POLITIQUE RELATIVE À LA PROTECTION DES DONNÉES

Politiques de conformité – Politique 7.4 – Protection des données

Approuvé par	Le Conseil d'administration
Date d'origine :	24 août 2014
Date de la dernière révision :	2 juin 2018
Titulaire(s) de la Politique :	Responsable de la Conformité au niveau du Groupe
Contact(s) :	Responsable de la Conformité internationale

Dans ce document, la « Société » ou « ERG » désigne Eurasian Resources Group S.à.r.l et comprend, le cas échéant, toutes ses filiales directes et indirectes.

1. Objectif de la politique

1.1. Chaque Société du Groupe, dans le cadre de l'exploitation de son activité, collecte, stocke et traite des informations sur les personnes physiques. Ces personnes peuvent inclure les employés, les sous-traitants, les fournisseurs, les clients, les membres du Conseil d'administration, les directeurs, les actionnaires et les invités. Les Sociétés du Groupe respectent la vie privée des personnes susdites et leur droit à savoir ce que les Sociétés du Groupe font de leurs informations. Les Sociétés du Groupe appliquent la tolerence zéro à l'égard de toute infraction de la législation en vigueur, y compris et sans s'y limiter, le Règlement (UE) 2016/679 du Parlement européen et du Conseil 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 (Règlement général sur la protection des données).

1.2. La présente Politique a pour objet de :

1.2.1. veiller à ce que, en matière de collecte, de stockage, de traitement et de transfert des données à caractère personnel, chaque Société du Groupe exerce son activité dans le respect de l'ensemble des lois et règlements applicables et à ce que les données à caractère personnel soient toujours protégées et traitées dans le respect de la législation qui lui est applicable[1] ;

1.2.2. définir les types de Données à caractère personnel collectées par les Sociétés du Groupe et les objectifs de la collecte de ces données ;

1.2.3. définir les responsabilités de chaque Collaborateur en matière de collecte et de traitement des données conformément aux règlements en matière de protection des données ; et

1.2.4. veiller à ce que chaque Société du Groupe dispose d'un environnement de protection des données à caractère personnel normalisé pour permettre le transfert des données à caractère personnel entre les

[1] *Par exemple, dans l'**Union européenne**, la protection des données est régie par le Règlement général sur la protection des données (le Règlement (UE) 2016/679) et par autres documents documents exécutifs. Au **Royaume-Uni**, il s'agit essentiellement du Règlement général sur la protection des données et de la loi de 2018 (la Loi), mais aussi d'autres règlements ;*
*En **Suisse**, c'est la loi fédérale sur la protection des données du 19 juin 1992.*
*Au **Kazakhstan**, c'est la loi de la République du Kazakhstan du 21 mai 2013 № 94-V « Sur les données à caractère personnel et leur protection ».*
*En **Russie**, c'est la loi de la Fédération de Russie « Sur les données à caractère personnel » du 27.07.2006 n° 152-FZ avec des lois subordonnées et d'autres lois (par exemple le code sur les infractions administratives)*
*En **Afrique du Sud**, il s'agit de la loi n° 4 de 2013 : Loi de 2013 sur la protection des renseignements personnels*
*Il n'existe actuellement au **Brésil** aucune loi générale sur la protection des données. Néanmoins, un certain nombre de lois spécifiques, dont la loi sur les droits de l'Internet (Marco Civil da Internet) et le Code de protection des consommateurs (Codigo de Defensa de Consumidor), traitent de diverses questions relatives à la vie privée et à la protection des données. Un projet de loi sur la protection des données est cependant en cours d'examen au Congrès brésilien.*
*En **Chine –** la Décision sur le renforcement de la protection des réseaux d'information du 28 décembre 2012 ; le Règlement sur le service de l'emploi et la gestion de l'emploi ; les Mesures punissant les comportements portant atteinte aux droits et aux intérêts des consommateurs.*
*Aux **Émirats Arabes Unis** - Il n'existe pas de loi fédérale générale sur la protection des données aux Émirats Arabes Unis (EAU) comparable à celles applicables en Europe, bien que les organisations qui appartiennent à l'International Financial Center of Dubai (DIFC) soient régies par des lois générales complètes sur la protection des données.*

Sociétés du Groupe et s'assurer que les données à caractère personnel sont correctement protégées conformément aux lois internationales applicables en matière de transfert de données lorsqu'elles sont transférées au-delà des frontières.

