes de sensibilisation et aux sessions de formation avec le personnel de la Branche ou de l'Unité commerciale ;
- participer aux activités organisées par le Délégué Groupe aux Données Personnelles (en matière de bonnes pratiques, de *feed-back/retour* basé sur l'expérience antérieure, etc.) et ce, en tant que membre actif du réseau ;
- transmettre des rapports annuels sur les événements majeurs ;
- transmettre aux Responsables de l'Éthique des rapports sur tout incident tel que l'utilisation inappropriée de Données à caractère personnel ou de tout incident de sécurité conformément aux règles prévues par la Politique de Protection des Données à caractère personnel.

(c) Au niveau de l'Entité juridique

Chaque Filiale de ENGIE s'assurera que les présentes BCR et la Politique de Protection des Données à caractère personnel sont respectées avant tout Traitement de Données, pendant son exécution et son opération.

Si la loi l'exige, le DPD (ou une personne désignée en tant que telle) est responsable du respect des dispositions légales locales relatives à la Protection des Données, comme la réalisation des démarches d'enregistrement auprès des Autorités nationales de Protection des Données compétentes.

8.2 **Contrôle et audit**

(a) Contrôle interne

(i) Le Groupe ENGIE a mis en œuvre un programme de Contrôle Interne dans le cadre duquel les plus importantes Filiales ENGIE, à savoir celles qui contribuent à plus de 85 % du chiffre d'affaires du Groupe, doivent rendre compte chaque année de leur conformité avec un cadre de contrôles correspondant à la réglementation interne et externe. Les autres Filiales qui contribuent à moins de 85 % du chiffre d'affaires du Groupe doivent néanmoins participer au Contrôle Interne annuel dès qu'elles commencent à transférer des Données à caractère personnel.

(ii) La Politique de Protection des Données à caractère personnel fait partie du système de contrôles surveillé au moyen du Programme de Contrôle Interne.

(iii) Ces contrôles couvrent tous les aspects des BCR, en particulier les suivants :

- L'organisation ;
- Les procédures ;
- La transparence et la loyauté à l'égard des Personnes Concernées ;
- La limitation de la finalité du Traitement ;
- La garantie de la qualité des Données à caractère personnel ;
- La garantie des droits individuels d'accès, de rectification et d'opposition au Traitement ;
- Les mesures de sécurité et de confidentialité ;
- La limitation de la durée de conservation des Données.

La liste ci-dessus n'est pas exhaustive.

(iv) Dans le cadre du programme de Contrôle Interne, le Directeur opérationnel (ou le responsable des processus opérationnels) au sein de la Filiale réalise une évaluation annuelle de l'efficacité des contrôles.

(v) Les résultats de ces évaluations et les mesures correctives proposées sont communiqués à la Direction et au Comité de Direction du Groupe. Le(s) DPD concerné(s) et le Délégué Groupe aux Données Personnelles doivent en être informés. Les Autorités de Protection des Données peuvent être informées de ces résultats si elles en font la demande au Délégué Groupe aux Données Personnelles.

(b) Audits internes

(i) À la demande de la Direction (du Groupe, de la Branche, de la BU ou de la Filiale), les équipes d'Audit Interne de ENGIE effectuent des missions d'audit sur des sujets spécifiques tels que les entités juridiques, les risques ou les processus opérationnels et les transferts relayés de Données à caractère personnel. Outre ces missions spécifiques, les équipes d'Audit Interne se voient confier la responsabilité de vérifier l'efficacité du programme de Contrôle Interne.

(ii) Tous les aspects du Contrôle Interne sont couverts par l'Audit Interne, en particulier :

- La pertinence du cadre de contrôles par rapport à la réglementation ;
- Le champ d'application (Filiales de ENGIE tenues d'y participer) ;
- La pertinence des contrôles mis en œuvre au niveau opérationnel ;
- L'évaluation réalisée par le Directeur opérationnel conformément à l'Article 8.2.a.iii et iv et l'efficacité d'une telle évaluation ;
- Les éventuelles mesures correctives prises.

(iii) La vérification du Contrôle Interne par les équipes d'Audit Interne est réalisée chaque année au niveau du Groupe et tous les 5 à 7 ans en moyenne au niveau opérationnel.

(iv) Les résultats de ces évaluations et les mesures correctives proposées sont communiqués à la Direction et au Comité de Direction du Groupe. Le(s) DPD concerné(s) et le Délégué Groupe aux Données Personnelles doivent en être informés. Les Autorités de Protection des Données peuvent être informées de ces résultats si elles en font la demande au Délégué Groupe aux Données Personnelles.

(c) Audits externes

(i) ENGIE SA et chaque Filiale de ENGIE étant informées par les présentes que les Autorités de Protection des Données sont habilitées par la législation applicable à réaliser des audits le cas échéant, elles reconnaissent qu'elles peuvent être

soumises à un audit à cet égard par les Autorités de Protection des Données compétentes et s'engagent par les présentes à respecter les décisions des Autorités de Protection des Données concernant toute question afférente.

9 Procédure relative aux plaintes

9.1 Personnes Concernées

(a) **Plainte** : si une Personne Concernée fait une réclamation concernant le traitement de ses Données à caractère personnel en vertu des BCR, ou si une Personne Concernée a un motif raisonnable de présumer que ses Données à caractère personnel sont Traitées illégalement en vertu de la législation locale sur la Protection des Données, elle peut soumettre la question au DPD de son entité juridique ou, si l'entité ne dispose pas d'un DPD, au DPD de sa Business Unit, ou, si la Business Unit ne dispose pas d'un DPD, au DPD de sa Branche.

Les réclamations doivent être transmises par courriel et envoyées en copie au DPD approprié.

Les postulants ou les employés retraités auxquels les présentes BCR s'appliquent doivent envoyer leurs réclamations par courriel à l'adresse privacy@engie.com.

Le Délégué à la Protection des Données concerné agira comme il suit :

(i) il en informera le Délégué Groupe aux Données Personnelles ;

(ii) il déclenchera une investigation ; et

(iii) le cas échéant, il avisera les plus importantes filiales des mesures appropriées pour garantir le respect et le suivi de la procédure, jusqu'à l'achèvement de celle-ci, y compris les mesures visant à faciliter la mise en conformité avec la procédure.

