22 décembre 2020

POLITIQUE DE PROTECTION DES DONNÉES

Modèle organisationnel

Sommaire

POLITIQUE DE PROTECTION DES DONNÉES

Modèle organisationnel

1. Introduction

Le Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (le « RGPD ») est entré en vigueur le 25 mai 2018.

Le présent Modèle Organisationnel (le « Modèle Organisationnel ») recueille les mesures techniques et organisationnelles que la société Falck Renewables S.p.A. (la « Société ») met en place pour garantir - et être en mesure de prouver - la conformité au RGPD des activités de traitement des données à caractère personnel des personnes physiques, effectuées directement ou que des entités tierces effectuent en son nom, et afin de spécifier les mécanismes de supervision organisationnels et de processus dont la Société s'est dotée pour assurer une protection effective et efficace des données à caractère personnel dont elle est le responsable du traitement.

2. Champ d'application

Le présent Modèle Organisationnel s'applique aux administrateurs, dirigeants, employés, collaborateurs, conseillers de la Société ainsi qu'aux sous-traitants du traitement, fournisseurs et toute autre entité tierce qui effectue des opérations de traitement de données à caractère personnel pour le compte de la Société (les « Destinataires »).

Le présent Modèle Organisationnel s'applique à toutes les sociétés contrôlées directement ou indirectement par la Société, y compris (i) la Société, (ii) Vector Cuatro S.L.U. et les sociétés contrôlées directement ou directement par cette dernière ainsi que (iii) Falck S.p.A. (ensemble, le « Groupe ») soumises à l'application du RGPD1 et qui, en cohérence avec les principes d'autonomie et de responsabilité individuelle de chacune des sociétés du Groupe, s'engagent à transposer et à adopter le présent Modèle organisationnel, en définissant les principes de gouvernance et de contrôle en matière de contrôle des données à caractère personnel conformément au présent Modèle organisationnel.

Toute référence à la Société contenue dans le présent Modèle Organisationnel devra être considérée comme étant destinée à chacune des sociétés du Groupe.

3. Définitions

En plus des définitions fournies ci-dessus, les définitions suivantes s'appliquent aux fins du présent modèle d'organisation :

« **archives** » : ensemble structuré de données à caractère personnel qui sont accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de façon fonctionnelle ou géographique ;

« **Autorité de contrôle** » : l'autorité publique indépendante instituée par un État membre conformément à l'art. 51 du RGPD (https ://edpb.europa.eu/about-edpb/board/members_en) ;

[1] Conformément à l'art. 3 du Règlement, le Règlement s'applique (i) au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement par un responsable du traitement ou un sous-traitant établi dans l'Union Européenne, indépendamment du fait que le traitement soit effectué ou non au sein de l'Union ainsi que (ii) au traitement des données à caractère personnel de personnes concernées qui se trouvent dans l'Union, effectué par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités sont liées : (a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

« **consentement de la personne concernée** » : toute manifestation de la volonté libre, spécifique, éclairée et non équivoque de la personne concernée, celle-ci marque son consentement, par déclaration ou action positive non équivoque, à ce que les données personnelles la concernant fassent objet de traitement.

«Data Steward» : la personnes qui, choisie par le responsable de l'unité organisationnelle d'appartenance, est amenées à superviser et à veiller au respect du Modèle Organisationnel par les Destinataires, assister la Société dans l'application des Politiques de la protection de la vie privée et agir en tant que principaux référents concernant les questions en matière de traitement des données à caractère personnel au sein de leur unité organisationnelle ainsi que faire office de point de contact pour les personnes concernées et les Destinataires ;

« **données biométriques** » : les données à caractère personnelles obtenues à partir d'un traitement technique spécifique liées aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment l'identification univoque, telle que l'image faciale ou les données dactyloscopiques.

« **données génétiques** » : les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui fournissent des informations univoques sur la physiologie ou la santé de ladite personne physique, et qui résultent notamment de l'analyse d'un échantillon biologique de la personne physique en question ;

« **données concernant la santé** » : les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la fourniture de services de soins de santé, qui divulguent des informations relatives à son état de santé ;

« **donnée à caractère personnel** » : toute information concernant une personne physique identifiée ou identifiable (la « **personne concernée** ») ; une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par un identifiant tel que le nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, psychologique, économique, culturelle ou sociale.

« **limitation du traitement** » : le marquage de données à caractère personnel stockées dans le but de limiter leur traitement à l'avenir ;

« **Loi sur la protection de la vie privée** » : toutes les dispositions législatives ou réglementaires applicables en matière de protection des données à caractère personnel, y compris, à titre d'exemple mais non limitatif, les dispositions du RGPD et la législation nationale en matière de protection des données à caractère personnel ainsi que les mesures et directives de l'Autorité de contrôle ;

« **Pays tiers** » : pays situés hors de l'Espace Economique Européen ;

« **Politique de la protection de la vie privée**» : les politiques et procédures adoptées par la Société en vue de réglementer les divers aspects liés au traitement des données à caractère personnel, faisant partie intégrante et substantielle du présent Modèle Organisationnel, y compris, à titre d'exemple mais non limitatif, les politiques jointes au présent Modèle Organisationnel ;

« **Expert de la protection de la vie privée**» : les entités désignées directement par la Société qui, dans le cadre de l'exécution de leurs fonctions et dans les limites des pouvoirs qui leur sont conférés, font office de points de contact pour les Data Stewards pour ce qui est des questions en matière de traitement des données à caractère personnel et, en particulier, des questions relatives au respect du présent Modèle Organisationnel et de la Norme en matière de confidentialité par la Société ;

« **profilage** » : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique,

notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ;

« **pseudonymisation** » : le traitement de données à caractère personnel de telle sorte que ces données ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles garantissant qu'elles ne peuvent être attribuées à une personne physique identifiée ou identifiable ;

« **sous-traitant du traitement** » : la personne physique ou morale, l'autorité publique, le service ou un organisme autre qui traite des données à caractère personnel pour le compte du titulaire du traitement ;

« **tiers** » : une personne physique ou morale, une autorité publique, un service ou un autre organisme distinct que la personne concernée, le responsable du traitement, le sous-traitant et les personnes autorisées à traiter des données à caractère personnel sous l'autorité directe du responsable du traitement ou du sous-traitant ;

« **responsable du traitement** » : la personne physique ou morale, l'autorité publique, le service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ;

« **traitement** » : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, 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, la limitation, l'effacement ou la destruction ;

« **violation des données à caractère personnel** » : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, stockées ou traitées autrement.

Les expressions au singulier conserveront le même sens au pluriel si le contexte l'exige.

4. Rôles et responsabilités

Le Modèle Organisationnel dont la Société s'est dotée s'articule sur différents niveaux, en reconnaissant les pouvoirs et les responsabilités des différentes parties :

le titulaire du traitement est la Société dont la tâche est de déterminer les finalités et les moyens du traitement des données à caractère personnel ainsi que de prendre les mesures techniques et organisationnelles aptes à garantir, et à démontrer, la Loi sur la protection de la vie privée. En particulier, le Responsable du traitement est amené, à titre d'exemple mais non limitatif, à adopter dès la conception les solutions de confidentialité et de protection des données par défaut ; à mettre à jour le registre des traitements ; à mettre en place les notes d'information relatives au traitement des données à caractère personnel ; à préparer toute réalisation organisationnelle nécessaire à garantir l'exercice des droits des parties intéressées ; à faire adopter toutes les mesures prescrites par l'Autorité de contrôle ; à effectuer l'analyse d'impact relative à la protection des données conformément à l'art. 35 du RGPD ; à consulter l'Autorité de contrôle dans les cas et selon les modalités prévus à l'art. 36 du RGPD ; à souscrire avec les responsables du traitement l'accord prévu à l'art. 28 du RGPD ;

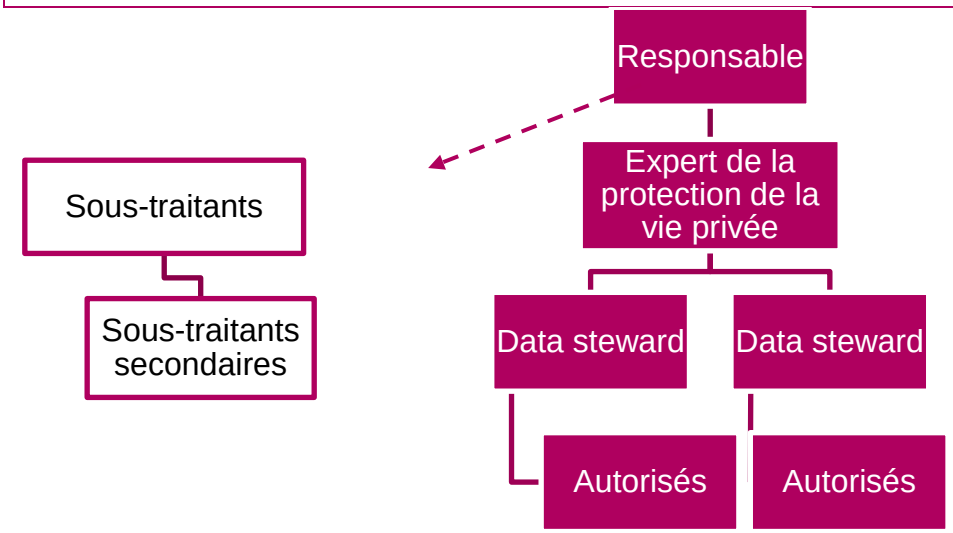
les responsables du traitement sont les entités tierces, extérieures à l'organisation de la Société, qui effectuent pour le compte et conformément aux instructions du titulaire les opérations de traitement des données dont la Société est responsable ; les responsables du traitement doivent souscrire avec le titulaire l'accord visé à l'art. 28 du RGPD ;

les sous-traitants secondaires sont les entités tierces, extérieures à l'organisation de la Société, à qui le responsable du traitement confie l'exécution d'activités de traitement déterminées par la signature d'un accord spécifique qui impose au sous-traitant secondaire les mêmes obligations en matière de protection des données que celles contenues dans l'accord signé avec le responsable du traitement mentionné ci-dessus;

les personnes autorisées au traitement des données sont toutes les personnes physiques qui effectuent des opérations de traitement des données à caractère personnel sur instruction du responsable, y compris les employés de la Société qui opèrent à quelque titre que ce soit sous l'autorité directe de la Société ;

les Experts de la protection de la vie privée sont les entités désignées directement par la Société qui, dans le cadre de l'exécution de leurs fonctions et dans les limites des pouvoirs qui leur sont conférés, font office de points de contact pour les Data Stewards pour ce qui est des questions en matière de traitement des données à caractère personnel et, en particulier, des questions relatives au respect du présent Modèle Organisationnel et de la Norme en matière de la protection de la vie privée par la Société ; les experts de la protection de la vie privée peuvent être contactés en écrivant à l'adresse privacyexpert@falckrenewables.com

les Data Stewards sont les personnes qui, choisies par le responsable de l'unité organisationnelle d'appartenance, sont amenées à superviser et à veiller au respect du Modèle Organisationnel de la part des Destinataires, assister la Société dans l'application des Politiques de la protection de la vie privée et agir en tant que référents principaux pout tout ce qui concerne les questions en matière de traitement des données à caractère personnel au sein de leur unité organisationnelle ainsi que de faire office de point de contact pour les personnes concernées et les Destinataires.



5. Principes applicables au traitement

Les traitements mis en œuvre par la Société se font exclusivement dans le respect des principes identifiés par l'article 5 du RGPD selon lequel les données personnelles sont :

traitées de façon licite, correcte et transparente à l'égard de la personne concernée ;

recueillies dans des finalités déterminées, explicites et légitimes, puis, traitées successivement d'une façon non incompatible avec ces finalités ;

appropriées, pertinentes et limitées à ce qui est nécessaire par rapport aux finalités pour lesquelles elles ont été traitées ;

exactes et, si nécessaire, actualisées ; toutes les mesures raisonnables doivent être adoptées pour effacer ou

rectifier dans les meilleurs délais les données inexactes en rapport aux finalités pour lesquelles elles sont traitées ;

conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées ;

traitées de manière à garantir une sécurité adéquate des données à caractère personnel, y compris la protection, par des mesures techniques et organisationnelles appropriées, contre les traitements non autorisés ou illicites et contre la perte, la destruction ou les dommages accidentels.

À cette fin, les Destinataires sont tenus de vérifier, avant de réaliser un traitement des données à caractère personnel, le respect des principes indiqués plus haut.
En cas de doutes relatifs à l'application correcte des principes en rapport au traitement spécifique, les Destinataires peuvent s'adresser au Data Steward.

6. Licéité du traitement

Les traitements effectués par la Société se font exclusivement dans le respect des critères de licéité identifiés par l'article 6 du RGPD conformément auquel le traitement est licite uniquement et dans la mesure où au moins l'une des conditions suivantes est remplie :

la personne concernée a donné son consentement au traitement de ses données à caractère personnel pour l'une ou plusieurs finalités spécifiques ;

le traitement est nécessaire à l'exécution d'un contrat dont la personne concernée fait partie ou à l'exécution de mesures précontractuelles adoptées à sa demande ;

le traitement est nécessaire pour satisfaire une obligation légale à laquelle le responsable du traitement est soumis ;

le traitement est nécessaire à la préservation des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

le traitement est nécessaire à l'exécution d'une tâche d'intérêt public ou liée à l'exercice de pouvoirs publics dont le responsable du traitement est investi ;

le traitement est nécessaire à la réalisation de l'intérêt légitime du responsable du traitement ou de tiers à moins que ne prévalent les intérêts ou les droits et les libertés fondamentales de la personne concernée demandant la protection des données à caractère personnel, en particulier, si la personne concernée est un mineur.

À cette fin, les Destinataires sont tenus de vérifier, avant un traitement des données à caractère personnel, l'existence d'au moins une des exigences de licéité susmentionnées.
En cas de doutes relatifs à la licéité du traitement ou concernant la base juridique à utiliser en rapport au traitement spécifique, les Destinataires peuvent s'adresser au Data Steward.

6.1 Le consentement

Lorsque le traitement est basé sur le consentement, le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement des données à caractère personnel. Le consentement doit être :

libre (la personne concernée doit réellement avoir la capacité de choisir ainsi que le contrôle sur ses données, ne pas se sentir obligée de donner son consentement ou subir des conséquences négatives si elle ne donne pas son consentement ;

spécifique (il doit être exprimé en rapport à une ou plusieurs finalités spécifiques et la personne concernée doit pouvoir choisir en rapport à chacune d'elles) ;

éclairé (fournir des informations aux personnes concernées avant d'en obtenir le consentement est fondamental afin de leur permettre de prendre des décisions éclairées, comprendre ce à quoi elles donnent leur consentement et, par exemple, exercer le droit de retirer leur consentement) ;

non équivoque (nécessitant une déclaration ou une action positive non équivoque de la part de la personne concernée, ce qui signifie que le consentement doit toujours être exprimé soit par une déclaration, soit activement; le silence, l'inactivité ou la présélection de cases ne doit pas valoir comme consentement donné).

La personne concernée a le droit de retirer son consentement à tout moment et le retrait du consentement ne porte pas préjudice à la licéité du traitement basé sur le consentement avant son retrait. Avant de donner son consentement, la personne concernée doit en être informée en ce sens. Le consentement est retiré avec la même facilité avec laquelle il est donné.[2]

À la lumière de ce qui précède, les Destinataires sont tenus de vérifier, avant un traitement des données à caractère personnel, l'existence des conditions susmentionnées.

En cas de nouvelles opérations de traitement basées sur le consentement, la rédaction et/ou la mise à jour des formulaires de consentement de la Société est du ressort de l'Expert en protection de la vie privée, avec le soutien des Data Steward et/ou des responsables de l'unité organisationnelle concernée. Il est convenu que l'Expert en protection de la vie privée pourra, après avoir évalué la complexité de l'activité demandée, et après communication à la Société, avoir recours à des conseillers externes pour l'exécution de l'activité même.

Il est également convenu que les Destinataires ne pourront en aucun cas modifier ou mettre à jour les formulaires de consentement de la Société sans l'autorisation écrite préalable de l'Expert en protection de la vie privée. En cas de doutes, les Destinataires peuvent s'adresser au Data Steward.