2. Champ d'application

2.1. Cette politique s'applique à :

2.1.1. toutes les Sociétés du Groupe telles que définies ci-dessous et leurs agents ;

2.1.2. tous les Collaborateurs ; et

2.1.3. l'ensemble des Données à caractère personnel collectées, stockées et traitées par les Sociétés du Groupe au cours de leurs activités professionnelles, quel que soit le support sur lequel elles sont exploitées.

3. Définitions

Les définitions données ci-dessous sont des définitions internes qui, tout en conservant leur sens prévu par la législation applicable, peuvent avoir des noms différents selon les lois locales. Lors de l'élaboration des procédures locales, les Régions devraient suivre la terminologie et les concepts juridiques utilisés dans leurs législations nationales respectives, tout en veillant au respect des principes de la Politique.

3.1. **Le Conseil d'administration** désignera le Conseil d'administration d'Eurasian Resources Group SARL.

3.2. **Données personnelles des clients** désigne les données à caractère personnel collectées dans le cadre de la gestion ordinaire de la relation client, telles que les coordonnées des clients, leurs noms et adresses professionnelles.

3.3. **Responsable du contrôle des données** désigne la personne physique ou morale, autorité publique, agence ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les modalités du traitement des Données à caractère personnel.

3.4. **Délégué à la protection des données** désigne la personne physique qui est chargée de consulter et de veiller au respect de la législation locale en matière de protection des données par le Groupe, aussi bien que de remplir la foction de la personne à contacter pour les demandes internes et externes des Personnes concernées en matière de collecte et de traitement des données personnelles.

3.5. **Responsable du traitement des données** désigne la personne physique ou morale (y compris une Société du Groupe), autorité publique, agence ou toute autre entité qui traite des Données à caractère personnel pour le compte d'une Société du Groupe.

3.6. **Personne concernée** désigne toute personne physique identifié ou identifiable que les Données à caractère personnel concernent.

3.7. **Collaborateurs** désigne les employés à temps plein, à temps partiel et intérimaires des Sociétés du Groupe, stagiaires et sous-traitants travaillant dans les locaux des Sociétés du Groupe ou ayant accès aux systèmes informatiques des Sociétés du Groupe.

3.8. **Union européenne** désigne 28 pays membres qui forment l'Union européenne et sur lesquels s'étend la législation européenne.

3.9. **Espace économique européen (EEE)** désigne les pays européens qui ont inclu dans leur législation certaines normes reglémentaires de l'Union européenne et ont consenti à respecter pleinement la législation européenne en matière de protection des données personnelles.

3.10. **Données personnelles relatives aux Ressources humaines** désigne les Données à caractère personnel collectées dans le cadre de l'administration normale des ressources humaines, telles que le

nom, l'adresse, la nationalité, le sexe, l'état matrimonial, le numéro de sécurité sociale et le compte bancaire.

3.11. **Règlement général sur la protection des données** désine le Règlement (UE) 2016/679 du Parlement européen et du Conseil 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 et le Règlement 679/2018, acte législatif de l'UE dans le domaine de la confidentialité et de la protection des données personnelles qui est censé harmoniser les règles dans cette sphère. Ce règlement s'applique dans tous les pays de l'Union Européen et de l'EEE et régit le transfert et le traitement des données personnelles des personnes concernées dans l'UE et dans l'EEE qu'il s'agisse des actions réalisées sur le territoire de l'Union Européen ou l'EEE ou en dehors de leurs territoires.