(b) **Réponse à la Personne Concernée :** dans un délai d'un mois à compter de la réception de la réclamation, le Délégué à la Protection des Données de l'entité juridique de la Personne Concernée ou le DPD de la Branche ou de la Business Unit notifiera par écrit à la Personne Concernée la position de ENGIE concernant la réclamation et toute mesure prise ou à prendre par ENGIE pour remédier au préjudice. Si le Délégué aux Données Personnelles concerné n'est pas en mesure de notifier la position de ENGIE dans un délai d'un mois, il informera la Personne Concernée de la date à laquelle la position de ENGIE lui sera notifiée, cette date ne devant pas dépasser un délai de deux mois suivant la réception de la réclamation. Le Délégué à la Protection des Données Personnelles concerné envoie une copie de la réclamation et de sa réponse écrite au Délégué Groupe aux Données Personnelles.

Si la réclamation de la Personne Concernée est rejetée et si la Personne Concernée n'est pas satisfaite de la manière dont la réclamation a été gérée, elle a le droit de déposer une plainte auprès d'une autorité de Protection des Données d'un pays de l'EEE ou d'une autorité nationale de Protection des Données ayant compétence et/ou d'engager une action devant un tribunal compétent pour faire appliquer ses droits en vertu des BCR.

(c) **Plainte directe :** Une Personne Concernée conserve en tout cas le droit de déposer directement une plainte devant une autorité de Protection des Données d'un pays de l'EEE ou une autorité nationale de Protection des Données ayant compétence et/ou devant un tribunal compétent, sans suivre la procédure de réclamation interne décrite dans les paragraphes précédents.

9.2 **Règles communes**

(a) Dans le cadre des présentes BCR, les Délégués à la Protection des Données personnelles ont les obligations suivantes :

- identifier et enregistrer les réclamations individuelles des Personnes Concernées,
- établir une liste de ces réclamations,
- examiner la réalité des infractions présumées,
- essayer de mener une médiation en proposant une indemnisation, après en avoir informé le Délégué Groupe aux Données Personnelles. Une procédure de médiation systématique et de règlement amiable est appliquée avant que les dossiers soient transmis au tribunal ou à l'autorité de surveillance ayant compétence.

(b) L'indépendance des Délégués à la Protection des Données personnelles est garantie pendant l'exécution de leurs obligations et ils sont liés par une obligation de neutralité et d'impartialité absolues dans les cas qu'ils gèrent.

(c) La confidentialité de l'identité de la Personne Concernée, du contenu de la réclamation et de l'identité de l'entité doit être respectée.

10 Responsabilité

10.1 Principes de responsabilité

La responsabilité des Exportateurs et Importateurs de Données à caractère personnel est engagée en cas de non-exécution de leurs obligations respectives à l'égard des Personnes Concernées en vertu des principes établis dans le présent Article 10. La charge de la preuve

leur incombe exclusivement à cet égard et, par conséquent, ils peuvent être mis hors de cause partiellement ou entièrement uniquement s'ils peuvent prouver qu'ils n'ont aucune responsabilité dans la cause du préjudice.

10.2 Dans le cas où l'Importateur est un Responsable de Traitement :

Si l'Importateur de Données a reçu les Données à caractère personnel en vue de les Traiter à ses propres fins en tant que Responsable de Traitement, l'Importateur et l'Exportateur de Données sont responsables vis-à-vis de la Personne Concernée en vertu des Clauses Contractuelles Types pour le transfert de données à caractère personnel vers des pays tiers émanant de la Décision de la Commission européenne 2001/497/CE.

Toute Personne Concernée ayant subi un préjudice dû à la non-exécution des obligations découlant des BCR par un Exportateur ou Importateur de Données a le droit de faire appliquer ses droits dans le pays où est établi l'Exportateur de Données et peut obtenir une indemnisation de l'Exportateur ou de l'Importateur de Données pour le préjudice subi.

10.3 Dans le cas où l'Importateur de Données est un Sous-Traitant :

Si l'Importateur de Données a reçu les Données à caractère personnel en tant que Sous-Traitant, l'Exportateur de Données est responsable vis-à-vis de la Personne Concernée en vertu des sections (i) et (ii) ci-dessous qui reprennent la clause de responsabilité (Clause 6) des Clauses Contractuelles Types pour le transfert de Données à caractère personnel vers des pays tiers en vertu de la Décision de la Commission européenne 2010/87/UE.

(i) Toute Personne Concernée ayant subi un préjudice dû à la non-exécution des obligations découlant des BCR par un Exportateur ou Importateur de Données peut obtenir une indemnisation de l'Exportateur de Données pour le préjudice subi.

(ii) Cependant, si l'Exportateur de Données est mis en liquidation de fait ou a cessé d'exister juridiquement, ou est devenu insolvable, l'Importateur de Données accepte que la Personne Concernée puisse déposer une plainte contre lui comme s'il était l'Exportateur de Données, sauf si une quelconque entité juridique qui lui aurait succédé a assumé toutes les obligations légales de l'Exportateur à titre contractuel ou par effet de la loi, auquel cas la Personne Concernée peut faire appliquer ses droits contre pareille entité dans la juridiction de l'Exportateur de Données.

10.4 Principes de responsabilité entre l'Exportateur et l'Importateur de Données :

Dans les relations entre les Exportateurs et les Importateurs de Données, chaque Filiale est responsable vis-à-vis des autres Filiales pour les préjudices qu'elle cause suite à la non-exécution des BCR, la responsabilité étant limitée au préjudice réel causé. À cet égard, si une

Filiale est tenue responsable d'un manquement commis par une autre Filiale, cette dernière indemnise la première Filiale, dans la mesure de sa responsabilité. Par exemple, si un Importateur de Données enfreint les BCR et que l'Exportateur de Données dédommage la Personne Concernée pour cette infraction, L'importateur de Données doit indemniser l'Exportateur. De la même façon, si un Exportateur de Données enfreint les BCR et que l'Importateur de Données dédommage la Personne Concernée pour cette infraction, l'Exportateur de Données doit indemniser l'Importateur de Données.