6.2 L'intérêt légitime

L'intérêt légitime est l'un des critères qui légitiment le traitement des données à caractère personnel par le responsable du traitement. De fait, il prévoit que l'intérêt légitime du responsable du traitement, ou bien des tiers auxquels les données sont communiquées, soit évalué par rapport aux intérêts ou aux droits fondamentaux de la personne concernée. L'issue de ce test comparatif permet d'établir si l'intérêt légitime peut être invoqué comme fondement juridique pour le traitement des données à caractère personnel.

Pour effectuer ce test, il faut évaluer pleinement toute une série de facteurs pour qu'il soit possible de garantir que les intérêts et les droits fondamentaux des personnes concernées soient dûment pris en compte. En même temps, le test comparatif est adaptable, il peut varier de simple à complexe et ne doit pas résulter indûment lourd. Parmi les facteurs dont tenir compte dans l'exécution du test comparatif, figurent :

- la nature et l'origine de l'intérêt légitime ainsi que l'éventualité que le traitement des données est nécessaire à l'exercice d'un droit fondamental ou encore à l'exécution d'une tâche d'intérêt public ou reconnue par la communauté concernée ;
- l'impact sur les personnes concernées et leurs attentes raisonnables sur le sort des données les concernant ainsi que la nature des données et les modalités du traitement ;

des garanties supplémentaires qui pourraient limiter l'impact indu sur la personne concernée, comme la

[2] Pour en savoir plus à ce propos, voir également les Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 du Groupe de travail « Article 29 ».

minimisation des données, les technologies de renforcement de la protection de la vie privée, une meilleure transparence, le droit général et inconditionné de retrait et la portabilité des données.

Compte tenu de ce qui précède, les Destinataires sont tenus de vérifier, avant un traitement des données à caractère personnel basé sur l'intérêt légitime, que le responsable du traitement ait procédé à l'analyse de l'intérêt légitime susmentionnée.

En cas de nouvelles opérations de traitement basées sur l'intérêt légitime, la rédaction et/ou la mise à jour de l'analyse de l'intérêt légitime de la Société sont du ressort de l'Expert en protection de la vie privée, assisté des Data Steward et/ou des responsables de l'unité organisationnelle de référence. Il est convenu que l'Expert en protection de la vie privée pourra, après avoir évalué la complexité de l'activité demandée et après communication à la Société, avoir recours à des conseillers externes pour l'exécution de l'activité même.

Il est également convenu que les Destinataires ne pourront en aucun cas modifier ou mettre à jour les analyses de l'intérêt légitime de la Société sans l'autorisation écrite préalable de l'Expert en protection de la vie privée En cas de doutes, les Destinataires peuvent s'adresser au Data Steward.

7. Transparence

En cas de collecte de données relatives à la personne concernée, le responsable du traitement fournit à celle-ci, au moment où les données à caractère personnel sont collectées, les informations prévues par l'art. 13 du RGPD. En effet, les modalités selon lesquelles les données à caractère personnel concernant les personnes physiques sont collectées, consultées ou traitées d'une autre manière doivent être transparentes, idem pour ce qui est de la mesure selon laquelle les données à caractère personnel sont ou seront traitées. Le principe de transparence exige que les informations et les communications relatives au traitement de ces données à caractère personnel soient facilement accessibles et compréhensibles et qu'un langage simple et clair soit utilisé.

Le responsable communique aux personnes concernées les informations suivantes avant de réaliser un traitement des données à caractère personnel :

a) l'identité et les coordonnées du responsable du traitement et, si applicable, de son représentant ;
b) les coordonnées du délégué à la protection des données, si applicable ;
c) les finalités du traitement pour lesquelles les données à caractère personnel sont destinées ainsi que la base juridique du traitement ;
d) les intérêts légitimes du responsable du traitement ou de tiers, si applicables ;
e) les éventuels destinataires ou les éventuelles catégories de destinataires des données à caractère personnel ;
f) si applicable, l'intention du responsable du traitement de transférer les données à caractère personnel vers un pays tiers ou vers une organisation internationale et l'existence ou l'absence d'une décision d'aptitude de la Commission ou la référence aux garanties appropriées ou opportunes ainsi que les moyens pour obtenir une copie de ces données ou le lieu où elles sont rendues disponibles.
g) la durée de conservation des données à caractère personnel ou, si cela n'est pas possible, les critères utilisés pour déterminer cette durée ;
h) l'existence du droit de la personne concernée à demander au responsable du traitement l'accès aux données à caractère personnel et la rectification ou leur effacement ou la limitation du traitement la concernant ou à s'opposer à leur traitement, en plus que du droit à la portabilité des données ;

i) l'existence du droit à retirer le consentement à tout moment sans porter préjudice à la licéité du traitement basée sur le consentement accordé avant son retrait, si applicable ;

j) le droit d'introduire une réclamation auprès d'une Autorité de contrôle.

k) si la communication des données à caractère personnel est une obligation légale ou bien une exigence nécessaire à la conclusion d'un contrat et si la personne concernée a l'obligation de fournir les données à caractère personnel ainsi que les conséquences possibles en cas de non-communication de ces données ;

l) l'existence d'un processus de prise de décision automatisé, y compris le profilage et, au moins dans ces cas, les informations significatives concernant la logique appliquée ainsi que l'importance et les conséquences attendues de ce traitement pour la personne concernée.

Compte tenu de ce qui précède, les Destinataires sont tenus de vérifier, avant de réaliser un traitement des données à caractère personnel, que les informations visées plus haut soient fournies correctement aux personnes concernées à travers les notes d'information prévues à cet effet et mises en place par la Société. En cas de doutes, les Destinataires peuvent s'adresser au Data Steward.

En cas de nouvelles opérations de traitement, la rédaction et/ou la mise à jour des notes d'information de la Société sont du ressort de l'Expert en protection de la vie privée, assisté des Data Stewards et/ou des responsables de l'unité organisationnelle de référence. Il est convenu que l'Expert en protection de la vie privée pourra, après avoir évalué la complexité de l'activité demandée et après communication à la Société, avoir recours à des conseillers externes pour l'exécution de l'activité même.

Il est également convenu que les Destinataires ne pourront en aucun cas modifier ou mettre à jour les notes d'information de la Société sans l'autorisation écrite préalable de l'Expert en protection de la vie privée.

8. Conservation

L'un des principes généraux établis par le RGPD est que les données à caractère personnel doivent être stockées sous une forme permettant l'identification des personnes concernées sur une période de temps non supérieure à la réalisation des finalités pour lesquelles elles sont traitées. À l'issue de cette période, les données doivent être supprimées ou rendues anonymes parce qu'elles ne sont plus nécessaires par rapport aux finalités pour lesquelles elles ont été collectées ou traitées.[3]

Des obligations de stockage obligatoire peuvent également être prescrites par des normes, même sectorielles, ou des obligations contractuelles dérivant d'accords pris avec des prestataires de services ou des partenaires commerciaux.

[3] Pour que certaines données soient rendues anonymes, elles doivent être privées d'éléments suffisants afin d'empêcher l'identification de la personne concernée. Plus précisément, les données doivent être traitées de sorte à ne plus pouvoir être utilisées pour identifier une personne physique en utilisant « *l'ensemble des moyens qui peuvent être raisonnablement utilisés* » par le responsable du traitement ou par d'autres entités. Et cette procédure doit être irréversible. Parmi les techniques d'anonymisation les plus utilisées, se trouvent les techniques basées sur la randomisation qui modifie la véracité des données afin d'en éliminer l'étroite corrélation qui existe entre les données et la personne (à savoir si les données sont suffisamment incertaines, elles ne peuvent plus être mises en relation avec une personne spécifique) et les techniques basées sur la généralisation qui « dilue » les attributs des personnes concernées, en modifiant l'échelle ou l'ordre de grandeur respectif (à savoir une région au lieu d'une ville, un mois au lieu d'une semaine).

Afin de garantir le respect du principe de limitation de la conservation susmentionné, la Société a adopté une politique portant sur les durées de conservation visée à l'Annexe E, dont le but est d'illustrer les durées de conservation qui devront être respectées dans les activités de traitement réalisées par les Destinataires.

À la lumière de ce qui précède et dans le cadre des activités de traitement réalisées par les Destinataires, ces derniers sont tenus de vérifier le respect ponctuel des durées de conservation susmentionnées. En cas de doutes, les Destinataires peuvent s'adresser au Data Steward.

9. Accord avec les sous-traitants du traitement

Lorsqu'un traitement doit être effectué pour le compte de la Société, celle-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée.

De plus, la Société stipule avec le sous-traitant un contrat spécifique conforme à l'art. 28 du RGPD qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.

Compte tenu de ce qui précède, avant de procéder à tout traitement de données à caractère personnel nécessitant l'intervention d'un responsable du traitement, les Destinataires doivent s'assurer que la Société a signé le contrat susmentionné avec le responsable du traitement. En cas de doute, les Destinataires peuvent contacter le Data Steward.

En cas de nouvelles opérations de traitement nécessitant l'implication d'un sous-traitant, la rédaction et/ou la négociation du contrat susmentionné est du ressort de l'Expert en protection de la vie privée, avec le soutien des Data Stewards et/ou des responsables de l'unité organisationnelle de référence. Il est convenu que l'Expert en protection de la vie privée pourra, après avoir évalué la complexité de l'activité demandée et après communication à la Société, avoir recours à des conseillers externes pour l'exécution de l'activité même.

Les Data Stewards devront tenir une liste complète des entités tierces désignées comme responsables du traitement et, si possible, de tout sous-traitant secondaire au sein de l'unité organisationnelle d'appartenance ainsi que communiquer dans les meilleurs délais toute mise à jour et/ou modification de cette liste à l'Expert en protection de la vie privée.

La liste complète des sous-traitants et, si possible, des sous-traitants secondaires de la Société est consultable auprès de l'Expert en protection de la vie privée.

10. Transfert des données à caractère personnel vers des pays tiers

Tout transfert des données à caractère personnel en cours de traitement ou destiné à être traité après le transfert vers un pays tiers, y compris les transferts successifs de données à caractère personnel d'un pays tiers vers un autre pays tiers, ne peut avoir lieu que si le responsable du traitement et le sous-traitant respectent les conditions prévues aux art. 44 et suivants du RGPD.

En particulier, le transfert des données ne peut avoir lieu que si au moins une des conditions suivantes est remplie :

a) le pays tiers a reçu de la part de la Commission européenne une décision d'adéquation :[4]

b) le responsable a fourni des garanties adéquates et à condition que les personnes concernées disposent de droits exerçables et de réels moyens de recours (par exemple, les règles d'entreprise contraignantes et les clauses types de protection des données adoptées par la Commission européenne constituent des garanties adéquates).

À la lumière de ce qui précède, les Destinataires sont tenus de vérifier, avant de réaliser un traitement des données à caractère personnel qui prévoit le transfert des données à caractère personnel vers un pays tiers, l'existence d'au moins l'une des exigences susmentionnées. En cas de doutes relatifs au transfert des données à caractère personnel vers des pays tiers, les Destinataires peuvent s'adresser au data steward.

11. Droits de la personne concernée

Le RGPD permet à la personne concernée d'exercer à tout moment les droits suivants :

- droit d'accès aux données à caractère personnel et aux informations suivantes : finalités du traitement, catégories de données à caractère personnel en question, destinataires ou catégories de destinataires auxquels les données à caractère personnel peuvent être communiquées, la durée de conservation des données à caractère personnel (si possible) ainsi que, lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toutes les informations disponibles sur leur origine ;
- droit de rectification des données à caractère personnel inexactes ;
- droit d'obtenir l'effacement des données à caractère personnel la concernant ;
- droit de demander la limitation du traitement ;
- droit de recevoir ou de demander le transfert des données à caractère personnel la concernant qui sont en possession du responsable dans un format structuré, couramment utilisé et lisible, pour d'autres usages personnels ou pour les fournir à un autre responsable de traitement ;
- droit de s'opposer au traitement ;
- droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé des données à caractère personnel la concernant, si présent, produisant des effets juridiques la concernant ou l'affectant de manière significative ;
- droit de retirer son consentement, aussi pour les finalités liées à l'envoi des communications commerciales (vaut seulement pour l'avenir) ;
- droit d'introduire une réclamation auprès d'une autorité de contrôle.

Il se peut que des limitations soient applicables aux droits mentionnés plus haut lorsque, de leur exercice, peut dériver un préjudice effectif et concret, par exemple, aux intérêts légitimes du responsable du traitement et, bien que l'exercice des droits est normalement gratuit, le responsable du traitement peut se réserver le droit de demander une contribution en cas de demandes manifestement non fondées ou excessives.

Le responsable du traitement doit donner suite à la demande de la personne concernée dans les meilleurs délais et, dans tous les cas, au plus tard un mois à compter de la réception de la demande même. Ce délai peut être prolongé de deux mois si nécessaire, en cas de complexité et du nombre des demandes. Il est convenu que, en cas de prolongement, le responsable du traitement devra en informer la personne concernée, en lui précisant les

[4] Les décisions prises à ce jour sur l'adéquation, en vigueur jusqu'à leur modification, remplacement ou abrogation par la Commission européenne, sont énumérées sur le site web de la Commission européenne (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

raisons du retard, le tout sous un mois à compter de la réception de la demande.

Les Destinataires sont tenus d'assister la Société afin de lui permettre de gérer convenablement les demandes présentées par les personnes concernées et, le cas échéant, à les communiquer dans les meilleurs délais au Data Steward qui veillera à les communiquer, à son tour, à l'Expert en protection de la vie privée, afin qu'il soit possible de donner un retour d'information aux parties intéressées dans les conditions impératives indiquées ci-dessus..

12. Violation des données à caractère personnel

Le RGPD prévoit qu'un responsable du traitement, dès qu'il a connaissance d'une violation des données à caractère personnel, notifie cette violation à l'autorité compétente, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que le responsable du traitement ne soit pas en mesure de démontrer que, conformément au principe de responsabilisation, la violation en question n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

En effet, une violation des données à caractère personnel peut, si elle n'est pas traitée de façon adéquate et rapide, engendrer des dommages physiques, matériels ou immatériels aux personnes physiques, par exemple, comme la perte de contrôle des données à caractère personnel les concernant ou la limitation de leurs droits, la discrimination, le vol ou l'usurpation d'identité, des pertes financières, le déchiffrage non autorisé de la pseudonomysation, porter préjudice à la réputation, la perte de confidentialité des données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social significatif au détriment de la personne physique concernée.

Ci-dessus la liste de quelques exemples de violations des données à caractère personnel qui devront être communiquées dans les meilleurs délais au Data Steward :

- perte d'une sauvegarde contenant des données à caractère personnel ;
- accès à des bases de données par des entités non autorisées ;
- attaque au système informatique ;
- vol ou perte d'ordinateurs de bureau, d'ordinateurs portables, de dispositifs électroniques portables, clés USB, smartphones/tablettes de la Société ;
- vol d'identité et/ou *hameçonnage*.

Afin de garantir la gestion convenable de la violation de données à caractère personnel, la limitation des effets préjudiciels de celle-ci ainsi que le respect des obligations de notification susmentionnées, la Société a mis en place une procédure pour la gestion des violations des données à caractère personnel visée à l'Annexe D, le but étant d'illustrer les modalités à travers lesquelles la Société identifie les actions nécessaires à mettre en place dans les cas où une violation des données à caractère personnel se matérialiserait ou serait suspectée. Ladite procédure identifie également les entités chargées d'évaluer la gravité de la violation des données à caractère personnel.

À cette fin, les Destinataires sont tenus, conformément à ce que prévoit la procédure susmentionnée, à signaler toute violation potentielle des données à caractère personnel dont ils seraient amenés à prendre connaissance, en contactant dans les meilleurs délais le Data Steward ainsi que d'assister la Société afin de permettre une gestion convenable de la violation des données à caractère personnel.

13. Registre des activités de traitement

Le responsable du traitement a l'obligation de tenir un registre des activités de traitement réalisées, placées sous sa propre responsabilité. Ce registre contient toutes les informations suivantes, telles que prévues par l'art. 30 du RGPD :

a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
b) les finalités du traitement ;
c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers et les documents attestant de l'existence de garanties appropriées ;
f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en place.