3.12. **Sociétés du Groupe** englobe Eurasian Resources Group SARL et toute entité dans laquelle cette dernière détient, directement ou indirectement, plus de cinquante pour cent (50 %) des droits de vote, ou dans laquelle le pouvoir de contrôle de l'entité est détenu par ou pour le compte d'Eurasian Resources Group SARL.

3.13. **Actionnaires des Sociétés du Groupe** désigne les personnes physiques et (ou) les sociètès publiques ou privées étant en possession des actions des Sociétés du Groupe qui leur donnent le droit de vote.

3.14. **Représentant externe** désigne une personne extérieure aux Sociétés du Groupe nommée par le département de la Conformité afin de représenter les intérêts des bureaux des Sociétés du Groupe sans participation du Responsable de la Conformité. Le représentant externe intervient en tant que personne à contacter pour les questions relatives aux données personnelles de la part des citoyens et des résidents de l'UE et de l'EEE qui séjournent constamment ou temporairement en dehors des pays de l'UE et de l'EEE.

3.15. **Données à caractère personnel** désigne toute information de tout type quel que soit le support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable. Une personne physique est considérée comme identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel que le nom, le numéro d'identification, les données sur sa position géographique, l'identifiant sur Internet ou un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, mentale, culturelle, sociale ou économique. Même s'il n'est pas immédiatement évident de savoir si une personne peut être identifiée, cette personne peut néanmoins être identifiable si les Sociétés du Groupe disposent ou peuvent disposer de moyens raisonnables pour l'identifier.

3.16. **Atteinte à la confidentialité des Données personnelles** désigne une atteinte à la confidentialité des Données personnelles qui a causé la suppréssion fortuite ou illégale, la perte, le changement ou la divulgation non autorisée des Données personnelles transférées, gardées ou traitées d'une autre manière ou l'accès non autorisé à ces données.

3.17. **Traitement** désigne toute opération ou tout ensemble d'opérations effectuées sur les Données à caractère personnel, qu'elles soient ou non automatisées ou électroniques, telles que la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou l'altération, la récupération, la consultation, l'utilisation, la divulgation par transmission, diffusion ou toute autre forme de mise à disposition, alignement ou combinaison, blocage, effacement ou destruction.

3.18. **Régions** désigne un groupe d'une ou plusieurs Sociétés du Groupe situées dans la même zone géographique. Les régions du Groupe sont le Kazakhstan, l'Afrique, le Brésil et l'Europe.

3.19. **Données personnelles sensibles** désigne les Données à caractère personnel (d'après le Règlement général de la Commission européenne sur la protection des données et les actes de la législation locale des pays non-membres de l'UE) révélant la santé physique ou mentale de la Personne concernée, ses convictions religieuses ou similaires, ses opinions politiques, l'origine raciale ou ethnique, l'appartenance syndicale, les infractions pénales, l'orientation sexuelle, la vie sexuelle ainsi que les données génétiques.

3.20. **Données personnelles des clients** désigne les données à caractère personnel collectées dans le cadre de la gestion ordinaire de la relation client, telles que les coordonnées des clients, leurs noms et adresses professionnelles.

4. Énoncés de politique

4.1. Chaque Société du Groupe traite les Données à caractère personnel conformément aux lois et règlements en vigueur en matière de protection des données.

4.2. Chaque Société du Groupe et toutes les divisions opérationnelles, quelle que soit leur juridiction, doivent respecter les normes de pratique minimales suivantes :