10.5 Chaque Filiale accepte formellement par les présentes ses responsabilités décrites ci-dessus à l'égard des Personnes Concernées.

10.6 Les Filiales garantissent disposer d'une capacité financière suffisante pour indemniser les Personnes Concernées du préjudice généré par un Traitement de Données illicite en vertu des BCR.

11 Mesures internes

Si une Filiale enfreint les présentes Règles Contraignantes d'Entreprise, n'applique pas les recommandations et conseils transmis après la vérification de la conformité par les Délégués à la Protection des Données Personnelles, ou ne coopère pas dans le cadre des audits relatifs au respect des BCR réalisés par les DPD ou par les Autorités de Protection des Données compétentes, et si le Délégué Groupe aux Données Personnelles le demande, ENGIE SA prendra les mesures suivantes :

- publication des recommandations du DPD sur l'Intranet du Groupe,
- publication des sanctions décidées par l'Autorité de Protection des Données,
- interdiction temporaire ou définitive des flux de données continus.

12 Coopération avec les Autorités de Protection des Données

Le Groupe ENGIE s'engage à coopérer, et veille à ce que tous les membres du Groupe ENGIE coopèrent avec les Autorités de Protection de Données, en particulier dans le cadre d'audits ou d'investigations par ces Autorités, et à prendre en considération les conseils et les recommandations des Autorités de Protection de Données concernant tous problèmes relatifs aux présentes BCR.

Cette coopération comprendra en particulier les actions suivantes :

- mettre à disposition le personnel nécessaire pour assurer le dialogue avec l'Autorité/les Autorités de Protection de Données compétente(s) ;

- examiner de manière approfondie et prendre en considération les décisions prises par toute Autorité de Protection de Données ayant compétence pour statuer sur les questions juridiques en matière de Protection des Données qui peuvent avoir un impact sur les présentes BCR ;

- aider dans tout audit ou toute investigation réalisée par une Autorité de Protection des Données comme énoncé dans l'Article 8.2 (c) ci-dessus ;

- s'engager à respecter toute décision officielle et définitive d'une Autorité de Protection de Données ayant compétence pour statuer sur toute question relative à l'interprétation ou à l'application des présentes BCR.

13 Mise à jour des BCR

13.1. Seul le Comité des Données à Caractère Personnel peut décider de toute modification des présentes BCR.

13.2. Le Comité des Données à Caractère Personnel désignera une équipe ou une personne chargée de mettre à jour la liste des Filiales ENGIE jointe aux présentes en Annexe 1.

13.3. ENGIE SA notifiera toute modification significative des présentes BCR ou de la liste des Filiales de ENGIE aux Autorités de Protection des Données concernées, étant prévu que :

(a) certaines de ces modifications peuvent nécessiter une nouvelle autorisation de l'Autorité de Protection des Données ;

(b) les mises à jour des BCR ou de la liste des Filiales de ENGIE peuvent être effectuées sans demander une autorisation à condition que :

(i) une personne identifiée tienne entièrement à jour la liste des entités soumises aux BCR et effectue le suivi et l'enregistrement des mises à jour des BCR, et fournisse les informations nécessaires aux Personnes Concernées ou aux Autorités de Protection des Données à leur demande ;

(ii) aucun transfert ne soit réalisé vers une Filiale de ENGIE venant d'être créée ou vers une Filiale de ENGIE qui n'a pas encore adhéré aux BCR, jusqu'à ce que cette Filiale de ENGIE soit expressément liée par les BCR et s'engage à les respecter ;

(iii) les modifications des BCR ou de la liste des Filiales de ENGIE soient communiquées une fois par an à l'Autorité de Protection

des Données concernée, avec une explication concise des raisons qui justifient la mise à jour.

13.4. Les présentes BCR spécifieront la date à laquelle la dernière révision des BCR a eu lieu, ainsi que la date des révisions.

14 Documents contractuels

Les documents contractuels sont indiqués ci-dessous par ordre de priorité décroissant :

1. Les présentes BCR ;
2. Les Annexes aux présentes BCR ;
3. L'Accord de Groupe signé par chaque Entité du Groupe ENGIE.

Cet ordre de priorité s'applique et les BCR prévaudront toujours en cas de conflit ou de contradiction.

15 Droit applicable

Les présentes BCR sont régies par le droit français.

16 Date de Prise d'Effet – Durée

Les présentes BCR prendront effet à partir du [_____], pour une durée illimitée.

Annexe 1 : Liste des entités devant approuver les BCR

Périmètre GDF SUEZ
sociétés en intégratio

Annexe 2 : Politique Groupe de Protection des Données à caractère personnel

GDF SUEZ

DECISION GDF SUEZ

Date : 31 Janvier 2014

Référence : GDF SUEZ 2013 – 005

Emetteur : Secrétariat Général

Interlocuteur : Jacques PERRET jacques.perret@gdfsuez.com Tel.: +33 (0)1 44 22 50 17

Politique Groupe de protection des données à caractère personnel

Résumé

La présente note constitue la Politique Groupe de protection des données à caractère personnel de GDF SUEZ.

Elle précise les principes et objectifs retenus, l'organisation mise en place, le système de pilotage défini ainsi que les rôles et responsabilités en matière de protection des données à caractère personnel.

La présente Politique Groupe de protection des données à caractère personnel, validée après débat en COMEX du 20 Janvier 2014, prend effet immédiatement.

Jacques Perret	Alain Chaigneau	Gérard Mestrallet
Délégué Groupe aux Données Personnelles	Secrétaire Général	Président Directeur Général

Document(s) annulé(s) ou modifié(s) : à qualifier
Pièce(s) jointe(s) : à qualifier
Diffusion : à qualifier

Table des matières

1. Contexte et enjeux

Le Groupe GDF SUEZ doit traiter des Données à caractère personnel relatives à ses employés, clients, partenaires, prestataires de services, sous-traitants et fournisseurs.

Les Données à caractère personnel ne figurent pas seulement dans les documents papier, mais aussi dans tous les Systèmes d'Information du Groupe tels que les datacenters de l'entreprise, les applications logicielles, l'Internet et l'Intranet, le cloud, le big data, les smartphones, le BYOD[3] (Bring Your Own Device), le smartgrid, etc.