Compte tenu de ce qui précède, la Société a prévu de mettre en place le registre des traitements afin de cartographier les différentes opérations de traitement des données à caractère personnel effectuées sous sa propre responsabilité, d'effectuer une analyse d'impact et une planification des traitements appropriées.

La mise à jour et l'intégration du registre des traitements sont confiées par la Société à l'Expert en protection de la vie privée lequel, avec une fréquence minimum semestrielle, met à jour le registre en fonction des communications de mise à jour fournies, avec une fréquence minimum trimestrielle, par les Data Stewards, en référence à l'unité organisationnelle d'appartenance.

14. Analyse d'impact

Si un type de traitement, lorsqu'il implique notamment l'utilisation de nouvelles technologies, compte tenu de la nature, de l'objet, du contexte et des finalités du traitement, est susceptible de présenter un risque élevé au regard des droits et libertés des personnes physiques, le responsable du traitement procède, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.[5]

Il s'agit de l'un des éléments les plus importants du nouveau cadre normatif car il exprime clairement la responsabilisation du responsable du traitement à l'égard des opérations de traitement effectuées.

L'analyse d'impact est obligatoire dans tous les cas où un traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques. Parmi les cas où une analyse d'impact peut se révéler nécessaire, figurent les suivants :

[5] Pour plus de détails, voir également les Lignes directrices concernant l'analyse d'impact relative à la protection des données à caractère personnel et détermination, le cas échéant, si le traitement est « susceptible d'engendrer un risque élevé » au sens du Règlement 2016/679 du Groupe de travail « Article 29 ».

- les traitements d'analyse et évaluation, y compris le profilage ;
- décisions automatisées qui produisent des effets juridiques significatifs (par ex. : embauches) ;
- surveillance systématique (par ex. : surveillance vidéo) ;
- traitement de données sensibles, judiciaires ou de nature extrêmement personnelle (par ex. : informations sur les idées politiques) ;
- traitements des données à caractère personnel à grande échelle ;
- combinaison ou comparaison d'ensembles de données dérivant de deux ou plusieurs traitements réalisés pour des finalités différentes et/ou par des responsables de traitement distincts, selon les modalités ressortant du consentement initialement donné (comme cela advient, par exemple, avec les mégadonnées) ;
- données relatives à des personnes vulnérables (mineurs, personnes atteintes de troubles psychiatriques, demandeurs d'asile, personnes âgées) ;
- utilisations innovantes ou application de nouvelles solutions technologiques ou organisationnelles (par ex. : reconnaissance faciale, dispositifs IdO) ;
- traitements qui, en soi, pourraient empêcher les personnes concernées d'exercer un droit ou d'avoir recours à un service ou à un contrat.

L'analyse d'impact contient au minimum :

a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement par rapport aux finalités ;
c) une évaluation des risques pour les droits et libertés des personnes concernées ;
d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

L'analyse d'impact doit être effectuée avant de procéder au traitement et, toutefois, il convient de prévoir un réexamen continu de l'évaluation, l'évaluation devant être répétée à intervalles réguliers.

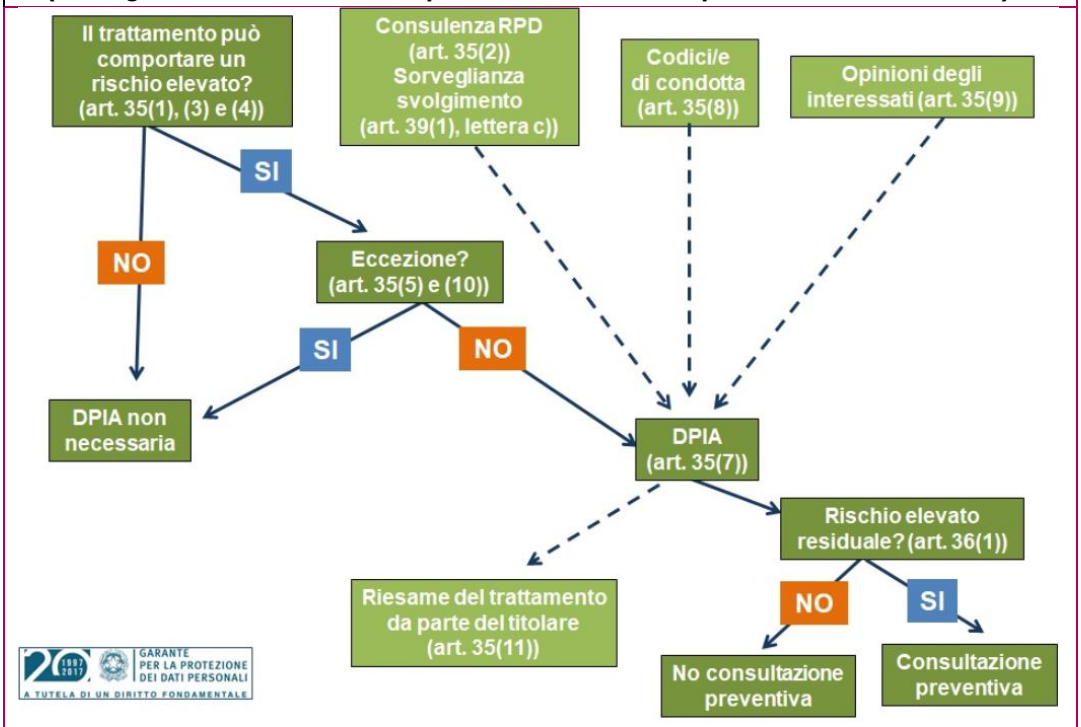
En ce sens, l'analyse d'impact permet de respecter concrètement les principes de la protection des données dès la conception et de la protection des données par défaut tel que visé à l'art. 25 du RGPD de n'importe quel traitement. En effet, compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées qui sont destinées à mettre en œuvre les principes relatifs à la protection des données de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée (Principes de *privacy-by-design* - protection de la vie privée dès la conception).
De la même façon, le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées (principe de *privacy-by-default* - protection des données par défaut).

À la lumière de ce qui précède et afin de garantir l'exécution convenable de l'analyse d'impact ainsi que le respect des principes de protection de la vie privée dès la conception et par défaut, susmentionnés, la Société a rédigé le document visé à l'Annexe B. Celui-ci devra être considéré

comme support, à adapter à la particularité d'un cas spécifique, pour l'exécution de l'analyse d'impact.

La Société a confié à l'Expert en protection de la vie privée les activités relatives à l'exécution de l'analyse d'impact, y compris la phase de choix préalable sur la nécessité de la réaliser ou non. Ces activités devront être réalisées en accord avec le Data Steward et/ou le responsable de l'unité organisationnelle de référence ainsi que les Destinataires concernés. L'Expert en protection de la vie privée devra donc être informé par le Data Steward et/ou le responsable de l'unité organisationnelle de référence en cas de nouveau projet. En accord avec la Société, l'Expert en protection de la vie privée pourra, après avoir évalué la complexité de l'activité demandée, avoir recours à des conseillers externes pour l'exécution de l'activité même.

Quand faut-il procéder à une évaluation d'impact sur la protection des données (en anglais *Data Protection Impact Assessment* ci-après dénommée "DPIA") ?



15. Surveillance et contrôle

Afin de vérifier le respect du présent Modèle Organisationnel et de la norme en matière de protection de la vie privée par les Destinataires, y compris les sous-traitants, la Société met en œuvre, au moins une fois par an, des opérations de surveillance et de contrôle des traitements effectués par la Société et du respect, de la part des Destinataires, du Modèle organisationnel.

Compte tenu de ce qui précède, la société a confié les activités de surveillance et de contrôle décrites ci-dessus à l'Expert en protection de la vie privée.

Suite à ces contrôles, l'Expert en protection de la vie privée enverra, au moins une fois par an, à l'administrateur délégué de la Société et, par connaissance, à l'organe d' Audit Interne, un rapport À la suite de ces contrôles, l'expert en protection de la vie privée enverra, au moins une fois par an, au directeur général de la Société et, pour information, à l'Audit Interne, un rapport indiquant, entre autres, les demandes reçues de l'autorité de surveillance, les éventuels manquements aux exigences de protection des données à caractère personnel et les mesures correctives pertinentes, les risques ou les problèmes

importants liés au traitement des données à caractère personnel, une liste des analyses d'impact réalisées et/ou suggérées, les nouveaux projets et leur conformité avec les principes de protection de la vie privée lors de leur conception et par défaut.

16. Formation

Pour un fonctionnement efficace du Modèle Organisationnel, la formation des Destinataires autorisés au traitement est gérée par la Société en étroite collaboration avec l'Expert en protection de la vie privée et la division ressources humaines de la Société. En particulier, les formations portent sur l'intégralité du Modèle Organisationnel, à savoir sur toutes ses composantes, ainsi que sur les notions relatives à la législation en matière de protection de la vie privée.

La participation aux formations fait l'objet d'une surveillance à travers un système de relevé des présences. Au terme de chaque formation, chaque participant est soumis à un test final afin d'en évaluer le niveau d'apprentissage atteint et l'orienter vers d'autres formations. La participation aux formations est obligatoire pour tous les Destinataires autorisés au traitement par la Société. Cette obligation constitue une règle fondamentale du présent Modèle Organisationnel dont la violation est subordonnée à l'application des sanctions prévues dans le système disciplinaire.

Les Destinataires de la formation sont tenus de :

acquérir la connaissance des principes et du contenu du Modèle Organisationnel ;

connaître les modalités de travail selon lesquelles réaliser leur propre activité ;

contribuer activement, en rapport à leur propre rôle et responsabilités, à la mise en œuvre efficace du Modèle organisationnel, en en signalant les éventuelles lacunes constatées.

17. Non-respect du Modèle Organisationnel

Il est porté à la connaissance de tous les Destinataires que le présent Modèle Organisationnel ainsi que les politiques de la protection de la vie privée qui en font partie intégrante et substantielle, revêt un caractère contraignant pour les Destinataires.

Une violation du Modèle Organisationnel ainsi que des politiques de la protection de la vie privée peuvent avoir de graves répercussions sur la Société et comporter, à l'égard des Destinataires salariés de la Société défaillants, l'application de mesures disciplinaires, conformément aux dispositions légales et à l'accord de négociation collective applicable et, à l'égard des Destinataires non-salariés de la Société, la fin de la relation contractuelle avec la Société, sans préjudice d'une éventuelle action pour protéger les droits de la Société.

Les comportements qui constituent une violation du présent Modèle Organisationnel peuvent déterminer, parallèlement, la violation de dispositions légales telles à rendre les Destinataires défaillants passibles de poursuites civiles et pénales.

La Société aussi peut être poursuivie et sanctionnée en raison d'une conduite défaillante des Destinataires et la violation des dispositions prévues par le RGPD peut entraîner l'application d'amendes administratives allant jusqu'à 20 000 000 euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

18. Mises à jour et modifications

Le présent Modèle Organisationnel peut être mise à jour, modifié ou intégré à tout moment par la Société. Le cas échéant, les modifications seront portées à l'attention des Destinataires dans les meilleurs délais, à travers leur publication sur les canaux d'information de la Société. À cette fin, les Destinataires sont tenus de consulter

périodiquement les canaux de communication internes et prendre connaissance de la version à jour du Modèle organisationnel.

19. Contacts

En cas de questions ou de doutes sur le présent Modèle Organisationnel ou les politiques de confidentialité, veuillez contacter l'Expert en protection de la vie privée en écrivant à l'adresse suivante : privacyexpert@falckrenewables.com.

20. Liste des pièces jointes

A. Politique sur l'utilisation des outils informatiques (17)
B. Analyse d'impact sur la protection des données (25)
C. F.A.Q. (32)
D. Politique sur la violation des données (**Errore. Il segnalibro non è definito.**)
E. Politique sur la conservation des données (45)

Annexe A
Politique d'utilisation des outils informatiques

1. Champ d'application

L'objectif de la présente politique est de définir les règles et les modalités suivant lesquelles les salariés, les collaborateurs et les conseillers de la Société (les « **Utilisateurs** ») peuvent utiliser leur ordinateur portable, leur tablette, leur smartphone, leurs périphériques (y compris la *webcam*, les micros et les périphériques audio) et tout autre outil informatique qui leur est attribué ou mis à disposition par la Société (les « **outils informatiques** ») pour l'accomplissement de leurs tâches.

Les définitions du Modèle Organisationnel s'appliquent à la présente politique. Il est convenu que toute référence à la Société contenue dans la présente politique devra être considérée comme s'adressant à chaque société du Groupe.

2. Utilisation des outils informatiques

Les outils informatiques sont des outils de travail.

Leur utilisation n'est permise que pour les finalités directement reconductibles ou, dans tous les cas, liées au travail, conformément aux critères de bonne foi et de professionnalisme, en cohérence avec le type d'activité réalisée et en conformité avec les dispositions légales et les politiques de la Société. Dans tous les cas, toute utilisation à des fins privées et/ou personnelles est exclue.

Les outils informatiques sont confiés par la Société aux Utilisateurs, avec toutes les obligations de garde et d'utilisation appropriées qui en découlent. Les Utilisateurs doivent utiliser les outils informatiques avec le plus grand soin et la plus grande diligence

À la date de cessation de la relation contractuelle avec la Société, l'Utilisateur doit retourner les outils informatiques à la Société.

L'utilisation des outils informatiques n'implique aucune propriété, de la part de l'Utilisateur autorisé, sur les données ou des informations traitées au moyen des outils informatiques, qui appartiennent exclusivement à la Société qui se réserve donc, donc le droit d'y accéder et dans les limites autorisées par la loi, selon les modalités décrites ci-après.

L'utilisation des outils informatiques de la Société non conforme à la présente politique ou, dans tous cas, contraire à la loi, peut entraîner l'application de sanctions disciplinaires, y compris le licenciement.

3. Obligations

Les Utilisateurs doivent :

- éteindre les outils informatiques et les éventuels périphériques (par exemple : ordinateur portable et écran) une fois leur travail terminé ou en cas d'éloignement prolongé de leur poste de travail, sauf indication contraire de la part des administrateurs du système ;
- adopter les autres précautions prévues par les procédures et/ou les instructions fournies par la Société, aussi en cas d'éloignements de courte durée ;
- faire effectuer les opérations de maintenance et/ou de réparation des outils informatiques uniquement par le personnel autorisé de la Société ;

- éviter toute utilisation d'équipements informatiques personnels sur le lieu de travail ou à des fins professionnelles, sauf autorisation expresse de la Société ;
- périodiquement (au moins tous les trois mois), nettoyer les archives (dossiers de données et boîte de messagerie électronique), en supprimant les fichiers obsolètes ou inutiles ;
- signaler dans les meilleurs délais toute anomalie ou dysfonctionnement, même partiel, des outils informatiques ainsi qu'informer immédiatement la Société en cas de vol ou dommage suspecté de ceux-ci ;
- respecter les autres politiques, instructions et/ou procédures fournies par la Société et relatives à l'utilisation des outils informatiques.

4. Interdictions

Les Utilisateurs n'ont pas le droit de :

- installer, sur les outils informatiques, des logiciels, même gratuits (*freeware* ou *shareware*), non distribués et/ou, dans tous les cas, non expressément autorisés par la Société, ni brancher, aux outils informatiques, des périphériques ou dispositifs non mis à la disposition par la Société ;
- modifier les réglages de sécurité et de confidentialité du système d'exploitation, du logiciel de navigation, du logiciel de messagerie électronique et de tout autre logiciel installé sur les outils informatiques ;
- modifier ou désactiver la fonction d'écran de veille avec mot de passe de son propre poste de travail de quelque manière que ce soit ;
- charger ou, dans tous les cas, conserver, sur les outils informatiques, du matériel informatique, des données et des informations personnelles ou, dans tous les cas, non liés à l'emploi couvert ;
- charger ou, dans tous les cas, conserver du matériel informatique dont le contenu (par ex. : texte, audio ou vidéo) est couvert par des droits d'auteur, est lié ou concerne des données confidentielles (sauf dans le cas de données qu'il est essentiel de traiter par de tels moyens, conformément aux dispositions et instructions, pour les tâches assignées), permet de connaître des données confidentielles, est contraire à la loi et/ou, dans tous les cas, concerne des activités ludiques ou de loisirs ;
- mener des activités qui diminuent la performance des systèmes et services de la Société, les rendent indisponibles ou introduisent des vulnérabilités ou des menaces à la sécurité.