4.2.1. Traitement loyal et licite des Données à caractère personnel : Les Sociétés du Groupe traitent les Données à caractère personnel d'une manière loyale et licite, ce qui nécessite notamment les éléments suivants :

a) Utilisation licite : Les Données à caractère personnel ne peuvent pas être utilisées d'une manière qui aurait des effets préjudiciables injustifiés ou disproportionnés sur une Personne concernée et/ou qui pourrait être illicite ;

b) Transparence : Les Sociétés du Groupe doivent être transparentes avec les Personnes concernées sur leurs activités de traitement (notamment sur l'existence et les conditions de traitement) ;

c) Restriction de l'objet : Les Données à caractère personnel ne doivent être collectées qu'à des fins spécifiques et licites et ne doivent être utilisées que d'une façon dont une Personne concernée peut raisonnablement s'attendre à ce qu'elles soient utilisées. Elles ne doivent également être traitées que d'une manière compatible avec les finalités pour lesquelles elles ont été collectées ;

d) Adéquation/minimisation des données : Les Données à caractère personnel doivent être adéquates et être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;

e) Précision : Les Données à caractère personnel doivent être exactes et mises à jour ;

f) Conservation : Les Données à caractère personnel doivent être conservées conformément aux exigences des politiques du groupe relatives à ce sujet et aux lois applicables. Néanmoins, elles ne devraient pas être conservées sous la forme qui permette d'établir la personnalité de la Personne concernée ou en dehors de la période nécessaire à la finalité pour laquelle elles sont traitées. EN principe, les Données à caractère personnel devraient être supprimées ou anonimisées une fois que la finalité pour laquelle elles sont traitées n'existe plus ;

g) Respect des droits des Personnes concernées : chaque Société du Groupe doit respecter et donner effet aux droits légaux des Personnes concernées lorsqu'elle traite leurs Données à caractère personnel.

4.2.2. Information et/ou consentement préalable : Si la loi locale l'exige, les Sociétés du Groupe doivent fournir aux Personnes concernées les informations de base requises sur les Données à caractère personnel qu'elles collectent et sur la manière dont elles vont les traiter[2] et, si nécessaire en conformité avec la législation locale, obtenir un consentement clair et explicite à cet effet de la Personne concernée. Ce consentement ne peut pas être exprimé sous la forme de l'inaction de la Personne concernée ou de l'utilisation par celle-ci d'une case du document comportant une remarque quelconque. Les avis de

[2] *Par exemple, en fonction des règles locales applicables en matière de protection des données, chaque Membre du groupe peut avoir besoin d'informer les Personnes concernées (i) de son identité ou de sa raison sociale ; (ii) des données collectées ou traitées ; (iii)(dans certains cas) des fins auxquelles les données sont traitées ; (iv) de la question de savoir si les données seront partagées avec quiconque ; et (v) de leurs droits postulés par la législation et de la manière de les réaliser.*

confidentialité doivent être mis à la disposition des Personnes concernées (par exemple publiés sur les sites Internet de toutes les Sociétés du Groupe ou via d'autres moyens de communication).

4.2.3. Sécurité des données : Chaque Société du Groupe est tenue de prendre des mesures nécessaires techniques, physiques et organisationnelles, y compris les mesures de protection contre tout Traitement non autorisé ou illicite de Données à caractère personnel et contre toute perte, destruction ou détérioration accidentelle.

a) La Sécurité de l'information est gérée selon les politiques et procédures dans le domaine de la Sécurité de l'information.

b) Chaque Société du Groupe est également responsable de l'ensemble des traitements effectués par les Responsables du traitement des données pour le compte de ces Sociétés du Groupe. Les Sociétés du Groupe s'acquittent de cette responsabilité en procédant à une vérification diligente détaillée des éventuels Responsables du traitement des données et en incluant des conditions particulières de protection des données dans les contrats conclus avec ceux-ci en conformité avec les exigences des actes normatifs relatifs à la protection des données, notamment, avec l'article 28 du Règlement général sur la protection des données.

c) Les Collaborateurs qui souhaitent engager un Responsable du traitement des données pour effectuer un traitement pour le compte d'une Société du Groupe doivent procéder à une vérification diligente détaillée des normes de traitement des données auprès d'un Responsable du traitement des données et prendre contact avec le directeur juridique local et au Délégué à la protection de données dans cette région pour s'assurer de la mise en place de clauses contractuelles adéquates de protection des données et assurer le respect des actes normatifs relatifs à la protection des données par chaque Responsable du traitement des données moyennant l'analyse des risques, les audits et les contrôles.