Par conséquent, le Groupe est de plus en plus exposé aux risques de collecte et d'usage interne/externe inappropriés, d'altération, de compromission et même de falsification des Données à caractère personnel.

Ce phénomène peut porter atteinte à l'image et à la réputation et entraîner des poursuites judiciaires et des sanctions financières importantes pour le Groupe.

Conscient de l'importance des règles de Protection des Données à caractère personnel et des risques encourus en cas de violation, le Groupe s'est engagé à protéger cet actif immatériel. Cette action a également un effet positif direct sur la confiance du personnel et des clients, ainsi que sur l'image et la réputation du Groupe.

La Protection des Données à caractère personnel constituant une obligation légale et une enjeu stratégique pour le Groupe et sa réputation, il est essentiel de mettre en œuvre la présente politique (la « Politique »).

2. Définitions

• « **Chargé de Projet** » : personne agissant pour le compte du Responsable de Traitement, qui pilote le projet jusqu'à mise en œuvre du Traitement. Il doit protéger les Données à caractère personnel tout au long de la construction du projet.

• « **Délégué Groupe aux Données Personnelles** » : la personne désignée au niveau du Groupe en charge notamment de définir et diffuser les bonnes pratiques relatives aux Données à caractère personnel et de s'assurer de leur application (voir § 5.1).

• « **Délégué à la Protection des Données** » (**DPD**) : la personne désignée comme responsable des actions relatives à la Protection des Données à caractère personnel au niveau de la Branche, de la Business Unit ou de l'Entité (voir § 5.2).

[3] Pratique qui consiste à utiliser ses équipements personnels (ordinateur portable, …) dans un contexte professionnel.

• « **Données à caractère personnel** » : toute information relative à une personne physique identifiée ou qui peut être identifiée (« **Personne Concernée** »), directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (i.e. nom, prénom, n° de sécurité sociale, e-mail, adresse IP, etc.).

• « **Entité** » : entité juridique du Groupe dans le périmètre consolidé par intégration globale.

• « **Groupe** » : le Groupe GDF SUEZ.

• « **Responsable de Traitement** » : Entité qui détermine les finalités et moyens du ou des Traitements qu'il met ou fait mettre en place. Le Responsable de Traitement est tenu de prendre toute précaution nécessaire à la Protection des Données à caractère personnel.

• « **Sous-Traitants** » : entités traitant des Données à caractère personnel pour le compte du Responsable du Traitement.

• « **Traitement** » : toute opération ou tout ensemble d'opérations portant sur des Données à caractère personnel, quel que soit le procédé utilisé (traitements automatisés tels qu'applications informatiques, fichiers excel,… ou traitements non-automatisés de Données à caractère personnel contenues ou appelées à figurer dans des fichiers structurés et stables), et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Un glossaire annexé au présent document vient compléter les définitions ci-dessus.

3. Champ d'application et objectifs

La Politique Groupe de Protection des Données à caractère personnel s'inscrit dans le cadre de la charte Ethique du Groupe, dans sa démarche de maîtrise des risques et de Protection de son Patrimoine Immatériel[4].

Elle s'applique à l'ensemble des domaines fonctionnels spécifiés dans une charte d'utilisation des ressources informatiques et télécoms ainsi qu'à l'ensemble du personnel et des Entités du Groupe, même si elle peut être annulée par les réglementations nationales applicables à une Entité, notamment par des réglementations spécifiques prévoyant l'indépendance des fournisseurs d'infrastructures au sein de l'Union Européenne ou par toute autre réglementation équivalente applicable ailleurs.

Les principes de la présente Politique sont basés sur les réglementations internationales énumérées en annexe.

[4] Cf. Politique de Protection des Patrimoines Matériels et Immatériels

La Politique Groupe de Protection des Données à caractère personnel définit les **objectifs**, les **moyens** et la **gouvernance** qui permettent au Groupe de respecter les réglementations applicables concernant la Protection des Données à caractère personnel dans le respect de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques[5]. La présente Politique permet en outre d'anticiper certains points du projet de Règlement Européen relatif à la Protection des Données à caractère personnel que le Groupe a décidé d'inclure dans ses principes fondamentaux car considérés comme de bonnes pratiques en la matière.

La présente Politique sera progressivement accompagnée et détaillée par des documents complémentaires (méthodologies, bonnes pratiques, sensibilisation, …) devant permettre l'atteinte des objectifs fixés.

Les exigences suivantes doivent être respectées avant la mise en œuvre de tout Traitement et doivent par conséquent être prises en compte dans la planification de tout projet impliquant des Données à caractère personnel. Une fois mis en œuvre, le Traitement doit respecter à tout moment les principes énoncés. Des exigences similaires peuvent également s'appliquer en cas de modification des conditions dans lesquelles le Traitement est effectué.

3.1. Finalités explicites et légitimes

Les Données à caractère personnel doivent être collectées et traitées par des moyens équitables pour des finalités déterminées, explicites et légitimes, et ne pas être utilisées ou traitées ultérieurement de manière incompatible avec ces finalités.

Le respect de ces principes de légalité et d'équité peut exiger, en vertu de la législation applicable sur la Protection des Données à caractère personnel que :
- la Personne Concernée soit informée du Traitement et de ses finalités ; et/ou
- la Personne Concernée consente expressément au Traitement; et/ou
- l'Autorité de Protection des Données soit informée du Traitement prévu.

Les Données à caractère personnel ne pourront être communiquées au sein des services ou départements, à d'autres Entités du Groupe ou à des tiers qu'au regard des finalités du Traitement, et les Personnes Concernées devront être informées de la communication de leurs Données à caractère personnel (ou parfois donner leur consentement à cette communication).

[5] Article 12 de la Déclaration universelle des droits de l'homme (Nations Unies) : *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée…*

Article 17 du Pacte international relatif aux droits civils et politiques (Haut-Commissariat aux droits de l'homme) : *Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée…*

3.2. Pertinence et proportionnalité des données collectées

Les Données à caractère personnel collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour leurs traitements ultérieurs. Elles doivent être exactes, complètes et mises à jour si nécessaire.