Toute la gestion des outils informatiques, y compris les modifications de la configuration du système, peut être effectuée uniquement par la Société ou par des entités expressément autorisées par la Société. Par exemple, sont considérées comme modifications du système et, à ce titre, ne peuvent être réalisées sans autorisation préalable de la Société :

- la modification des connexions de réseau existantes ;
- l'utilisation des dispositifs amovibles (par ex. : USB, CD, DVD, disques durs) ;
- l'ouverture de la structure externe (*boîtier*) des outils informatiques et la modification, élimination ou ajout de composants à l'intérieur ;
- l'installation de logiciels, y compris ceux téléchargés sur Internet, ou, dans tous les cas, l'altération de la configuration des outils informatiques prêtés.

Le personnel dûment chargé par la Société peut à tout moment procéder à l'élimination de fichiers ou d'applications qu'il juge dangereux pour la sécurité de la Société tant sur les outils informatiques que sur les unités en réseau.

5. Gestion des mots de passe

L'accès aux outils informations est subordonné à la saisie correcte des codes d'accès (identifiant et mot de passe).

Le mot de passe doit être choisi selon les règles suivantes :

- un mot de passe doit contenir au moins huit caractères, au moins un caractère numérique, au moins un caractère alphabétique majuscule et au moins un caractère alphabétique minuscule, et au moins un caractère spécial ;
- un mot de passe ne doit pas être un mot du dictionnaire, ni un mot d'argot ou de dialecte d'une langue quelconque, ni aucun de ces mots orthographiés à l'envers;
- un mot de passe ne doit pas être basés sur les données à caractère personnel de l'Utilisateur ou d'un proche (par ex. : date de naissance, adresse, nom) ;
- un mot de passe ne peut être identique aux dix derniers mots de passe utilisés.

Lors de la sélection et de l'utilisation des mots de passe, les Utilisateurs doivent appliquer les règles de sécurité suivantes:

- les mots de passe ne doivent pas être révélés à d'autres personnes, y compris les administrateurs de gestion et du système ;
- les mots de passe ne doivent pas être transcrits, à moins qu'une méthode sûre n'ait été approuvée par la Société ;
- les mots de passe générés par l'Utilisateur ne doivent être distribués par aucun canal ;
- les mots de passe doivent être changés si des indices montrent que les mots de passe ou le système ont pu être compromis (auquel cas, un incident de sécurité doit être signalé à la Société).

En cas d'attribution ou d'utilisation de mots de passe, les règles suivantes doivent être appliquées :

- les Utilisateurs doivent garder les mots de passe confidentiels et ne pas partager leur identifiant avec d'autres Utilisateurs ;
- chaque utilisateur doit avoir la possibilité de choisir son mot de passe, s'il y a lieu;
- le mot de passe provisoire utilisé lors du premier accès au système doit être unique et respecter les règles susmentionnées ;
- le système de gestion des mots de passe doit demander à l'Utilisateur de modifier le mot de passe provisoire au moment du premier accès au système ;
- les mots de passe provisoires doivent être communiqués à l'Utilisateur de façon sécurisée et l'identité de l'Utilisateur doit être vérifiée au préalable ;
- le système de gestion des mots de passe doit demander à l'Utilisateur de sélectionner des mots de passe complexes ;
- le système de gestion des mots de passe doit demander à l'Utilisateur de changer leur mot de passe tous les trente jours ;
- le mot de passe ne doit pas être visible à l'écran lors de la connexion ;
- si un Utilisateur saisit un mot de passe erronée 10 fois de suite, le système doit bloquer le compte en question.

6. Messagerie électronique

6.1 Finalités d'utilisation

La Société met à la disposition des Utilisateurs un service de messagerie électronique, en attribuant à chacun d'eux des boîtes aux lettres institutionnelles à des fins professionnelles uniquement.

L'adresse de messagerie électronique mise à disposition des Utilisateurs par la Société constitue exclusivement un outil de travail. En conséquence, son utilisation par les Utilisateurs n'est autorisée qu'à des fins directement

liées ou, dans tous les cas, en rapport à l'exercice de leurs fonctions et activités correspondantes, à l'exclusion de toute utilisation à des fins ou des raisons privées et/ou personnelles.

Afin de faciliter l'exécution du travail, la Société peut également mettre à disposition des adresses de messagerie électronique partagées entre plusieurs Utilisateurs (par ex. : boîtes de messagerie créées pour chaque unité organisationnelle), en complément de celles individuelles.

6.2 Interdictions

Pour un usage correct de la messagerie électronique, il est interdit de :

utiliser la messagerie électronique à des fins personnelles et, dans tous les cas, pour envoyer ou recevoir des logiciels ou du matériel informatique ou encore des données ou des informations de toute nature à des fins personnelles, par ex. pour participer ou s'inscrire à des débats, des enchères en ligne, des concours, des forums, des réseaux sociaux ou des listes de diffusion, sauf si cela a été expressément autorisé par la Société ou est nécessaire pour l'exercice de ses fonctions professionnelles ;

l'envoi ou l'échange et le stockage de messages électroniques contenant des données à caractère personnel sensibles ou judiciaires ou en mesure de révéler des données sensibles ou judiciaires (sauf si nécessaire pour l'exécution de son propre travail) ;

participer à des chaînes télématiques (ou chaînes de lettres); en cas de réception de messages de ce type, ceux-ci doivent être immédiatement supprimés ;

l'envoi ou la mémorisation de messages de nature offensive, vulgaire, diffamatoire et/ou discriminatoire portant sur le sexe, la race, la langue, la religion, l'origine ethnique, les idées et l'appartenance à un syndicat et/ou parti politique, qui soient contraires à la loi, la décence ou la pudeur ou, dans tous les cas, au contenu offensif et, d'une quelque autre manière, aptes à offenser ou vexer. Cette règle valant aussi pour les chaînes de messages et/ou courriers indésirables ;

l'usage d'un langage ou d'images obscènes, trompeuses, diffamatoires, discriminatoires et/ou dans tous les cas susceptibles de nuire à la Société ou à des tiers ;

l'échange de messages en se faisant passer par une autre personne, à savoir en se substituant à l'envoyeur réel ;

envoyer ou recevoir ou encore échanger des messages électroniques, avec ou sans pièces jointes, contenant : des images, films et n'importe quel type de fichier au contenu illégal, violent et/ou pornographique ; des fichiers protégés par des droits d'auteur (par ex. : fichiers de musique ou vidéo) ; liens vers des sites à contenu illégal, violent et/ou pornographique ; mots de passe et/ou codes d'accès à des programmes protégés par des droits d'auteur et/ou à des sites Internet ;

ouvrir des messages électroniques ou des pièces jointes de type « exécutable » (par ex. : *.Exe*) ou qui font référence à des liens externes.

6.3 Obligations

Les Utilisateurs doivent :

- limiter la dimension des messages envoyés, surtout dans les cas où il y a plusieurs destinataires ;
- éviter tout comportement pouvant permettre à des tiers de divulguer des informations de quelque nature que ce soit pouvant ramener à un expéditeur involontaire ;
- éviter de répondre à des messages électroniques qui contiennent un message générique demandant des informations personnelles pour des raisons non clairement précisées (par ex. : expiration, perte, problèmes techniques) ou au ton intimidant (par ex. : menace de bloquer une carte de crédit ou un compte en banque) ou, dans tous les cas, caractérisés par des éléments pouvant révéler des actions de

hameçonnage ;

- veiller à garder sa boîte de messagerie bien en ordre, en éliminant les messages inutiles et en archivant les messages importants pour la Société dans les sections prévues à cet effet, en limitant leur dimension et les pièces jointes correspondantes, en supprimant donc les documents inutiles et, surtout, les pièces jointes volumineuses; il est convenu que la destruction de toute communication envoyée ou reçue ayant un contenu important ou contenant des engagements contractuels ou précontractuels pour la Société ou des documents à considérer comme confidentiels en ce qu'ils sont marqués du sceau « strictement confidentiels » ou d'une mention similaire ou, dans tous les cas, ayant pour d'autres raisons ce contenu, doit être autorisée par écrit par la Société.

6.4 Absence de l'Utilisateur

En cas d'absence soudaine ou prolongée ou pour des besoins qui ne peuvent pas être différés liés au travail, l'Utilisateur pourra :

i. insérer, en toute autonomie, dans le système une « réponse automatique » qui informe les expéditeurs des messages qui lui sont adressés de son absence et leur suggère un destinataire alternatif ayant une adresse de courriel dans le domaine @falckrenewablesgroup.com ou @vectrorenewables.com

ii. demander, avec l'accord écrit préalable du Data Steward de sa propre structure, à ce que les messages adressés à son attention soient automatiquement transférés vers un autre destinataire ayant une adresse de courrier électronique dans le domaine @falckrenewablesgroup.com ou @vectorenewables.com;

iii. déléguer, sous réserve de l'autorisation écrite du Data Steward de sa propre structure, un autre Utilisateur (de confiance) pour vérifier le contenu des messages et et transmettre à la Société ceux qui sont jugés importants pour l'exécution du travail ; dans ce cas, l'administrateur du système de messagerie établira un rapport d'activité et informera l'Utilisateur de l'accès effectué dans les meilleurs délais.

Au cas où l'Utilisateur ne serait pas en mesure de faire les demandes ci-dessus (par ex. : hospitalisation avec capacités psycho-physiques limitées), la Société procèdera, par l'intermédiaire de l'administrateur du système et avec l'approbation écrite préalable de l'Expert en protection de la vie privée, à la mise en œuvre de la solution (i) et, en cas d'exigences spécifiques et justifiées de continuité des activités qui sont susceptibles d'être affectés par l'absence soudaine et prolongée de l'employé, pourra accéder au contenu de sa messagerie. Le cas échéant, l'administrateur du système de messagerie rédigera un procès-verbal de l'activité et informera l'Utilisateur de l'accès à la première occasion utile.

6.5 Signature

Les messages électroniques sortants doivent toujours contenir en pied-de-page la mention suivante portant sur la confidentialité de la communication :

« Ce message peut contenir des informations de nature extrêmement réservée et confidentielle. Si vous n'êtes pas le destinataire, veuillez nous en informer et supprimer le message, ainsi que ses éventuelles pièces jointes, sans en conserver de copie. Toute utilisation de ce message, en tout ou en partie, non expressément autorisée par le destinataire (telle que, à titre d'exemple mais non limitatif, la publication ou la reproduction sur Internet ou la distribution et/ou diffusion à des tiers en général) expose le responsable aux poursuites civiles et pénales correspondantes. Respectez l'environnement. N'imprimez pas cet email si ce n'est pas strictement nécessaire.

This message may contain information which is confidential or privileged. If you are not the intended recipient, please immediately notify us and destroy this message and any attachments without retaining a copy. Any unauthorized use of this message either whole or partial (including, without limitation, any copying or reproduction

on internet websites and any distribution and/or diffusion to third parties) may expose the responsible party to civil and/or criminal penalties. Respect nature. Do not print this email unless absolutely necessary ».

7. Internet

L'accès à Internet est autorisé aux Utilisateurs autorisés par la Société uniquement pour l'exécution de leurs activités professionnelles et toujours dans le respect des procédures internes et des lois applicables.

Il est convenu qu'il est strictement interdit de :

- modifier les paramètres du système afin de contourner une quelconque protection servant à limiter l'accès à Internet ;
- établir, pour quelque raison que ce soit, des connexions de pair à pair à l'internet;
- télécharger des fichiers volumineux afin d'éviter la saturation de la largeur de bande du réseau disponible pour les systèmes ;
- télécharger des logiciels, même gratuits (freeware et shareware), non conformes aux normes de la Société, afin d'éviter l des actes illicites et surtout le grave danger d'introduire des des virus informatiques.

8. Télétravail

En cas d'utilisation des outils informatiques par les Utilisateurs durant l'exécution du contrat de travail défini par un accord entre la Société et les Utilisateurs, aussi sous forme d'organisation par phases, cycles et objectifs et sans horaire fixe de travail ou de lieu de travail (le« ***télétravail*** »), toutes les règles illustrées par la présente politique sont applicables.

Afin de pouvoir utiliser ses outils informatiques personnels en *télétravail*, il est nécessaire que l'Utilisateur soit autorisé par la Société. Le cas échéant, l'Utilisateur :

- doit utiliser exclusivement les systèmes et les logiciels dont il détient une licence d'utilisation conforme et respecter les conditions d'utilisation prévues par celle-ci ;
- vérifier que le système utilisé est régulièrement mis à jour tant pour le logiciel de base que pour les systèmes antivirus et anti-spam installés;
- vérifier que la connexion Internet (*Wi-Fi* compris) utilisée soit protégée par un mot de passe afin de rendre improbable l'accès au réseau même par des personnes non autorisées ;
- garantir le respect des règles et des principes de sécurité illustrés dans la présente politique.

9. Surveillance et contrôle

Pour des questions d'organisation et de production, pour la protection du patrimoine de l'entreprise et pour vérifier le respect des lois et normes applicables, y compris des politiques internes de la Société, cette dernière peut avoir besoin de contrôler l'utilisation de ses propres systèmes informatiques et, par exemple, d'accéder aux messages électroniques envoyés ou reçus par l'Utilisateur. Cependant, cette activité ne doit pas être considérée comme une activité de surveillance du travail des employés et est menée en conformité avec les dispositions légales en vigueur en matière de droits des travailleurs et de protection de la vie privée.

Les activités de contrôle pour les raisons susmentionnées sont réalisées, dans le respect de la vie privée des Utilisateurs, par le personnel de la Société qui met en œuvre sa propre activité pour la gestion et l'assistance des services d'information en qualité de sous-traitant du traitement des données à caractère personnel avec le support, si nécessaire, du responsable de l'unité organisationnelle concernée qui veillera à identifier l'objet de recherche en ce que celle-ci ne peut être indiscriminée, générique et illimitée. Aucune autre personne ne sera impliquée dans de telles activités, ni n'aura accès aux données à caractère personnel des Utilisateurs contenues dans les comptes de messagerie électronique de l'entreprise.

La Société rappelle aux Utilisateurs que, sachant que les systèmes informatiques de la Société sont dotés de systèmes d'enregistrement technique des évènements (à savoir les fichiers *journaux*), la Société pourra accéder à ces données dans le cadre des finalités de contrôle susmentionnées. Ces enregistrements peuvent être utilisés pour rechercher la source d'éventuelles erreurs ou anomalies mais ne sauraient être utilisés pour pister le le déroulement du travail des Utilisateurs.

Les raisons pour lesquelles la Société pourrait effectuer une activité de contrôle incluent :

- identifier et prévenir tout accès ou communication d'informations non autorisées ;
- assurer la conformité aux lois et aux règlements ;
- prévenir, identifier ou contenir des activités criminelles ;
- contrôler les virus et les autres menaces de code malveillant ;
- en cas de suspicion, enquêter ou identifier les utilisations inappropriées des outils informatiques ;
- en cas de suspicion, enquêter sur les violations de la présente politique ou d'autres politiques spécifiques de la Société.

La surveillance est effectuée dans les limites de ce qui est permis ou requis par la loi et tel que nécessaire et justifiable aux fins illustrées plus haut.

Les informations identifiées lors du contrôle (y compris les données à caractère personnel) peuvent également être utilisées à des fins disciplinaires et conservées pendant toute la durée de la procédure d'investigation, disciplinaire, réglementaire ou criminelle et elles peuvent être divulguées à des tiers lorsque cela est nécessaire ou requis par la loi.

Les Utilisateurs peuvent contacter l'Expert en protection de la vie privée pour plus d'informations sur l'étendue et le type de contrôle qui peut être effectuée sur les systèmes d'information de la Société.

10. Utilisation des réseaux sociaux

L'accès à ses propres comptes de réseaux sociaux comme, par ex., Facebook, Twitter ou Instagram, est interdit avec les outils informatiques de la Société.