4.3. Chaque Région devra désigner un haut responsable qui agira en tant que Délégué à la protection des données et qui sera chargé des tâches suivantes :

4.3.1. responsabilité de la mise en œuvre locale et du respect de la Politique et des lois et règlements applicables en matière de protection des données ;

4.3.2. responsabilité de l'établissement des procédures visant à assurer la conformité à la Politique et aux lois et règlements applicables en matière de protection des données ;

4.3.3. responsabilité de l'interaction avec les autorités publiques compétentes dans le domaine de la protection des données ;

4.3.4. détermination, en concertation avec les responsables des divisions opérationnelles impliquées dans le Traitement, des finalités et des modalités de traitement des données à caractère personnel par chaque Société du Groupe et contrôle du la conformité de ces finalités et de ces modalités à la législation locale ;

4.3.5. réponse aux questions et préoccupations des Collaborateurs des Sociétés du Groupe concernant la mise en œuvre et le respect de la Politique et des lois et réglementations applicables en matière de protection des données ;

4.3.6. collecte des questions ou des plaintes des Personnes concernées relatives à la protection ou à la sécurité des données et fonction de la première personne à contacter pour les demandes des Personnes concernées liées avec la réalisation de leurs droits légaux.

4.4. En cas d'abscence de délégation au niveau régional, les fonctions de la personne à contacter sont remplies par le Délégué à la protection des données en chef de la région ou la personne qu'il a nommée.

4.5. Les responsables des divisions opérationnelles, avec l'aide de leurs Délégués à la protection des données, doivent mettre en œuvre des mesures nécessaires de protection des données qui sont aussi protectrices, ou plus protectrices, que celles définies dans la présente Politique, et qui assurent le

respect par ses Collaborateurs de la Politique et des lois locales applicables en matière de protection des données.

4.6. Les Collaborateurs doivent informer immédiatement le Délégué à la protection des données de tout cas de fuite de données avérée ou présumée. Dans le cas contraire, des mesures disciplinaires allant jusqu'au congédiement et à la résiliation du contrat seront prises.

4.7. Le Délégué à la protection des données informe immédiatement le conseiller juridique en chef local ou le Directeur général des Affaires juridiques du Groupe, le Responsable de la Conformité du Groupe, le Responsable du Département des risques du Groupe et le Responsable du Département de la Sécurité informatique du Groupe de tout risque lié à la protection des données, de tout problème potentiel de conformité et de toute Atteinte à la confidentialité des Données personnelles.

4.8. Le Délégué à la protection des données indépendamment de l'avis du conseiller juridique en chef local ou du Directeur général des Affaires juridiques du Groupe, du Responsable de la Conformité du Groupe, du Responsable du Département des risques du Groupe et du Responsable du Département de la Sécurité informatique du Groupe et des membres du Conseil et autres collaborateurs des Sociétés du Groupe prend la décision définitive d'informer les autorités compétentes en matière de protection des données de toute Atteinte à la confidentialité des Données personnelles dans les 72 heures après la détection de cette atteinte en conformité avec les règles de la Politique.

4.9. Le Délégué à la protection des données doit recenser les cas de toute Atteinte à la confidentialité des Données personnelles, y compris les actions entreprises afin de limiter les risques portés par une Société du Groupe, les contacts avec les autorités compétentes en matière de protection des données et les motifs pour lesquels l'information sur l' Atteinte à la confidentialité des Données personnelles n'a pas été transmise aux autorités compétentes en matière de protection des données.

4.10. Chanque Société du Groupe dans l'UE remplissant les fonctions du Responsable du contrôle des données et du Traitement des Données doit avertir le Délégué à la protection des données de toutes les opérations de Traitement des Données à caractère personnel en conformité avec les lois applicables. En cas de besoin, le Délégué à la protection des données charge les collaborateurs de l'Évaluation de l'impact sur la protection des données, si ceux-ci établissent qu'une telle ou telle opération de Traitement compte tenu de son caractère, envergure, contexte ou finalités de tratement, selon toute probabilité, porte atteinte aux droits et libertés des Personnes concernées.