La durée de conservation des Données à caractère personnel traitées doit être définie conformément aux finalités de la collecte et dans le respect des lois applicables. Lorsque les Données à caractère personnel ne sont plus nécessaires aux finalités légitimant leur traitement, elles doivent être effacées ou rendues anonymes.

3.3. Données sensibles

Certaines Données à caractère personnel sont considérées comme sensibles. Ces Données concernent l'intimité des Personnes Concernées ou sont susceptibles de donner lieu, en cas d'utilisation abusive, à une discrimination illégale ou arbitraire.

En particulier, les Données à caractère personnel concernant l'origine raciale ou ethnique, les opinions ou convictions politiques, religieuses ou philosophiques, ou relatives à la santé ou à la vie sexuelle d'une personne, doivent être considérées comme sensibles.

De plus, il convient de vérifier les lois relatives à la Protection des Données à caractère personnel applicables aux Entités, d'identifier toute autre Donnée à caractère personnel jugée sensible et de se conformer aux exigences en la matière.

Le Responsable de Traitement ne devra traiter des Données à caractère personnel sensibles qu'avec le consentement explicite de la Personne Concernée ou dans des circonstances limitées expressément autorisées par la loi.

3.4. Obligations de sécurité et de confidentialité

Toutes mesures utiles doivent être prises, au regard de la nature des Données à caractère personnel et des risques présentés par le Traitement, pour préserver la sécurité et la confidentialité de ces Données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Ces mesures dépendront du risque existant, des conséquences possibles pour la Personne Concernée, du caractère sensible des Données à caractère personnel, de la technologie disponible et de la pratique générale acceptée dans les juridictions compétentes de l'Entité.

Les Sous-Traitants seront sélectionnés sur la base des garanties offertes en matière de sécurité technique et organisationnelle et de confidentialité des Données à caractère personnel. Un contrat prévoyant l'obligation du Sous-Traitant de respecter ces mesures de protection devra être établi.

3.4.1. Classification et Protection des Données à caractère personnel

En règle générale, les Données à caractère personnel sont à classifier au niveau « Interne » ou « Restreint » (selon la Politique Groupe de Protection des Patrimoines Matériels et Immatériels / Règle Groupe 11).

Cependant, les « Données Sensibles » sont à classifier au niveau « Restreint » ou « Confidentiel » (cf. Règle Groupe 11).

La classification de ces Données est établie lors de l'exercice d'analyse d'impact sur la vie privée (cf. 3.4.2 Traitement du risque en amont).

Ces données sont à protéger conformément aux politiques et standards de sécurité des systèmes d'information.

3.4.2. Traitement du risque en amont

La mise en place d'un nouveau Traitement doit être accompagnée par les actions suivantes :

- L'analyse d'impact sur la vie privée : elle permet de déterminer le niveau de risque pour les personnes (en cas de perte ou compromission de leurs données par exemple) mais également pour l'entreprise (en cas d'atteinte à son image ou sa réputation par exemple) et vise l'identification des mesures de protection adéquates.

- La prise en compte de la Protection des Données à caractère personnel dès la conception : elle permet de s'assurer que les fonctionnalités requises sont définies en amont des développements et prennent en compte les obligations liées à la protection de ces Données.

- La Protection des Données à caractère personnel par défaut : elle vise notamment les principes de limitation des données (celles strictement nécessaires à la finalité du traitement), de conservation des données (dans le cadre de la finalité du traitement) et d'anonymisation.

Il importe de prendre toute précaution nécessaire à la Protection des Données à caractère personnel, dans toutes les phases du projet.

3.5. Transferts internationaux

Les transferts internationaux de Données à caractère personnel ne peuvent, par principe, être effectués que lorsque le pays vers lequel ces Données sont transmises offre a minima le niveau de protection décrit dans la présente politique.

A défaut, des clauses contractuelles appropriées devront être incluses dans les contrats conclus entre les expéditeurs (les « exportateurs ») et les destinataires (les « importateurs ») de Données à caractère personnel afin de garantir un niveau adéquat de protection à ces Données.

Par ailleurs, GDF SUEZ s'est doté de BCR (Binding Corporate Rules), validées par les Autorités de contrôle européennes afin d'assurer la Protection des Données personnelles transférées en dehors de l'Union Européenne au sein du Groupe. Ces règles internes reprennent les obligations légales et réglementaires en la matière et doivent être connues et respectées par l'ensemble des salariés du Groupe.

3.6. Transparence et respect des droits des personnes

Les Personnes Concernées par les Traitements disposent de droits leur permettant de garder la maîtrise des informations qui leur sont relatives. Elles doivent ainsi être informées de l'existence d'un Traitement de leurs Données à caractère personnel avant la mise en œuvre effective de ce Traitement et elles disposent à tout moment d'un droit d'accès et de rectification de leurs Données. Les Personnes Concernées ont également le droit de s'opposer à tout moment au traitement de leurs Données à caractère personnel pour des raisons impérieuses et légitimes relatives à leur situation personnelle spécifique, même si elles avaient donné leur consentement exprès à ce traitement.

Des politiques transparentes seront mises en œuvre en ce qui concerne le Traitement des Données à caractère personnel. Par conséquent, des informations de base seront fournies aux Personnes Concernées sur l'identité des Responsables de Traitement et la manière dont les Personnes Concernées pourront exercer leurs droits d'accès, de rectification et/ou leur droit de demander la suppression de leurs Données à caractère personnel.

4. Moyens

Les actions suivantes seront mises en œuvre pour atteindre les objectifs de la présente Politique :

4.1. Sensibilisation et formation

L'ensemble du personnel des Entités doit être sensibilisé aux enjeux liés à la Protection des Données à caractère personnel. Des campagnes de sensibilisation globales seront réalisées au niveau du Groupe. Des actions locales pourront être réalisées de manière complémentaire par les Entités.

La formation des Délégués à la Protection des Données sera réalisée selon les mêmes principes.

Ces actions devront être coordonnées au sein des Entités par le Délégué Groupe aux Données Personnelles et les Délégués à la Protection des Données (DPD).