Il est convenu que l'utilisation de ses propres comptes de réseaux sociaux personnels comme, par ex., Facebook, Twitter ou Instagram, hors de l'horaire de travail et en utilisant ses outils informatiques personnels, devra être effectuée sans porter préjudice à la Société (par ex., il est interdit de publier des documents confidentiels de la Société). À cette fin, la Société précise que :

toute utilisation contraire à la loi et aux règlements applicables, à l'ordre public, à toute règle de décence et/ou pouvant nuire à la réputation et à l'image de la Société, tant à l'intérieur qu'à l'extérieur, est strictement interdite ;

toute discussion ou publication sur les réseaux sociaux relative aux produits, projets ou services de la Société n'est permise qu'aux Utilisateurs expressément autorisés ;

il est interdit de partager des informations sur les performances, les projets, les produits, les services, les perspectives de développement, les données financières, les accords commerciaux, les données de vente, les stratégies et les résultats de la Société sur les réseaux sociaux à moins que les Utilisateurs n'aient été expressément autorisés en ce sens ;

toute discussion ou publication sur les réseaux sociaux concernant des tiers concurrents de la Société et/ou leurs produits ou activités est interdite ;

avant de partager tout contenu protégé par des droits de propriété intellectuelle (par ex. : noms, marques, logos), y compris les droits dont la Société est titulaire, il est nécessaire d'obtenir l'autorisation spécifique et explicite du

titulaire des droits ;

les données qui permettent d'identifier les personnes et leurs relations professionnelles (par ex. : clients, fournisseurs, salariés, collaborateurs) ne doivent pas être publiées sur les réseaux sociaux sans l'autorisation préalable et explicite des personnes concernées ;

les idées et opinions doivent être exprimées de façon respectueuse et appropriée au contexte afin d'éviter de porter préjudice à la dignité des personnes et/ou des entreprises concurrentes.

En référence à l'utilisation des réseaux sociaux professionnels et/ou strictement liés au travail (à savoir LinkedIn), les Utilisateurs doivent saisir des informations relatives à leur propre poste et fonctions occupées au sein de la Société qui soient véridiques, pertinentes et à jour.

Les Utilisateurs peuvent contacter le Data Steward en cas de besoin d'éclaircissements sur l'utilisation des réseaux sociaux.

11. Références externes.

P_STAFF 30 GR – ITGov _ Gestione Accessi Logici (Gestion des accès logiques)

P_STAFF 31 GR – ITSec _ Information Security Policy

P_STAFF 27 GR – ITGov _ IT Tools Management Policy

I_STAFF 18 GR – Op. Gestione Asset (Op. Gestion des infrastructures TIC)

Annexe B
Analyse d'impact sur la protection des données

1. Contexte

1.1 Aperçu du traitement

1.1.1 Quel est le traitement pris en considération ?

1.1.2 Quelles sont les responsabilités liées au traitement ?

1.2 Données, processus et ressources de support

1.2.1 Quelles sont les données traitées ?

1.2.2 Quel est le cycle de vie du traitement des données (description fonctionnelle) ?

1.2.3 Quelles sont les ressources de support aux données ?

2 Principes fondamentaux

2.1 Proportionnalité et nécessité

2.1.1 Les finalités du traitement sont-elles spécifiques, explicites et légitimes ?

2.1.2 Quelles sont les bases juridiques qui rendent le traitement licite ?

2.1.3 Les données collectées sont-elles appropriées, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

2.1.4 Les données sont-elles exactes et à jour ?

2.1.5 Quelle est la durée de conservation des données ?

2.2 Mesures de protection des droits des personnes concernées

2.2.1 Comment les personnes concernées sont-elles informées du traitement ?

2.2.2 Comment est obtenu le consentement des personnes concernées ?

2.2.3 Comment font les personnes concernées pour exercer leurs droits conformément au Règlement ?

2.2.4 Les obligations des responsables du traitement sont-elles clairement définies et réglementées par un contrat ?

2.2.5 En cas de transfert des données hors de l'Union européenne, les données bénéficient-elles d'une protection équivalente ?

3 Risques[6]

3.1 Mesures existantes ou planifiées

N°	Nom du contrôle	Description	Contrôles mis en œuvre
	Cryptographie	Les moyens mis en œuvre pour garantir la confidentialité des données stockées (dans les bases de données, fichiers, sauvegardes, etc. ...) tout comme les procédures pour gérer les clés cryptographiques (création, archivage, mise à jour en cas de suspicion de	

[6] Le risque ne se réfère pas au responsable du traitement mais à la personne concernée.

		compromission, etc.). Préciser les moyens cryptographiques employés pour les flux de données (VPN, TLS, etc. ...) mis en œuvre dans le traitement.	
	Anonymisation	Indiquer les mécanismes d'anonymisation mis en place, les garanties qu'ils introduisent contre l'éventuelle ré-identification et les finalités pour lesquels ils sont mis en œuvre.	
	Partitionnement	Méthodes utilisées pour compartimenter le traitement.	
	Contrôle des accès logiques	Décrire la façon dont les profils des utilisateurs sont définis et attribués. Préciser les systèmes d'authentification mis en place en précisant, si applicables, les règles relatives aux mots de passe (longueur minimale, caractères demandés, durée de validité, nombre de tentatives avant le blocage du compte, etc. ...).	
	Traçabilité	Politiques qui définissent la traçabilité des évènements et la gestion des registres correspondants.	
	Archivage	Politiques de conservation et de gestion d'archives électroniques contenant des données à caractère personnel, finalisées à en protéger, notamment, la validité juridique pendant toute la durée nécessaire (versement, conservation, migration, accessibilité, suppression, politiques d'archivage, protection de la confidentialité, etc. ...).	
	Sécurité des documents sur support papier	Politiques relatives aux documents sur support papier contenant des données à caractère personnel dans le cadre du traitement. Ces politiques décrivent la façon dont les documents sont imprimés, archivés, détruits et partagés.	
	Minimisation de la quantité de données	Il est possible d'utiliser les méthodes suivantes : filtrage et suppression, réduction du potentiel d'identification à travers la transformation, la réduction de la nature identificatrice des données, réduction de l'accumulation des données, limitation de l'accès aux données.	
	Vulnérabilité	Politiques visant à limiter la probabilité et la gravité des risques pour les ressources utilisées durant le travail (documenter les procédures de travail, inventaire et mise à jour des logiciels et du matériel informatique, correction des vulnérabilités, duplication des données, limitations à l'accès physique au matériel, etc. ...).	

	Gestion des postes de travail	Mesures adoptées pour réduire la possibilité que les caractéristiques du logiciel (systèmes d'exploitation, applications internes, logiciels de bureau, réglages, etc. ...) soient exploitées pour endommager les données à caractère personnel (mises à jour, protection physique et accès, travail sur un espace de réseau protégé, contrôles de l'intégrité, *connexions*, etc.).	
	Sauvegardes	Existence de politiques de sauvegarde aptes à assurer la disponibilité et/ou l'intégrité des données à caractère personnel, à en protéger la confidentialité (périodicité des sauvegardes, chiffrement du canal de transmission de données, test d'intégrité, etc. ...).	
	Maintenance	Existence d'une politique de maintenance physique des dispositifs, en précisant l'éventuel recours à l'externalisation. Elle devra comprendre la maintenance à distance, si autorisée, et préciser les méthodes de gestion de matériels défectueux.	
	Accords sur le traitement des données	Les données à caractère personnel communiquées aux responsables du traitement ou gérées par ces derniers doivent bénéficier de garanties suffisantes. Avoir recours uniquement à des sous-traitants du traitement qui offrent des garanties suffisantes (notamment en matière d'expertise, de fiabilité et de ressources). Exiger que le sous-traitant communique se propre politique de sécurité en matière de systèmes d'information. Adopter et documenter les mesures (audits de sécurité, visites des installations, etc.) qui permettent d'assurer l'effectivité des garanties offertes par le sous-traitant du traitement en matière de protection des données. Ces garanties comprennent notamment : - le chiffrement des données en fonction de leur sensibilité ou, en l'absence de chiffrement, l'existence de procédures aptes à garantir que le sous-traitant du traitement n'accède pas aux données qui lui sont confiées - le chiffrement des transmissions de données (par ex. : connexions type HTTPS, VPN, etc. ...) - des garanties en matière de protection du réseau, traçabilité (registres, audits), gestion des autorisations, authentification, etc. ... Prévoir un contrat avec les sous-traitants du traitement	

		dans lequel, notamment, l'objet, la durée, la finalité du traitement et les obligations de chaque partie contractante sont définis. Vérifier que ce contrat contienne notamment les dispositions relatives à ce qui suit : - les obligations des sous-traitants en matière de confidentialité des données à caractère personnel qui leur sont confiées - les exigences minimales d'authentification des utilisateurs - les clauses en matière de restitution et/ou destruction des données à la conclusion du contrat - les règles pour la gestion et la notification d'éventuels incidents. Ces dernières devront prévoir la communication au responsable du traitement en cas de constatation d'une violation de la sécurité ou de matérialisation d'un incident de sécurité. Communication qui devra être la plus rapide possible lorsque la violation concerne les données à caractère personnel.	
	Sécurité des canaux informatiques	En fonction du type de réseau sur lequel le traitement est effectué (isolé, privé ou Internet), le responsable du traitement doit mettre en place des systèmes de protection appropriés : pare-feu, détecteurs anti-intrusion ou d'autres dispositifs (actifs ou passifs) visant à garantir la sécurité du réseau.	
	Contrôle des accès physiques	Existence d'un contrôle des accès physiques aux locaux qui accueillent le traitement (zonage, accompagnement des visiteurs, distribution de badges, portes fermées, etc. ...). Indiquer si des procédures d'alarme en cas d'intrusion sont en place.	
	Traçabilité des activités en réseau	Existence de mesures mises en place pour détecter dans les meilleurs délais les incidents relatifs aux données à caractère personnel et disposer d'éléments utilisables pour les analyser ou pour fournir des preuves en cas d'enquêtes (politique d'enregistrement des évènements, respect des obligations en matière de protection des données, etc. ...).	
	Sécurité du matériel informatique	Existence de mesures adoptées pour réduire le risque que les caractéristiques des appareils (serveurs, ordinateurs de bureau, ordinateurs portables,	

		périphériques, dispositifs de communication, supports amovibles, etc. ...) soient utilisées pour endommager les données à caractère personnel (inventaire, compartimentation, redondance, limites à l'accès, etc. ...).	
	Prévention des sources de risque humaines et non humaines	Existence de mesures pour éviter que les sources de risque, humaines et non humaines, bien que très peu probables, ne portent préjudice aux données à caractère personnel (marchandises dangereuses, zones géographiques dangereuses, transfert des données hors de l'UE, phénomènes climatiques, incendies, dommages provoqués par l'eau, incidents internes ou externes, animaux).	
	Politique de protection de la vie privée	Existence d'une organisation apte à guider et à vérifier la protection des données à caractère personnel au sein de la structure (désignation d'un DPD, création d'un organe de surveillance, etc. ...).	
	Gestion des politiques de protection de la vie privée	Le responsable du traitement doit disposer d'une base documentaire établissant les objectifs et les règles à appliquer dans le domaine de la protection des données (plan d'action, révision périodique des politiques en matière de protection des données, etc. ...)	
	Gestion des risques	Existence d'une politique qui définisse les processus visant à maîtriser les risques que les traitements comportent pour les droits et les libertés des personnes concernées (recensement des traitements des données à caractère personnel, des données traitées, des supports utilisés, évaluation du risque, définition des mesures existantes ou prévues, etc. ...)	
	Intégration de la protection de la vie privée dans les projets	Existence de procédures qui décrivent les méthodes visant à tenir compte de la protection des données à caractère personnel dans tout nouveau traitement (certifications, référentiels, gestion du risque pour la personne concernée selon une méthodologie interne ou indiquée par l'autorité de contrôle, etc. ...)	
	Gestion des incidents de sécurité et des violations de données à caractère	Existence d'une organisation structurelle pour relever et gérer les évènements pouvant avoir une répercussion sur les libertés et la protection de la vie privée des personnes concernées (définition des responsabilités, plan de réaction, caractérisation des violations, etc. ...)	

	personnel		
	Gestion des effectifs	Existence d'un plan décrivant les mesures de sensibilisation adoptées au moment de la prise en charge d'un employé et d'une procédure décrivant les mesures adoptées à la cessation de la relation de travail avec les personnes qui ont accès aux données.	
	Surveillance de la protection des données	Existence de mesures qui permettent d'avoir une vision globale et actualisée de l'état de protection des données et de la conformité au Règlement (contrôle de la conformité des traitements, objectifs et indicateurs, responsabilités, etc. ...).	
	Autres contrôles		

3.2 Confidentialité des données (divulgation/accès)

3.2.1 Quels pourraient être les principaux impacts sur les personnes concernées si le risque se matérialise ?[7]

3.2.2 Quelles sont les principales menaces susceptibles de matérialiser le risque ?

3.2.3 Quelles sont les sources de risque ?

3.2.4 Parmi les mesures identifiées, quelles sont celles qui contribuent à atténuer le risque ?

3.2.5 Comme évalueriez-vous la gravité du risque, notamment à la lumière des impacts potentiels et des mesures planifiées ?

3.2.6 Comment évalueriez-vous la probabilité du risque, notamment en ce qui concerne les menaces, les sources de risque et les mesures planifiées ?

3.3 Intégrité des données (altération)

3.3.1 Quels seraient les principaux impacts sur les personnes concernées si le risque se matérialise ?

3.3.2 Quelles sont les principales menaces qui pourraient matérialiser le risque ?

3.3.3 Quelles sont les sources de risque ?

3.3.4 Parmi les mesures identifiées, quelles sont celles qui contribuent à atténuer le risque ?

3.3.5 Comme évalueriez-vous la gravité du risque, notamment à la lumière des impacts potentiels et des mesures planifiées ?

3.3.6 Comment évalueriez-vous la probabilité du risque, notamment en ce qui concerne les menaces, les sources de risque et les mesures planifiées ?

3.4 Disponibilité des données (perte/indisponibilité/destruction)

3.4.1 Quels pourraient être les principaux impacts sur les personnes concernées si le risque se matérialise ?

3.4.2 Quelles sont les principales menaces susceptibles de matérialiser le risque ?

3.4.3 Quelles sont les sources de risque ?

3.4.4 Parmi les mesures identifiées, quelles sont celles qui contribuent à atténuer le risque ?

[7] Par ex. : vol d'identité, pertes financières, dommages physiques ou psychologiques, perte de contrôle des données, autres désavantages économiques ou sociaux, impossibilité d'exercer les droits/services/opportunités, atteinte à la réputation, discrimination.

3.4.5 Comme évalueriez-vous la gravité du risque, notamment à la lumière des impacts potentiels et des mesures planifiées ?

3.4.6 Comment évalueriez-vous la probabilité du risque, notamment en ce qui concerne les menaces, les sources de risque et les mesures planifiées ?

3.5 Présentation des risques et des mesures correctives mises en place[8]

	Confidentialité des données	**Intégrité des données**	**Disponibilité des données**
Gravité			
Probabilité			
Résultat			

GRAVITÉ	Maximale 4	4	8	12	16
	Significative 3	3	6	9	12
	Limitée 2	2	4	6	8
	Négligeable 1	1	2	3	4
Niveau de risque (gravité par probabilité)		Négligeable 1	Limité 2	Significatif 3	Maximal 4
		PROBABILITÉ			

NIVEAU	**NÉGLIGEABLE**	**LIMITÉ**	**SIGNIFICATIF**	**MAXIMAL**
	La personne concernée ne sera pas affectée ou peut rencontrer peu de désagréments qui peuvent être surmontés sans problème.	La personne concernée pourrait rencontrer des inconvénients significatifs qui peuvent être surmontés avec quelques difficultés.	La personne concernée pourrait subir des conséquences majeures qu'elle devrait être en mesure de surmonter même si avec de graves et réelles difficultés.	La personne concernée pourrait être confronté à des conséquences significatives ou irréversibles qui pourraient ne pas être surmontables.