5. Règles

Finalités du Traitement des Données à caractère personnel :

5.1. Les Sociétés du Groupe ne peuvent traiter les Données à caractère personnel qu'aux fins suivantes :

Données personnelles relatives aux Ressources humaines

5.1.1. Le personnel des Ressources Humaines peut être amené à traiter les Données personnelles relatives aux Ressources humaines pour faire valoir les obligations contractuelles/prendre des mesures nécessaires à la conclusion des contracts, pour faire valoir les obligations légales ou les intérêts légitimes des Sociétés du Groupe (dans les cas établis pas le droit local du travail) aux fins de :

a) la gestion du personnel (local et transnational) et des équipes dans différentes juridictions ; permettre la rotation des postes au sein du groupe ;

b) la gestion administrative des Collaborateurs, y compris l'exécution du contrat de travail, le respect des lois et règlements sociaux, fiscaux et du travail applicables ; et

c) la gestion de l'administration générale des ressources humaines, y compris le recrutement, l'embauche, les salaires, les congés, la formation, les évaluations, l'analyse des effectifs, la planification des carrières et de la relève des cadres supérieurs ;

d) la collecte des informations permettant d'indentifier la personne, y compris le nom, l'adresse du domicile, la date de naissance, le sexe, les photographies prises sur le lieu du travail et le numéro de téléphone fixe ;

e) la collecte des numéros d'identité attribués par l'État, y compris le numéro de la carte d'identité aux fins de la rémunération du travail et de la gestion des systèmes informatiques ;

f) la collecte des informations relatives au statut migratoire, à l'autorisation de travail et au statut résidentiel ;

g) la collecte des contacts d'urgence et de certaines informations (limitées) sur la famille ;

h) la collecte des informations liées au travail, y compris l'exprérience de travail, l'identifiant du type de l'emploi, les certificats de travail, les informations sur les congés et les données contractuelles ;

i) la collecte des informations sur les diplômes et la formation et des informations sur le recrutement et l'efficacité du travail, y compris les objectifs, les évaluations, les commentaires, les retours reçus, l'expérience de travail, l'équipement de travail, le projet d'évolution professionnelle et le plan de succéssion, les savoir-faire et les compétences et autres qualifications liées au travail ;

j) la collecte des informations sur l'utilisation des actifs informatiques de ERG ;

k) la collecte des informations nécessaires à la gestion de la comformité et des risques, y comris les informations sur les sanctions, les résultats de la vérification des antécédents et les données relatives à la sécurité, et

l) la collecte des informations sur la rémunération et les cotisations ou avantages, y compris les information sur le salaire et l'assurance, les informations fiscales, les références bancaires et les informations sur les indemnités et les avantages sociaux pour les employés.

5.1.2. Le manager d'un Collaborateur et la direction générale sont également autorisés à traiter en tant que de besoin des Données personnelles relatives aux Ressources humaines pour le compte dudit Collaborateur afin de faire valoir les obligations contractuelles ou légales ou les intérêts légitimes d'une Société du Groupe en ce qui concerne la gestion (locale et transnationale) du personnel et des équipes dans différentes juridictions, ainsi que la gestion, le recrutement, l'embauche, l'évaluation du personnel et la planification de la relève des cadres supérieurs.

5.1.3. Le personnel comptable peut traiter les Données personnelles relatives aux Ressources humaines pour faire valoir des obligations légales ou des intérêts légitimes des Sociétés du Groupe en matière de gestion des comptes, des salaires, des avantages sociaux et des impôts et autres prélèvements, cotisations et indemnités.