4.2. Contrôles et audits

Des contrôles internes de conformité à la présente Politique et aux lois et réglementations localement applicables en matière de Protection des Données à caractère personnel devront être réalisés régulièrement par le Représentant Légal de l'Entité, qui délèguera cette activité à son DPD et à son Responsable de la Sécurité des Systèmes d'Information. Le Délégué Groupe aux Données Personnelles pourra également procéder à ces contrôles.

Dans le cadre de ces contrôles, l'accès aux Traitements et aux Données, ainsi que les mesures de confidentialité et les durées d'archivage pourront être vérifiés.

La réalisation effective de ces contrôles pourra faire, si nécessaire, l'objet de revues conduites par la Direction de l'Audit Interne.

4.3. Cartographie des Traitements

En ce qui concerne le principe de transparence et pour faciliter l'exercice du droit d'accès des Personnes Concernées, il est recommandé à chaque Entité d'établir une cartographie et un registre des Traitements. Cette cartographie, offrant une vue d'ensemble complète, permettra également le contrôle et la rationalisation des Traitements. Le registre, quant à lui, facilitera la gestion, par le Responsable de Traitement, des demandes d'accès des Personnes Concernées.

4.4. Traitement d'incidents

A cet égard, toute personne ayant connaissance d'une utilisation inappropriée des Données à caractère personnel informe son Délégué à la Protection des Données (DPD). Celui-ci traite du sujet avec le Déontologue qui en fait le reporting dans INFORM'ethics.

Dès lors que l'instruction d'un incident de sécurité démontre qu'il y a compromission de Données à caractère personnel, le Délégué Groupe aux Données Personnelles, membre du Comité de Traitement des Incidents, est informé et coordonne le traitement de l'incident en relation avec les autres membres de ce Comité (en relation avec l'Entité concernée).

Dans le cas où une gestion de crise est nécessaire pour traiter l'incident ayant entrainé la compromission de Données à caractère personnel, le Délégué Groupe aux Données Personnelles devient l'un des membres désignés de cette cellule de crise et œuvre à la résolution de l'incident.

Le traitement des incidents de sécurité doit être réalisé conformément à la Procédure de Traitements des Attaques Informationnelles[6].

4.5. Accords écrits

Dans le cadre de l'acquisition, l'utilisation voire la sous-traitance à un co-contractant de Données à caractère personnel (par exemple pour la mise à disposition d'offres complémentaires aux clients et prospects de GDF SUEZ), un accord écrit doit être établi entre les parties concernées (GDF SUEZ, ses clients ou partenaires). En tout état de cause, la collecte, l'utilisation ainsi que la sous-traitance de ces Données à caractère personnel doivent s'inscrire dans le respect des lois en vigueur, de la charte Ethique de GDF SUEZ et de la présente Politique.

[6] Procédure approuvée par le Comité de Sécurité de l'Information en octobre 2012, puis par le Comité exécutif (COMEX).

5. Gouvernance

Les objectifs et moyens décrits ci-dessus seront mis en œuvre au niveau du Groupe et au sein de chaque Entité.

5.1. Au niveau du Groupe

Le pilotage stratégique de la Politique de Protection des Données à caractère personnel est placé sous la responsabilité du Comité de Direction Générale de GDF SUEZ qui en délègue la coordination et le pilotage opérationnel à son Secrétaire Général. Ce dernier délègue cette responsabilité au Délégué Groupe aux Données Personnelles.

Toute difficulté d'application de la présente Politique doit être remontée au Délégué Groupe aux Données Personnelles.

5.1.1. Délégué Groupe aux Données Personnelles

Les principales missions du Délégué Groupe aux Données Personnelles sont les suivantes :

- Définir et diffuser, en relation avec les Entités du Groupe, les bonnes pratiques d'utilisation des données personnelles (clients, salariés, fournisseurs …).
- Veiller à leur application et conseiller / alerter les managers sur les risques associés.
- Favoriser la création de valeur dans l'utilisation de ces données, par la promotion des synergies autorisées entre fichiers relevant d'Entités différentes du Groupe.
- Animer en réseau les personnes en charge du domaine « données personnelles ».
- Représenter le Groupe, pour ce domaine, auprès des acteurs et organismes externes.
- Suivre l'évolution de la réglementation dans les principaux pays où le Groupe est implanté.
- Coordonner la gestion des incidents relatifs aux données personnelles en relation avec les Directions Sponsors des domaines d'INFORM'ethics.

5.1.2. Le Comité de Protection des Données

La présente Politique institue le Comité des Données à Caractère Personnel (Comité DCP) ayant pour objectif d'assurer le pilotage des activités relatives aux données personnelles.

Présidé par le Délégué Groupe aux Données Personnelles, le Comité DCP réunit de manière trimestrielle les Relais Informatique et Libertés. Ce Comité comprend également un représentant de la Direction Juridique, de la Direction de l'Ethique, de la Direction de l'Audit Interne ainsi que de la Direction des Ressources Humaines et en fonction des besoins, le Responsable Sécurité SI Groupe, un représentant de la Direction Santé Sécurité et le Directeur Sûreté Groupe en tant que représentant de l'Information Security Committee.

Il décide à son niveau des actions locales ou transverses et en réfère aux instances Groupe, le cas échéant au Comité de Direction Générale de GDF SUEZ, pour validation.

Une fois par an, le Comité DCP établit le bilan de ses activités (dont un point de situation sur l'application de la présente Politique) qu'il présente aux instances Groupe concernées.

Une fois par an, le Comité DCP organise un séminaire interne dont l'objectif est de réunir l'ensemble des acteurs concernés par la Protection des Données à caractère personnel. Cet évènement est un lieu d'échange et de partage entre ces acteurs.

Il permet également de présenter le bilan de l'année écoulée et de donner les orientations sur la période à venir.

5.2. Au niveau des Branches et des Business Units

Chaque Branche désigne un Délégué à la Protection des Données (DPD), qui coordonnera les activités relatives à son domaine de responsabilité.

Les missions du Délégué à la Protection des Données sont les suivantes :

- Mettre en œuvre la Politique Groupe de Protection des Données à caractère personnel et contrôler son application ;
- Informer, conseiller et, si nécessaire, alerter les Responsables de Traitements sur les questions relatives à la Protection des Données à caractère personnel ;
- Participer aux campagnes de sensibilisation du personnel ;
- Participer aux activités organisées par le Délégué Groupe aux Données Personnelles (bonnes pratiques, retour d'expérience, etc.) et être un membre actif du réseau ;
- Etablir un rapport annuel de ses activités ;
- Informer le Déontologue des usages inappropriés de Données à caractère personnel (cf. 4.4).