4 Avis des personnes concernées

[●]

5 Indice des versions

[●]

6 Évaluations finales

À l'issue de l'analyse d'impact et après avoir tenu compte de la nature, du champ d'application, du contexte et des finalités du traitement et des sources de risque ainsi que des mesures techniques et organisationnelles adoptées pour atténuer le risque éventuel en garantissant la protection des données à caractère personnel, la gravité du risque [●] et la probabilité du risque résulte [●].

[8] Pour en savoir plus, voir les « Lignes directrices sur l'analyse d'impact sur la protection des données » du Groupe de travail « Article 29 ».

Annexe C
F.A.Q.

	Question	Réponse
1.	J'ai du mal à comprendre le langage de la note d'information sur la protection de la vie privée et la formule de consentement, puis-je les modifier ?	Non, seul l'Expert en protection de la vie privée peut modifier ces documents. Vous devrez contacter le Data Steward de votre unité organisationnelle qui consultera l'Expert en protection de la vie privée.
2	Différentes formules de consentement sont présentes. Puis-je les remplacer par une seule qui englobe tout ?	Non, le consentement en vertu du RGPD doit être spécifique. Lorsque plusieurs consentements sont prévus, ceux-ci doivent être séparés. Il n'est pas possible de modifier les formules du consentement sans l'approbation préalable de l'Expert en protection de la vie privée.
3	Puis-je profiler les employés ou les clients ?	Cela n'est possible qu'en référence aux personnes qui ont donné leur consentement au profilage. Dans tous les cas, avant de se lancer dans cette activité, il est nécessaire de consulter le Data Steward de l'unité organisationnelle d'appartenance.
4	Je travaille sur un nouveau produit ou service qui nécessitera le traitement de données à caractère personnel et et j'envisage de ne demander un avis juridique qu'avant le lancement.	Non, le RGPD exige d'évaluer l'impact sur le traitement des données des produits/services dès le début du projet conformément à la procédure décrite au point 12 de la Politique de protection des données.
5.	Je garde dans le tiroir de mon bureau une liste de clients « historiques » contenant des données à caractère personnel, puis-je le faire ?	Non, il existe des durées de conservation spécifiques pour chaque type de données. Vous devez contacter le Data Steward car la Société doit être en mesure de cartographier tous les traitements des données à caractère personnel détenues pour son propre compte.
6	Je suis sur le point de stipuler un contrat avec un fournisseur informatique auquel je fais confiance car nous travaillons ensemble depuis des années et il est très connu sur le marché. Puis-je éviter d'effectuer les contrôles en matière de conformité à la norme sur la protection de la vie privée ?	Non, la procédure visée au point 8 de la Politique de protection des données doit être mise en œuvre pour chaque nouveau contrat stipulé par la Société.
7.	Je dois travailler depuis chez moi pendant le week-end. Puis-je envoyer les documents à mon adresse de courrier électronique privée afin de pouvoir y travailler dessus avec mon ordinateur personnel ?	Non, cela empêcherait la Société de protéger le document d'un éventuel accès par des tiers. Vous ne pouvez pas envoyer de documents liés au travail à votre adresse de messagerie privée et les enregistrer sur des appareils qui ne sont pas fournis par la Société.
8	Je viens de me rendre compte que j'ai oublié dans le train mon sac à dos avec la liste des clients et les données à caractère personnel les concernant. Que dois-je faire ?	Vous devez envoyer un courriel à l'adresse databreach@falckrenewables.com car il existe un risque d'accès non autorisé aux données.
9	L'ordinateur de mon entreprise a été volé, que dois-je faire ??	Vous devez envoyer un courriel à l'adresse databreach@falckrenewables.com car il existe un risque d'accès non autorisé aux données.

Annexe D
Politique de violation des données

L’objectif de cette procédure (la « **Procédure** ») est de définir les principes, les méthodes d’identification et de résolution et les flux de gestion conséquents de la Société en cas de violation des données à caractère personnel (**Violation des données**) en vertu du Règlement (UE) 2016/679 et de la Loi sur la protection de la vie privée.

1. Informations sur le document

1.1 **Références normatives**

- Règlement (UE) 2016/679 du Parlement et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi qu'à la libre circulation de ces données (ci-après le « **Règlement européen sur la protection de la vie privée** » ou « **RGPD** ») ;
- Directives sur la violation de données du Groupe de travail visé à l'art 29 » de la Directive 95/46/CE du 6 février 2018 (ci-après le « Groupe visé à l'art. 29 »).

1.2 Diffusion

Chaque Data Steward doit diffuser la présente procédure à tous les membres des unités organisationnelles agissant sous sa coordination, tant à l'occasion de la première émission que lors des mises à jour qui peuvent intervenir après.

1.3 Destinataires de la procédure

Tous les employés et collaborateurs à durée indéterminée ou à durée déterminée de la Société (ci-après dénommés conjointement les « **Destinataires** »).

1.4 Obligation de connaissance

Les Destinataires sont tenus de connaître et de respecter le contenu de la présente procédure.

1.5 Règles pour l'approbation, la mise à jour, l'archivage et la distribution de la Procédure.

L'approbation, la mise à jour et la modification de la présente procédure devront être approuvées par le Comité pour la protection de la vie privée en cas de mises à jour majeures, conformément aux révisions périodiques et aux éventuelles modifications qui pourraient être apportées aux documents du corps normatif susmentionnés et, dans tous les cas, avec une fréquence annuelle.

2. Définitions

En plus des termes définis dans le document de Politique de protection des données et des termes définis dans le RGPD, les termes supplémentaires suivants ont la signification indiquée ci-après :

Comité pour la protection de la Vie Privée	Il s'agit du comité formé par l'Expert en protection de la vie privée, le CDT&IO et le Data Steward de la structure de référence.
Violation des données à caractère personnel	Il s'agit d'une violation de la sécurité entraînant, accidentellement ou illégalement , la destruction, la perte, la modification la divulgation non autorisée ou l'accès aux données à caractère personnel transmises, stockées ou traitées d'une autre manière.
Donnée à caractère personnel	Toute information relative à une personne physique identifiée ou identifiable (la « personne concernée »). On considère comme étant identifiable la personne physique qui peut être identifiée, directement ou indirectement, en particulier grâce à un identifiant tel que le nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou grâce à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, psychologique, économique, culturelle ou sociale. Une donnée à caractère personnel ne peut se référer qu'à une personne physique (à savoir, un individu), et comprend également les entreprises individuelles et les travailleurs indépendants, alors que les données des personnes morales (à savoir, les sociétés) ne sont pas soumises à la la Loi sur la protection de la vie privée. L'adresse de courrier électronique prénom.nom@falck.it est une donnée à caractère personnel, alors que l'adresse générale info@falck.it n'en est pas une.
Traitement	Toute opération ou ensemble d'opérations, effectuées avec ou sans l'aide de processus automatisés et appliquées à des données à caractère personnel ou à des ensembles de données à caractère personnel, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication moyennant la transmission, la diffusion ou toute autre forme de mise à disposition, la comparaison ou l'interconnexion, la limitation, la suppression ou la destruction.
Expert en protection de la vie privée	Le sujet agissant en tant que contact principal pour toute question relative au respect de la Loi sur la protection de la vie privée.
CDT&IO	*Chief Digital Transformation & Information Officer* (Responsable de l'Information et de la Transformation Numérique)
Personne concernée	La personne physique (y compris les entreprises individuelles et les indépendants) identifiable, directement ou indirectement, au moyen des données à caractère personnel objet du traitement.
Autorité	Autorité de contrôle compétente
Équipe de crise	Le Comité consultatif, dirigé par le Gardien de l'information (*Gatekeeper*), chargé de l'analyse de l'événement de crise tel que défini dans la Procédure *de gestion de la communication de crise*.

3. Objet et champ d'application de la Procédure

Conformément à l'article 33 du RGPD, en cas de violation des données à caractère personnel (*Data Breach*), le Titulaire du Traitement notifie la violation à l'autorité de contrôle compétente qui, sans retard injustifié et, si possible, dans les 72 heures suivant le moment où il en a eu connaissance, à moins que la violation des données à caractère personnel ne soit pas susceptible de présenter un risque pour les droits et libertés des personnes physiques.
En outre, conformément à l'article 34 du RGPD, lorsque la violation des données à caractère personnel est susceptible de présenter un risque élevé pour les droits et les libertés des personnes physiques, le responsable du traitement doit communiquer la violation à la personne concernée dans les meilleurs délais. Cette communication n'est pas requise lorsque :

- le Titulaire du traitement a mis en œuvre les mesures techniques et organisationnelles appropriées pour la protection des données à caractère personnel et que ces mesures ont été appliquées aux données concernées par la violation (par ex. : chiffrement) ;
- le Titulaire du traitement a par la suite adopté des mesures visant à prévenir la matérialisation d'un risque élevé pour les droits et les libertés des personnes concernées ;
- la communication aux personnes concernées nécessite des efforts disproportionnés (dans ce cas, le Titulaire du Traitement procédera à une communication publique ou à une mesure similaire ayant une efficacité analogue).

La présente procédure de violation de données, rédigée conformément aux dispositions du RGPD, est activée en cas de détection d'une violation des données à caractère personnel et a pour but de définir quelles actions doivent être prises par l'ensemble de l'organisation de l'entreprise en présence de violation des principes illustrés ci-dessus. Le présent document décrit également les circonstances en présence desquelles il est nécessaire de notifier et/ou communiquer la violation des données à caractère personnel à l'autorité de contrôle pour la protection des données à caractère personnel et/ou à la personne concernée.
Le non-respect des règles énoncées dans le présent document pourrait entraîner des sanctions sévères.

La présente procédure vise à :
- identifier les modalités et les canaux pour détecter une violation de données ;
- prévoir une participation adéquate et réactive des Structures de direction en ce qui concerne les événements critiques en matière de violation des données à caractère personnel afin de garantir une action immédiate en conformité avec la législation applicable ;
- permettre l'adoption rapide de la solution à mettre en œuvre afin de limiter ou d'atténuer l'impact de la violation des données à caractère personnel sur les activités commerciales ;
- utiliser les données « événements à risque » afin d'améliorer l'identification et l'évaluation du risque ;
- remplir les obligations imposées par la loi applicable, en démontrant également à l'autorité de contrôle pour la protection des données à caractère personnel l'engagement de la Société dans l'adoption de pratiques de management des risques appropriées aux traitements effectués.

3.1 En quoi consiste une violation des données et qu'implique-t-elle ?

En relation à la définition fournie à l'article 4, point 12 du RGPD, l'expression « Violation des données » désigne toute violation de la sécurité impliquant, de façon accidentelle ou illicite, la destruction, la perte, la modification, la divulgation non autorisée ou l'accès aux données à caractère personnel transmises, conservées ou traitées d'une autre manière.

Selon l'article 32, point 1 du RGPD, le titulaire et les responsables du traitement mettent en place des mesures techniques et organisationnelles adéquates garantissant un niveau de sécurité adapté au risque. Entre autres, la Société doit :
- assurer de manière permanente la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement ;
- restaurer dans les meilleurs délais la disponibilité et l'accès aux données à caractère personnel en cas d'incident physique ou technique.

À partir de ces définitions, il existe trois catégories différentes de violation des données à caractère personnel selon les principes de sécurité internationalement reconnus :
- *Violation de la confidentialité :* elle se vérifie dans les cas où une divulgation ou un accès non autorisé ou accidentel a lieu ;

- *Violation de la disponibilité :* elle se vérifie dans les cas où des données sont perdues ou détruites de manière accidentelle et/ou non autorisée ;
- *Violation de l'intégrité :* elle se vérifie lorsque l'événement concerne la modification non autorisée ou accidentelle de données à caractère personnel.

La violation de la sécurité est donc conçue comme un acte accidentel, non autorisé ou intentionnel impliquant la divulgation, l'accès, l'altération, la destruction ou la perte de données à caractère personnel, allant ainsi à corrompre un ou plusieurs principes de sécurité des informations.

Événement	**Description de l'événement**	**Principe de sécurité violé**
Destruction/suppression des données à caractère personnel	Indisponibilité irréversible des données à caractère personnel traitées par la Société. La violation peut être liée à une suppression logique non autorisée (par exemple, suppression des données, perte irréversible des mesures de sécurité utilisées pour la protection des données) et/ou à la destruction physique (par ex. rupture des supports), avec l'impossibilité de restaurer les informations.	Disponibilité
Perte ou vol de données à caractère personnel	Perte de contrôle sur les ressources d'archivage physiques telles que la privation, la soustraction, la perte de périphériques ou de documents papier. Une violation peut ne pas se matérialiser lorsqu'il est possible d'exclure avec un degré de certitude raisonnable l'accès non autorisé aux données et si la perte de mémoire physique n'entraîne pas une perte permanente de données à caractère personnel.	Disponibilité et confidentialité
Altération ou modification de données à caractère personnel	L'altération ou la modification non autorisée ou illégitime des données, qui n'a pas été détectée ou modifiée dans les processus internes, causant ainsi le traitement ou la divulgation incorrecte des données à caractère personnel. Une altération illégitime peut survenir lors d'opérations de traitement ordinaires effectuées par le personnel autorisé ou en cas de modifications frauduleuses par des personnes non autorisées.	Intégrité
Divulgation des données à caractère personnel	La divulgation non autorisée ou inappropriée de données à caractère personnel à des tiers (personnes physiques ou morales, groupes d'entités, public). Une violation peut ne pas se matérialiser lorsqu'il est possible d'exclure avec un degré de certitude raisonnable l'accès non autorisé aux données.	Confidentialité
Accès illégitime ou non autorisé	Accès aux informations à caractère personnel traitées par la Société de la part de tiers non autorisés.	Confidentialité

Une violation des données à caractère personnel peut constituer un risque qui porte atteinte aux droits des personnes impactées et peut entraîner des dommages physiques, matériels ou immatériels à ces derniers. À titre d'exemple, parmi les dommages, figurent le vol d'identité, les pertes financières, les dommages économiques ou sociaux.

À cette fin, le responsable doit notifier la violation des données à caractère personnel à l'autorité de contrôle, sans retard indu et, si possible, dans les 72 heures à partir du moment où il en a eu connaissance. Cette mesure ne doit être accomplie que si la violation présente un risque pour les droits et les libertés des personnes concernées et si le responsable du traitement ne peut démontrer que, conformément au principe de responsabilité, un tel risque est improbable (article 33, point 1 du RGPD). Au-delà de la période de 72 heures, cette notification devrait

être accompagnée des raisons du retard et les informations pourraient être fournies à des stades ultérieurs sans autre retard injustifié.

Voici des exemples d'événements susceptibles de conduire à une violation de données, qui peuvent concerner à la fois des données personnelles stockées sous forme électronique et sur papier :

- vol de matériel contenant un dossier de données à caractère personnel ;
- perte de données ;
- interruption des lignes de transmission données (ou des lignes téléphoniques) qui empêchent aux personnes concernées de contacter le titulaire du traitement et d'avoir accès à leurs données ;
- attaque de type « *ransomware* » qui fait que toutes les données sont cryptées. Aucune sauvegarde n'est disponible et les données ne peuvent être restaurées ;
- communication de données à caractère personnel de personnes concernées à des destinataires erronés (non chargés du traitement), y compris la communication à des personnes qui ne sont pas autorisées à avoir accès aux données à caractère personnel (par ex : parents, amis ou personnes autres que les Destinataires ou les entités auxquels les données à caractère personnel doivent être communiquées pour l'exécution de l'activité de la Société) ;
- violation des sites Internet de la Société suite à une cyber-attaque, avec pour conséquence l'extraction de données à caractère personnel des personnes concernées ;
- toute installation de logiciel malveillant ou de virus téléchargé sur les appareils fournis par la Société qui peut créer une perte de disponibilité de données à caractère personnel, l'accès abusif à des données à caractère personnel ou la soustraction de données à caractère personnel ;
- violation de boîtes de messagerie électronique des employés ;
- vol d'identité signalé par les forces de l'ordre ;
- violation de la sécurité physique : vol ou intrusion dans les locaux du titulaire/responsable du traitement ;
- attaques par déni de service (DdS) qui indiquent un dysfonctionnement dû à une attaque informatique entraînant l'épuisement délibéré des ressources d'un système informatique qui fournit un service aux clients, par ex. un site Internet sur un serveur d'hébergement, jusqu'à le rendre inapte à rendre le service aux clients demandeurs ;
- attaques en déni de service distribué (DDoS) à savoir le trafic de données inondant la victime provient de nombreuses sources différentes;
- accès non autorisé aux données ;
- perte ou soustraction de documents papier ou électroniques contenant des données à caractère personnel, par exemple le vol d'un enveloppe contenant des données de clients ou d'employés.