Le cas échéant, les Branches pourront également décider d'identifier un DPD au niveau des Business Units.

La Protection des Données à caractère personnel pourrait également être organisée au niveau national, si cette approche est nécessaire par souci d'efficacité.

5.3. Au niveau de l'Entité

Chaque Entité est responsable des Traitements qu'elle met ou fait mettre en œuvre et son Représentant Légal engage sa responsabilité vis à vis des exigences des lois et réglementations applicables en matière de Protection des Données à caractère personnel.

Chaque Entité veillera au respect de la présente Politique et des lois en matière de Protection des Données à caractère personnel avant la mise en œuvre d'un Traitements et tout au long de son exécution.

Si la loi l'exige, le DPD (ou toute personne expressément désignée à cet effet) sera chargé de veiller au respect des lois locales exigeant, par exemple, que les Traitements soient notifiés à l'Autorité de Protection des Données.

5.4. Les autres acteurs

Le Responsable Sécurité SI de l'Entité apporte son expertise et son appui à la Protection des Données à caractère personnel, que celles-ci soient liées à un Traitement hébergé en interne ou chez un tiers. Ses principales missions dans ce domaine sont les suivantes :

- Assister les DPD dans la classification des Données à caractère personnel (cf. Règle Groupe 11) et dans le déroulement de la gestion de projet SI (cf.3.4.2 Traitement du risque en amont).
- Conseiller dans le choix des fonctions et mécanismes de Protection des Données à caractère personnel.
- Etre le contact pour toute requête relative à la Protection des Données à caractère personnel d'un traitement en production (ou lorsqu'il est nécessaire de compléter l'annexe sécurité dans le cadre d'une déclaration ou demande d'autorisation).

Les Chargés de Projet, agissant pour le compte des Responsables de Traitement, pilotent le projet jusqu'à mise en œuvre du Traitement. Ils doivent protéger les Données à caractère personnel tout au long de la construction des projets.

Les Directions Juridiques et les Directions des Ressources Humaines peuvent apporter conseils et informations au regard de la législation et de la jurisprudence applicables.

Les Déontologues peuvent apporter aux DPD appui et conseil en relation avec INFORM'ethics.

Tous les personnels (occasionnels ou permanents) sont responsables, à leurs niveaux, de la Protection des Données à caractère personnel qu'ils sont amenés à manipuler.

Toute personne amenée à mettre en œuvre une application traitant de données à caractère personnel doit en informer préalablement le DPD de son Entité.

Les tiers, dont les Sous-Traitants, mandatés par les Entités du Groupe pour effectuer des prestations pour le compte de ces dernières, doivent être informés de l'obligation de respecter les principes énoncés dans la présente Politique.

Annexe 3 : Traitement des Données

Champ d'application : Catégories de Données et finalités des transferts de Données et du Traitement couvertes par les BCR.

Les BCR s'appliquent à toutes les Données à caractère personnel des ressources humaines du Groupe qui sont ou ont été soumises à la Directive européenne et, plus particulièrement, à toutes les Données à caractère personnel des employés, postulants, stagiaires, travailleurs temporaires ou employés retraités du Groupe, qui ont été collectées dans l'EEE, transférées et traitées au sein du Groupe pour la gestion de ses ressources humaines au niveau international dans le cadre de son activité. Il s'agit des données dans les domaines suivants :

- Organisation (les répertoires, les organigrammes, ainsi que le contrôle de l'accès aux Systèmes d'Information du Groupe à des fins de traçabilité ou de surveillance du système, etc.),
- Rémunération et avantages (augmentations annuelles, rémunération variable, salaire brut, détention de parts, etc.),
- Recrutement et mobilité nationale/internationale,
- Développement des ressources humaines (compétences, formation, évaluation des performances, plans de développement, etc.),
- Gestion administrative du personnel (gestion des données du personnel, effectifs, gestion du temps, indemnité/frais de déplacement, etc.),
- Alertes Professionnelles (incidents éthiques, discrimination, etc.),
- Santé, sécurité et environnement (sécurité des déplacements, accidents du travail, etc.),
- Gestion des incidents de sécurité (investigation informatique, etc.).

Annexe 4 : Sécurité du Système d'Information de GDF SUEZ

Politiques de sécurité thématiques et du Groupe

- Politique Groupe de Sécurité des Systèmes d'information : décrit l'ensemble de l'organisation de la filière sécurité du Groupe, les différents comités ainsi que les rôles et responsabilités de chacun des acteurs
- Politique Thématique de Sécurité des Mots de passe : décrit les contraintes liées à la constitution et la gestion des mots de passe pour l'ensemble du SI
- Politique Thématique de Sécurité de l'IAM (Identity Access Management) : décrit les contraintes de sécurité liées à la gestion des identités et des comptes utilisateurs, les habilitations et autorisations.
- Politique Thématique de Sécurité Réseaux et Télécoms : décrit l'ensemble des contraintes de sécurité liées aux ressources réseaux et télécoms du Groupe, notamment la sécurité en datacenter
- Politique Thématique de Sécurité des Accès Internet : décrit l'ensemble des contraintes de sécurité liées à la mise en place et l'utilisation des accès Internet du Groupe et notamment la nécessité de déployer une politique de filtrage des sites accessibles par les utilisateurs
- Politique Thématique de Sécurité des Accès Partenaires : décrit l'ensemble des contraintes de sécurité liées aux accès des partenaires externes sur notre SI quelque soit le type d'accès considéré : permanents, temporaires, à distance…
- Politique Thématique de Sécurité des Accès Distants : décrit l'ensemble des contraintes de sécurité liées aux accès à notre SI depuis l'extérieur pour les employés du Groupe, notamment en ce qui concerne les ressources accessibles, le niveau d'authentification nécessaire etc…
- Politique Thématique de Sécurité des Exigences dans le cadre d'une prestation d'hébergement : décrit l'ensemble des contraintes de sécurité liées à l'hébergement externes de ressources internes de notre SI, contraintes à faire respecter par l'hébergeur.
- Politique Thématique de Sécurité des Sites Internet / Extranet hébergés chez un tiers : décrit l'ensemble des contraintes de sécurité liées à l'hébergement externe de sites Internet / Extranet du Groupe, à faire respecter par le prestataire d'hébergement
- Politique Thématique de Sécurité des Points de présence Internet : décrit l'ensemble des contraintes de sécurité liées à la sécurité des points de présence du Groupe sur Internet : sites web, routeurs d'interconnexion…
- Politique Thématique de Sécurité de recette des applications web: décrit l'ensemble des contraintes de sécurité liées à la recette des applications web développées par le Groupe (tests de sécurité avant mise en production)
- Politique Thématique de Sécurité du WiFi : décrit l'ensemble des contraintes de sécurité liées à l'utilisation des technologies WiFi au sein du Groupe, que ce soit pour accéder au LAN local d'une entité ou pour mettre à disposition un accès de type Guest aux visiteurs