3.2 Structures impliquées

Afin de gérer les éventuelles violations de données à caractère personnel de manière optimale et fonctionnelle, le Comité pour la protection de la vie privée assure des compétences spécifiques, pertinentes en matière de protection des données, de sécurité des informations et des systèmes informatiques.

4. Les étapes de gestion d'une violation de données

4.1 Détection

Le processus d'analyse et de gestion d'une violation de données à caractère personnel commence par le signalement d'un événement, d'une anomalie ou d'un dysfonctionnement susceptible de constituer une violation de données à caractère personnel. Le début du délai temporel utile pour la communication à l'autorité de contrôle commence à partir du moment où la violation est connue. Il est donc essentiel que, dans un premier temps, le canal qui active l'alerte soit informé de la présence de données à caractère personnel dans le lot d'informations affectées.
Jusqu'à la conclusion formelle de la phase de détection, la violation ne peut être considérée comme certifiée.

La détection de la violation est la phase durant laquelle il faut identifier correctement le type de violation de données à caractère personnel, les catégories d'entités impliquées et la classification de l'incident de sécurité (confidentialité, indisponibilité, intégrité).

Les violations peuvent donc être détectées aussi bien à l'intérieur qu'à l'extérieur de la Société et parvenir à celle-ci par le signalement direct de la part de la personne concernée, d'un employé, des forces de l'ordre ou de l'autorité de contrôle, d'un fournisseur et, en particulier, des sous-traitants externes du traitement, ou encore par d'autres canaux tels que les médias.

5. **Procédure en cas de violation de données détectée par une personne faisant partie de la Société**

Toute violation détectée en interne par la Société doit être signalée immédiatement.

En outre, dès que la violation est identifiée, le Destinataire concerné doit immédiatement - et en tout cas au plus tard deux heures à compter de la prise de connaissance ou la suspicion de la violation des données à caractère personnel – envoyer une communication à la Société en écrivant à l'adresse électronique dédiée, à savoir databreach@falckrenewables.com, en fournissant les informations suivantes :

- la nature de la violation des données à caractère personnel concernées et si possible ;
- les catégories et le nombre approximatif de personnes dont les données ont fait l'objet de la violation ;
- les catégories et le nombre approximatif d'enregistrements des données à caractère personnel en question ; et
- toute autre information permettant d'identifier les données objet de la violation et d'en atténuer les conséquences négatives.

Dans les 24 heures après la communication, le Comité pour la protection de la vie privée devra organiser une réunion à laquelle participeront des intervenants spécialisés dans les domaines techniques et informatiques relatifs au type de violation avérée. La procédure devra ensuite suivre les modalités décrites au paragraphe 5.2 ci-après.

6. Procédure en cas de violation de données détectée par une entité externe à la Société

Si un responsable du traitement – comme par exemple un prestataire de services, un agent, un partenaire commercial ou un consultant – détecte ou suspecte une violation de données à caractère personnel dont la Société est le responsable du traitement, le tiers devra, dès que la violation est détectée, immédiatement et sans retard injustifié, et en tout cas dans les 24 heures suivant la prise de connaissance de la violation des données à caractère personnel, en lui écrivant à l'adresse databreach@falckrenewables.com

Dans les 24 heures suivant la communication, le Comité pour la protection de la vie privée doit organiser une réunion à laquelle participeront des intervenants spécialisés dans les domaines techniques et informatiques relatifs au type de violation avérée, en évaluant la participation possible également d'un représentant du tiers afin d'obtenir plus de détails sur la violation et de pouvoir mieux définir les mesures à prendre afin de remédier à la violation des données personnelles et atténuer les effets négatifs possibles. La procédure devra ensuite suivre les modalités décrites au paragraphe 5.2 ci-après.
Les contrats avec les tiers devront prévoir la désignation d'un responsable du traitement qui comprendra la procédure prévue au présent paragraphe 5 et les obligations de collaboration énoncées dans le RGPD.

Tout au long de la période de résolution de l'incident, les informations y afférentes et partagées entre les membres du Comité pour la protection de la vie privée sont considérées comme confidentielles et ne doivent être divulguées qu'aux unités organisationnelles et aux fonctions d'entreprise concernées.

7. Gestion et vérification des violations

Après la survenance d'un incident, le Comité pour la protection de la vie privée se charge de la gestion de la violation, en identifiant et en mettant en œuvre la stratégie d'isolement et d'action la plus efficace pour réduire au minimum toute conséquence supplémentaire en adoptant des contre-mesures spécifiques, et pour éviter l'aggravation de la situation, ainsi que pourvoir à restaurer en temps opportun la disponibilité et l'accès aux données à caractère personnel.

Dans les 24 heures suivant la communication, le Comité pour la protection de la Vie Privée devra organiser une réunion à laquelle toutes les structures opérationnelles (les « Structures ») jugées nécessaires en vue de la collecte d'informations sur la violation de données à caractère personnel seront conviées à participer. Dans cette réunion, et pendant les phases préparatoires de celle-ci, les Structures devront obtenir des entités concernées toutes les informations relatives à la violation des données à caractère personnel. Le but de la réunion sera de :

- définir les causes, la nature et l'étendue de la violation des données personnelles, la quantité, le type et le nombre de personnes concernées auxquelles se réfèrent les données à caractère personnel faisant l'objet de la violation, en rassemblant les informations à notifier éventuellement à l'autorité de contrôle conformément à l'article 33 avec le support du département informatique et des sous-traitants internes du traitement ;
- analyser les actions déjà entreprises et définir les actions à entreprendre pour remédier à la violation des données à caractère personnel et pour atténuer les éventuels effets négatifs (y compris la possibilité de supprimer à distance les données contenues dans le dispositif électronique) ; et
- évaluer le niveau de risque lié à la violation, comme cela est décrit au paragraphe 5.3 suivant, afin de déterminer si une notification à l'autorité de contrôle en vertu de l'article 33 du RGPD et une communication aux personnes concernées en vertu de l'article 34 du RGPD sont nécessaires.

Ci-après, une liste non exhaustive des activités prévues pour l'isolement de l'incident :

- Suivi constant de l'évolution de la situation ; le suivi du niveau de criticité est un processus continu et transversal à toutes les phases de gestion de l'incident puisque, en l'absence de contre-mesures efficaces, l'évolution de la situation relative à un incident en cours peut s'aggraver et nécessiter l'implication progressive de niveaux supérieurs de l'entreprise.
- L'analyse du dommage, le statut des actifs impactés et le volume de données violées.
- Suivi du temps employé et des ressources nécessaires.
- Isolement de l'incident, tout en réduisant au minimum les impacts produits par celui-ci et en prévenant d'autres dommages par l'application de contre-mesures techniques, organisationnelles et procédurales, qui doivent être formalisées et faire l'objet d'un traçage.

- Mise en œuvre des activités nécessaires pour rétablir, si possible, la situation avant l'incident.

Le Comité pour la protection de la vie privée vérifie le signalement de la violation potentielle de données à caractère personnel afin de déterminer la présence effective d'une menace pour les droits et les libertés des entités concernées, en vérifiant au moins :

- les informations relatives à la nature de l'incident (quand, où, type de violation de sécurité, systèmes et/ou dispositifs ayant fait l'objet de la violation) ;
- les catégories d'entités concernées affectées ;
- le volume des données affectées ;
- les mesures prises ou à prendre pour y remédier ;
- les risques probables sur les droits et les libertés des entités concernées par la violation de données ;
- les méthodes et les outils pour la résolution de l'incident.

Il est estimé que la Société peut acquérir un degré de certitude raisonnable quant à une violation de données à caractère personnel en présence de :

- informations concrètes concernant la violation des données à caractère personnel ;
- preuves de la perte de confidentialité, intégrité, disponibilité des données à caractère personnel ;
- conséquences sur les droits et les libertés des personnes concernées découlant sans aucun doute possible de l'incident de sécurité.

8. Niveau de risque

Lors de la définition du niveau de risque, toutes les conséquences potentielles et les effets négatifs probables susceptibles d'avoir un impact sur les personnes concernées doivent être pris en compte.

Sur la base des indications du Groupe de travail visé à l'Article 29. « *Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679* », et en particulier du document préparé par ENISA « Recommandations pour une méthodologie de l'évaluation de la gravité des violations des données à caractère personnel », Document de travail, v. 1.0, décembre 2013, les éléments à prendre en compte dans l'évaluation sont :

- *Contexte du Traitement (CT) : le critère prend en considération le type de données à caractère personnel impliquées dans la violation des données à caractère personnel en corrélation à des facteurs spécifiques du traitement qui pourraient aggraver ou atténuer l'impact sur la personne concernée (volume des données enfreintes, circonstances particulières de la Société, circonstances particulières de la personne concernée, disponibilité publique des données, exactitude des données).* La valeur du critère est comprise entre 1 et 4.
- *Facilité d'Identification (FI) :* le critère envisage la possibilité d'identifier ponctuellement une personne sur la base de la donnée objet de la violation, en considérant aussi les cas de violation simultanée de plus d'une typologie de données d'une même personne. Le critère est utilisé comme valeur de correction du contexte du traitement, car moins la personne est identifiable sur la base des identifiants communs, moins la violation sera grave.
- *Circonstances de la Violation (CV) :* circonstances spécifiques de la violation en corrélation avec la catégorie de la violation (perte d'intégrité, confidentialité, disponibilité).

En tenant compte de ces éléments, il est possible de classer tous les événements. Pour chacun des critères ci-dessus, il a été défini un ensemble de valeurs à sélectionner par rapport aux caractéristiques de la violation analysée.

Le résultat final est converti en une échelle qualitative à 4 valeurs (Faible, Moyenne, Élevée, Très Élevée). Selon le niveau de risque obtenu, on distingue :

- la présence ou l'absence de préjudices pour les personnes faisant l'objet de la violation ;
- la nécessité d'établir des communications avec l'autorité de contrôle et/ou les personnes concernées.

Gravité de la violation des données (*severity*) – tableau récapitulatif	
FAIBLE	Les personnes concernées ne seront pas affectées ou pourront rencontrer quelques problèmes mineurs, surmontables sans difficultés particulières (temps passé à ressaisir les informations, gêne, colère, etc.).
MOYENNE	Les personnes concernées peuvent connaître des difficultés majeures, qu'elles seront en mesure de surmonter malgré quelques difficultés (frais supplémentaires, refus d'accéder aux services de l'entreprise, peur, manque de compréhension, stress, troubles physiques mineurs, etc. ...).
ÉLEVÉE	Les personnes concernées peuvent faire face à des conséquences significatives, qu'ils devraient pouvoir surmonter même si avec de graves difficultés (détournement de fonds, mise sur la liste noire par les banques, atteinte à la propriété, perte d'emplois, litiges, problèmes de santé, etc.).
TRÈS ÉLEVÉE	Les personnes peuvent être confrontées à des conséquences lourdes, voire même irréversibles, qu'elles ne seront pas en mesure de surmonter (difficultés financières telles qu'une dette substantielle ou une incapacité de travail, troubles psychologiques ou physiques à long terme, décès, etc. ...).

Les systèmes de mesure et la méthodologie utilisée permettent de classer comme faibles tous les événements qui, bien qu'ils puissent présenter formellement des caractéristiques de violation des données à caractère personnel, ne constituent en rien un préjudice pour les personnes concernées et pour lesquels aucune communication n'est jugée nécessaire, ni à l'attention de l'Autorité de contrôle ni à l'égard des personnes concernées.
En général, en analysant la classification des violations, il est considéré que :

- en cas d'éventuelle *violation de la confidentialité ou de l'intégrité*, si les données à caractère personnel sur lesquelles porte la violation ne sont pas intelligibles, ont été anonymisées ou pseudonymisées, l'impact associé à la violation pourrait être faible et de ce fait ne nécessiter aucune notification à l'attention de l'Autorité de contrôle ou de la personne concernée ;
- en cas d'éventuelle *perte de disponibilité*, s'il existe des copies ou des sauvegardes des données, l'impact associé à la violation pourrait être faible et de ce fait ne nécessiter aucune notification à l'attention de l'Autorité de contrôle ou de la personne concernée.

Si la Société n'arrive pas à évaluer, dans les 48 heures suivant sa détection, la violation survenue en raison d'un manque d'informations précises, il faudra réaliser une analyse d'impact qui prendra en compte le *pire des cas* afin de pouvoir envoyer la communication à l'Autorité de contrôle dans les 72 heures suivant la connaissance de la violation.

Si la violation des données à caractère personnel revêt une gravité élevée ou très élevée, qui nécessite une notification à l'Autorité de contrôle en vertu du paragraphe 5.4 ci-dessous, celle-ci sera classée comme un événement de crise aux fins de la Procédure de *gestion de la communication de crise* et l'Équipe de crise sera impliquée conformément aux prescriptions de cette procédure.

9. Notification

Comme indiqué précédemment, dès que le responsable du traitement est raisonnablement certain que la violation pourrait comporter un risque pour les personnes concernées, il a le devoir de notifier à l'autorité de contrôle toutes les violations de données à caractère personnel susceptibles de porter atteinte aux droits et aux libertés des personnes concernées.

Plus précisément, cette notification doit contenir au moins :

- une description des mesures prises ou proposées pour remédier à la violation de données à caractère personnel et aussi, le cas échéant, pour atténuer ses éventuels effets négatifs;
- le nom et les coordonnées du responsable de la protection des données ou d'un autre point de contact auprès duquel il est possible d'obtenir de plus amples informations ;
- une description des conséquences probables de la violation des données à caractère personnel ;
- une description des mesures prises ou envisagées pour remédier à la violation des données à caractère personnel et, le cas échéant, pour en atténuer les effets négatifs éventuels.

Au cas où les informations ne seraient pas disponibles d'ici 72 heures, il sera possible de les fournir par étapes successives sans autre retard injustifié et de choisir l'une des deux options suivantes :

- *Notification par étapes : en raison de la complexité de la violation ou de la prolongation des analyses sur la violation de la sécurité, le responsable du traitement peut fournir, dans les 72 heures, une première description du contexte de la violation afin d'alerter l'autorité de contrôle.* Les informations manquantes seront communiquées par étapes successives au moyen d'autres notifications appropriées pour dresser le panorama complet et exhaustif de la violation des données à caractère personnel.
- *Notification avec données approximatives* : approximation de certaines informations qui peuvent être détaillées dans les étapes successives (par exemple, approximation du nombre de personnes physiques impliquées dans la violation des données à caractère personnel).

En général, si une notification n'est pas envoyée dans les 72 heures, la notification doit inclure les raisons du retard sur la base des circonstances spécifiques.
L'obligation de notification à l'attention de l'Autorité de contrôle et/ou des personnes concernées ne s'applique pas lorsque la Société démontre, conformément au principe de responsabilisation, que la violation ne comporte pas de risque pour les droits et les libertés des personnes concernées.

L'identification de l'inexistence de risques pour les droits et les libertés des personnes concernées doit prendre en considération :

- le résultat de l'évaluation de la violation des données ;
- toutes les conséquences possibles, actuelles ou futures, découlant de la perte des principes de sécurité, ainsi que de la protection des données : intégrité, disponibilité, confidentialité ;
- les mesures techniques et organisationnelles mises en œuvre précédemment et suite à la violation des données à caractère personnel afin de protéger la personne concernée en réduisant l'impact de la violation sur les personnes physiques, et de restaurer rapidement la disponibilité et l'accès aux données à caractère personnel.

10. Notification à la personne concernée

Si le niveau de risque découlant de la violation des données à caractère personnel suite à l'évaluation visée au paragraphe 5.3 s'avère élevé ou très élevé pour les droits et les libertés de la personne physique dont les données à caractère personnel ont été affectées par l'événement, le responsable du traitement (lorsqu'il n'y a aucune raison de ne pas donner suite à la communication) a l'obligation de communiquer la nouvelle de l'événement également aux personnes physiques dont les données sont concernées par la violation. La notification a pour but de permettre à la personne concernée de prendre toutes les précautions nécessaires pour atténuer les effets négatifs potentiels et elle doit obligatoirement être envoyée sans retard injustifié.
Pour la définition et la préparation d'une communication adéquate à l'attention des personnes concernées affectées par la violation, il faut prendre en considération :

- les informations nécessaires et adaptées au contexte qui doivent être fournies à la personne concernée :
- les modalités d'exécution.