- Politique Thématique de Sécurité de la gestion des vulnérabilités et correctifs de sécurité : décrit le processus à mettre en place au sein de chaque entité pour la gestion des vulnérabilités et correctifs de sécurité en fonction de leur criticité
- Politique Thématique de Sécurité des Postes de Travail et Terminaux mobiles : décrit l'ensemble des contraintes de sécurité liées à l'utilisation des postes de travail utilisateurs et des terminaux mobiles, notamment en termes de chiffrement, de protection antivirale…
- Politique Thématique de Sécurité de la Virtualisation : décrit l'ensemble des contraintes de sécurité liées à l'utilisation des technologies de virtualisation au sein du SI : protection des images virtuelles, des serveurs physiques, exploitation, supervision…
- Politique Thématique de Sécurité des Active Directory : décrit l'ensemble des contraintes de sécurité liées aux annuaires Active Directory : exploitation, supervision, revue des comptes, gestion fine des habilitations…
- Politique Thématique de Sécurité de la continuité d'activité informatique: décrit l'ensemble des contraintes de sécurité à respecter pour assurer la continuité d'activité informatique au sein d'une entité et son maintien en conditions opérationnelles
- Plan de protection SI : décrit l'ensemble des contraintes de sécurité liées au cycle de vie de l'information, en fonction de son niveau de confidentialité (accès, sauvegarde, transport, suppression…)

Liste d'autres documents liés à la sécurité de l'information :

- Politique de protection du Patrimoine matériel et immatériel : décrit l'ensemble du dispositif de protection du patrimoine qui protège les informations sensibles à la hauteur des enjeux, responsabilise l'ensemble des acteurs sur ce thème et garantisse une adaptation permanente aux menaces.
- Règle Groupe n°11 sur la classification des informations, définissant les 4 niveaux de confidentialité d'une information et les contraintes de sécurité liées à chacun de ces niveaux.

Annexe 5 : Clause de Protection des Données à caractère personnel

1.1. Afin d'exécuter le Contrat-Cadre et/ou le Contrat d'Application, le Prestataire de service est amené à traiter les données des clients et des employés du Client et, notamment des données à caractère personnel. Ces données à caractère personnel sont particulièrement sensibles pour l'image et le patrimoine du Client.

1.2. Chaque partie est informée que les données à caractère personnel et les traitements afférents sont soumis à des dispositions légales et réglementations dites Informatique et Libertés (et notamment la loi du 6 Janvier 1978). Le cas échéant, chaque Partie procèdera pendant la durée de l'Contrat-Cadre à toute déclaration lui incombant et, plus généralement, respectera la réglementation Informatique et Libertés.

1.3. Le Client reste dans tous les cas propriétaire des données traitées par le Prestataire au titre du contrat.

1.4. Le Prestataire de service s'engage à respecter l'ensemble des directives, lignes directrices et recommandations formulées par le Client à cet égard.

1.5. Le Prestataire de service s'engage, au titre des obligations souscrites dans le Contrat-Cadre et/ou le Contrat d'Application, à prendre les mesures de sécurité destinées à:

- Assurer la sécurité et l'intégrité des données à caractère personnel contre les risques de divulgation, destruction, corruption, piratage, détournement de ces données par un tiers non habilité ;

- Ne pas utiliser les données à caractère personnel à des fins autres que la stricte exécution de ses obligations contractuelles. En conséquence, le Prestataire s'interdit d'exploiter, y compris pour ses besoins propres, directement ou indirectement, ces données. Le Prestataire s'engage à ne pas céder ni mettre à disposition les données et fichiers à des tiers à quelques fins que ce soit et notamment à des fins de prospection commerciale ;

- Ne pas conserver les données à caractère personnel au-delà de la durée nécessaire à la réalisation de ses obligations contractuelles ;

- Assurer la sécurité, l'intégrité et la confidentialité des échanges;

- Veiller à prendre toutes les dispositions nécessaires pour ne pas risquer de diffuser de virus ;

- Ne pas transférer les données recueillies vers un pays ne disposant pas d'une protection suffisante, au sens de la Directive européenne sur la Protection des Données, sans l'accord préalable et écrit du Client;

- Utiliser la clause contractuelle appropriée proposée par la Commission européenne et la faire signer par les entités localisées dans des pays ne disposant pas d'une protection suffisante au sens de la Directive européenne 95/46/CE du 24 Octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**.**

- Ne prendre aucune copie de tous documents et supports d'information contenant des données à caractère personnel, à l'exception de celles nécessaires pour les besoins de l'exécution des Prestations et procéder ou faire procéder auprès de ses sous-traitants, en fin de Contrat, à la destruction des données, des fichiers informatisés ou manuels où figurent les données recueillies dans le cadre du Contrat.

- S'assurer que toute violation ou fuite de données est signalée au Client dans les 48 heures suivant la constatation, et prendre les mesures appropriées afin de limiter les conséquences d'une telle violation ou fuite.

1.6. Le Client se réserve le droit de procéder ou de faire procéder à toute vérification raisonnable qui lui apparaîtra indispensable pour constater le respect des obligations précitées du Prestataire, après l'en avoir préalablement informé.