La communication aux personnes concernées doit fournir au moins :

- la description de la nature de la violation des données à caractère personnel ;
- la description des conséquences probables des violations des données à caractère personnel ;
- la description des mesures adoptées ou envisagées pour remédier à la violation des données à caractère personnel et, le cas échéant, pour en atténuer les effets négatifs éventuels ;
- le nom et les coordonnées du responsable de la protection des données ou d'un autre point de contact auprès duquel de plus amples informations peuvent être obtenues;
- dans la mesure du possible ou en cas de suggestion spécifique de la part de l'Autorité de contrôle, la liste des bonnes pratiques et/ou des mesures spécifiques à adopter par les personnes physiques affectées par la violation, afin d'atténuer les conséquences négatives ;
- toute autre information jugée utile.

Les contenus énumérés devront être transmis à la personne concernée par des canaux directs (exemple : courrier électronique, texto), en recourant à une communication claire, transparente et explicite. Le choix de la modalité de communication devra tenir compte de l'accessibilité des personnes concernées aux différents formats et, en cas de besoin, les diversités linguistiques des destinataires.
Sur la base des circonstances spécifiques de l'événement, il conviendra de choisir la méthode de communication permettant de maximiser la réception des informations par la personne concernée de manière correcte, simple et pratique, tout en garantissant la sécurité du transfert des informations.
La communication doit être effectuée dès que cela est raisonnablement possible, en tenant compte des orientations pertinentes en la matière émanant de l'autorité de contrôle, des conséquences qui pourraient dériver du contexte spécifique de la violation ainsi que de la nature des données et des finalités du traitement, des conséquences qui pourraient affecter la gestion de l'incident et l'isolement de la violation.

La Société n'est pas tenue de communiquer la violation aux personnes concernées si l'une des conditions suivantes est remplie :

- des mesures techniques et organisationnelles de protection appropriées ont été mises en place et ces mesures ont été appliquées aux données à caractère personnel objet de la violation, en particulier celles qui visent à rendre les données à caractère personnel incompréhensibles à toute personne non autorisée à y accéder (exemple : chiffrement) ;
- après la détection de l'événement, le responsable du traitement a adopté, en temps opportun, des mesures visant à éviter l'apparition d'un risque élevé pour les droits et les libertés des personnes concernées ;
- si le mode de communication directe s'avère être un effort disproportionné pour le Titulaire du traitement dont les données ont été affectées par la violation, ce dernier peut recourir aux canaux de communication publique, dès lors que le mode de communication est efficace du point de vue de l'exactitude et de la transparence, et qu'il ne porte pas davantage atteinte à la vie privée de la personne concernée.

11. Registre des violations de données

Conformément au Règlement, le Titulaire du Traitement documente toute violation des données à caractère personnel, y compris les circonstances qui s'y rapportent, ses conséquences et les mesures prises pour y remédier, dans un registre des violations. Cette documentation permet à l'Autorité de contrôle de vérifier la conformité des évaluations, des précautions et des décisions prises en vertu de l'article 33 du RGPD.

Ce document est conservé et implémenté par l'Expert en protection de la vie privée ou, à sa place, par le CDT&IO, qui garantissent l'exhaustivité, la mise à jour et l'intégrité des informations qu'il contient.
Rappelons que, dans le cas où l'événement signalé n'a pas été évalué comme une violation des données à caractère personnel, il faudra noter les raisons qui ont conduit à ce type d'évaluation.

Annexe E
Politique de conservation des données

1. Introduction et finalité

La présente Politique de conservation des données (ci-après la « Politique ») vise à illustrer les obligations auxquelles tous les employés et collaborateurs (ci-après les « Destinataires ») doivent se conformer en référence aux durées de conservation des données à caractère personnel afin de garantir la conformité des sociétés du Groupe au Règlement (UE) 2016/679 du Parlement et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que la libre circulation de ces données (ci-après le « Règlement sur la protection de la vie privée » ou « RGPD »).

2. À qui ou à quoi la présente Politique s'applique-t-elle ?

La Politique s'applique à :

a) tous les documents, archives ou registres créés (ci-après les « Documents ») ou reçus par le Groupe, quel que soit le support ou le format (à savoir, électronique, courriel, image, papier, etc.) contenant des données à caractère personnel ;
b) tous les environnements physiques où les Documents sont stockés (y compris les structures gérées par d'éventuels prestataires de services) ;
c) tous les employés et collaborateurs des différentes unités organisationnelles du groupe et de ses fournisseurs.

Là où cette Politique ne fait pas référence à un précis document, archive ou registre, il faut se conformer aux principes suivants :

a) les données à caractère personnel devront être stockées pour la durée strictement nécessaire pour satisfaire aux finalités pour lesquelles les données ont été collectées ;
b) lorsque les données à caractère personnel contenues dans le Document sont supprimées ou anonymisées, ce Document pourra être conservé pour une période plus longue (sans préjudice des restrictions imposées par toute disposition légale ou d'éventuelles mesures dues à la sensibilité du document) ;
c) il est généralement interdit de conserver les documents pour une durée indéterminée, sauf circonstances particulières.

d) Où puis-je obtenir plus d'informations concernant cette Politique ?

Pour toute clarification concernant cette politique, vous pouvez vous adresser à l'Expert en protection de la vie privée du Groupe qui peut être contacté à l'adresse suivante : privacyexpert@falckrenewables.com.

e) Destruction des données

Les Documents qui dépassent les délais de conservation indiqués dans le tableau suivant peuvent être détruits après l'approbation de l'Expert en protection de la vie privée. En tout état de cause, la destruction prématurée du document est expressément interdite.

TABLEAU DE CONSERVATION DES DONNÉES

Description des disposition réglementaire concernant le stockage des données à caractère personnel	**Nature des documents contenant des données à caractère personnel**	**Durée de conservation**	**Commentaires**
PRINCIPE GÉNÉRAL – Limitation à la conservation des données à caractère personnel.	Tout document contenant des données à caractère personnel.	Les Documents doivent être conservés sous une forme permettant l'identification des personnes concernées pour une période n'excédant pas la réalisation des finalités pour lesquelles les données ont été collectées ou, en tout cas, traitées. Cependant, lorsque les règles applicables au cas concret prévoient un délai plus long, celui-ci prévaut.	Ce principe est applicable à tout traitement de données à caractère personnel. En ce qui concerne les contrats contenant des données à caractère personnel, il est conseillé de conserver les Documents jusqu'à une période de 10 ans après la fin du même contrat à des fins probatoires en cas de litige.
SANTÉ ET SÉCURITÉ			
Registre de contrôle des équipements de travail.	Le Registre de contrôle des équipements de travail est un document contenant la description de l'état de conservation des outils de travail.	Durée indéfinie. Le document doit toujours être disponible en cas d'inspection par les autorités.	

Registre des expositions et dossiers de santé et Registre des personnes exposées et des événements accidentels concernant les employés susceptibles de réaliser des activités dangereuses ou de travailler dans des environnements insalubres (c'est-à-dire les activités nécessitant l'utilisation de substances dangereuses).		À conserver jusqu'à la fin de la relation contractuelle. Il est cependant conseillé de (i) mettre à jour ces registres régulièrement (idéalement sur une base annuelle) et de (ii) conserver les registres pendant au moins 10 ans à compter de la fin de la relation de travail.	Ce registre devra être disponible en cas d'inspection par les autorités.

Obligation de dresser une évaluation des risques liés aux équipements de travail et des substances ou mélanges chimiques utilisés. L'évaluation des risques a pour but d'identifier : (i) tout risque pour la sécurité et la santé pendant le travail, (ii) les mesures de prévention et de protection mises en œuvre et les équipements de protection individuels adoptés ; (iii) le programme des mesures jugées opportunes pour assurer l'amélioration des niveaux de sécurité dans le temps ; (iv) l'identification des procédures pour l'application des mesures à mettre en œuvre ; (v) l'indication du nom du responsable du service de prévention et de protection, du représentant des travailleurs pour la sécurité ou du service territorial et du médecin compétent qui a	Documentation sur l'évaluation des risques.	À durée indéterminée.	

participé à l'évaluation des risques, (vi) l'identification des tâches susceptibles d'exposer les travailleurs à des risques spécifiques nécessitant des compétences professionnelles reconnues.			
Obligation de conserver toutes les données relatives aux visites médicales de l'employé, si nécessaire.	Registre des visites médicales.	Il n'existe aucune indication quant aux durées de conservation de ce document. Il est cependant conseillé de (i) mettre à jour ce registre régulièrement (au moins une fois par an) et de (ii) conserver le registre pendant au moins 10 ans à compter de la fin de la relation de travail.	
COMPTABILITÉ et AUDIT / DROIT DES SOCIÉTÉS			
Obligation de conserver les livres, les écritures comptables et la correspondance commerciale.	Les livres, les écritures comptables et la correspondance commerciale (par exemple, le livre-journal, les livres auxiliaires, les pièces justificatives qui documentent les éléments importants des enregistrements et tous les documents écrits envoyés, reçus ou internes ayant un caractère et une pertinence comptable).	10 ans à compter de la date de rédaction de ces documents – ce délai peut être plus long (i) pour des fins fiscales et (ii) en cas de jugement lorsqu'une demande de présentation de ces documents a été formulée.	Il est impératif que les indications sur la façon de rédiger les livres et les écritures comptables requis par le Code Civil soient respectées.
DROITS DE PROPRIÉTÉ INTELLECTUELLE			

Documentation relative aux marques, brevets, noms de domaine, secrets industriels, etc.		Il n'existe pas de durée définie pour la conservation des documents relatifs aux droits de propriété intellectuelle. Toutefois, à des fins probatoires, nous suggérons de conserver ces documents indéfiniment (par exemple, les certificats d'enregistrement des marques, brevets, etc.)	
LUTTE CONTRE LE BLANCHIMENT D'ARGENT			
Obligation de conserver les documents, les données et les informations utiles pour prévenir, identifier ou vérifier toute activité de blanchiment de capitaux ou de financement du terrorisme et pour permettre la réalisation des analyses effectuées, dans le cadre des attributions respectives, par la cellule de renseignement financier ou une quelconque autorité compétente.	Documents et données collectés lors de la vérification des clients et/ou des fournisseurs.	10 ans à compter de la fin de la relation d'affaires.	

DOCUMENTS RH			
Obligation de conserver (i) les données concernant les employés (à savoir, le nom et le prénom et le numéro d'identification fiscale), (ii) le nombre total	Livre unique.	5 ans à compter de la date de la dernière inscription.	Pendant la durée de conservation, les données doivent être conservées dans

d'employés ainsi que leur qualification et leur niveau professionnel, (iii) les positions d'assurance.			le respect des règles de protection des données à caractère personnel En référence aux données/documents relatifs aux anciens employés, ceux-ci doivent être inclus dans un fichier électronique accessible uniquement au dirigeant de la DRH ou à une entité spécifiquement désignée en ce sens par ce dernier et au Conseil d'administration et à d'autres organes de direction internes éventuellement autorisés.
Obligation de conserver toutes les données relatives aux procédures d'embauche et de la relation de travail.	Documentation sur les procédures d'embauche, sur le contrat de travail et la documentation correspondante.	Aucune disposition spécifique n'est prévue à cet égard. Toutefois, il est conseillé de conserver ces documents pour une période d'au moins 10 ans à compter de la fin de la relation de travail. Les données des candidats seront conservées, dans le cas de candidatures envoyées pour postuler à des postes déterminés, jusqu'à 12 mois après la fin de la phase de sélection et, dans le cas de candidatures spontanées, jusqu'à 24 mois après la collecte des données.	

Obligation de conserver toutes les données relatives aux salaires versés aux employés.	Bulletins de paie et autres documents relatifs aux paiements.	Les bulletins de paie et autres documents similaires relatifs à la rémunération des employés doivent donc être conservés pendant une période de 5 ans à compter de leur dernier enregistrement. Toutefois, il est conseillé de conserver ces informations pendant une période d'au moins 10 ans à compter de la fin de la relation de travail.	
Hormis le cas où d'autres prévisions spécifiques prévoyant autrement, les données à caractère personnel des employés (y compris les données contenues dans les contrats de travail et les contrats de travail mêmes) doivent être conservées pendant une période non supérieure à ce qui nécessaire dans le cadre des finalités pour lesquelles les données ont été collectées.	Autres données d'employés.	Afin de protéger les intérêts de la société en cas d'actions de la part des employés suite à la fin d'une relation de de travail, il est conseillé de conserver ces documents pour une période d'au moins 10 ans à compter de la fin de la relation de travail.	
Obligation de conserver toutes les données relatives aux cotisations retraites et déductions fiscales.	Données relatives aux cotisations retraites et déductions fiscales.	Ces informations sont soumises à une obligation de conservation de cinq ans. Toutefois, il est conseillé de conserver ces documents pour une période d'au moins 10 ans à compter de la fin de la relation de travail.	
Obligation de conserver toutes les données relatives (i) aux certificats de famille et aux documents relatifs à la Prime pour l'Unité Familiale et (ii) tout paiement effectué aux institutions de sécurité sociale	Obligation de conserver toutes les données relatives (i) aux certificats de famille et aux documents relatifs à la Prime pour l'Unité Familiale et (ii) tout paiement effectué aux institutions de sécurité sociale	Ces informations sont soumises à une obligation de conservation de cinq ans. Toutefois, il est conseillé de conserver ces documents pour une période d'au moins 10 ans à compter de la fin de la relation de travail.	

contre les Accidents du Travail).			
Limite à la conservation des images de vidéosurveillance	Vidéos relatives aux individus.	Vingt-quatre heures après l'enregistrement, à l'exception d'exigences spéciales relatives à une conservation plus longue en raison de jours de fête ou de fermeture des bureaux ou magasins ainsi que dans le cas où une enquête de l'autorité judiciaire ou de la police serait en cours.	
Limite à la conservation des communications échangées par courriers électroniques des anciens employés	Communications contenues dans la boîte de messagerie des anciens employés.	Pour le courrier électronique entrant/sortant de l'ancien employé : 3 mois après la fin du contrat de travail pour assurer la continuité de l'activité professionnelle et de l'*activité de l'entreprise*. Concernant uniquement les communications stockés par l'ancien employé dans le système de gestion documentaire car importantes pour la continuité de l'activité de l'entreprise : 10 ans après la fin du contrat de travail. En cas d'exigences démontrées de protection ou d'exercice d'un droit de la Société devant une instance judiciaire ou extra-judiciaire ou de demandes des autorités : jusqu'à la conclusion du dernier jugement et/ou conclusion de la phase extra-judiciaire et, dans tous les cas, jamais au-delà des 10 ans après la fin du contrat de travail.	

Limite à la conservation des données à caractère personnel des employés collectées au moyen des badges d'accès	Données d'accès par badges Données d'accès par badges.	5 ans à compter de la collecte 5 ans à compter de la collecte.	
Obligation de conserver toutes les données relatives à la présence des employés	Calendrier de présence.	5 ans à compter du dernier enregistrement.	

au travail.			
DOCUMENTS RELATIFS AUX ACTIVITÉS DE MARKETING			
Données collectées et traitées à des fins de marketing.	Tout document pertinent.	Aucune disposition spécifique n'est prévue à cet égard. Toutefois, en fonction des préférences, il est possible de conserver ces données, après consentement de la part des personnes concernées, pendant 24 mois après leur collecte	
Données traitées à des fins de profilage.	Tout document pertinent.	Aucune disposition spécifique n'est prévue à cet égard. Toutefois, en fonction des préférences, il est possible de conserver ces données, après consentement de la part des personnes concernées, pendant 24 mois après leur collecte	
JOURNAL DU SYSTÈME			
Enregistrement du journal du système	Fichiers électroniques	La durée de conservation des données est de 6 mois à compter de leur collecte.	