5.1.4. Le comité de rémunération a le droit de traiter les Données personnelles relatives aux Ressources humaines pour faire valoir des obligations légales ou des intérêts légitimes des Sociétés du Groupe dans le but d'établir le montant de rémunération du Collaborateur.

Données personnelles des clients

5.1.5. Les Collaborateurs ne peuvent traiter les Données personnelles des clients qu'en appui de la gestion de la relation client afin de faire valoir des obligations contractuelles des Sociétés du Groupe, de garantir une approche commune vis-à-vis des clients et de gérer les contrats clients des Sociétés du Groupe (systèmes de gestion d'information sur les clients, CRM) afin de faire valoir des obligations légales ou des intérêts légitimes des Sociétés du Groupe.

Données personnelles des fournisseurs

5.1.6. Les Collaborateurs ne peuvent traiter les Données personnelles des fournisseurs qu'en appui de la gestion des fournisseurs afin de faire valoir des obligations contractuelles des Sociétés du Groupe, des obligations légales ou des intérêts légitimes des Sociétés du Groupe en ce qui concerne la satisfaction de ses besoins en ressources, d'assurer une approche commune vis-à-vis des fournisseurs et de gérer les contrats fournisseurs des Sociétés du Groupe.

Données personnelles des actionnaires

5.1.7. Les Secrétaires généraux de chacune des Sociétés du Groupe et les personnes nommées aux Services juridiques (désignés par le Directeur général des Affaires juridiques) ne peuvent traiter, stocker et utiliser les Données personnelles des actionnaires, de ses directeurs, du Conseil, des bénéficiaires du Groupe, des dirigeants et cadres dirigeants des Sociétés du Groupe que si une Société du Groupe en a besoin afin de réaliser les intérêts du Groupe, de faire valoir des obligations légales ou d'autres intérêts légitimes des Sociétés du Groupe.

5.1.8. Les Données personnelles des actionnaires des Sociétés du Groupe, du Conseil et de la Direction générale sont conservées par le Secrétaire général du Groupe dans un endroit sécurisé accessible uniquement par le Secrétariat général du Groupe et le représentant légal désigné par le Directeur général des Affaires juridiques, avec l'appui nécessaire de l'IT. Le Secrétaire général confirmera aux personnes nommées aux Services juridiques (désignés par le Directeur général des Affaires juridiques) tous les changements apportés à ces données à caractère personnel sur une base semestrielle ou plus tôt s'il est informé des changements apportés.

5.1.9. Les Données personnelles des Actionnaires et du Conseil de chacune des Sociétés du Groupe dans les Régions doivent être conservées par le Secrétaire général régional compétent ou par le conseiller juridique régional (ou son délégué) lorsqu'un Secrétaire général régional n'a pas été nommé. Ces données doivent être conservées dans un endroit sûr accessible uniquement par le Secrétariat général ou la Direction des Affaires juridiques (selon le cas), avec l'appui nécessaire de l'IT. Le Secrétaire général régional ou le conseiller juridique régional (ou son délégué) confirmera tous les changements apportés à ces données personnelles sur une base semestrielle ou plus tôt si le Secrétaire général est informé des changements apportés. Ces informations seront transmises au Secrétaire général du Groupe dans un délai de 6 mois, après confirmation de toute modification des Données à caractère personnel.

5.1.10. Toute demande d'information concernant le Bénéficiaire économique ultime (« Ultimate Beneficial Ownership » - UBO) ou toute autre demande de « Know Your Customer » (« KYC ») adressée aux Actionnaires de la Société et à l'administration de chacune des Sociétés du Groupe, aux bénéficiaires du Groupe et aux administrateurs, dirigeants et cadres supérieurs des Sociétés du Groupe reçue par le Groupe doit être transmise au Secrétaire général du Groupe.

5.1.11. Si le Secrétaire général le juge nécessaire aux intérêts du Groupe, il répond dans les délais prescrits en utilisant l'information détenue conformément au paragraphe 5.1.6 fournie tous les six mois, ou plus tôt si le Secrétaire général est informé des changements apportés ou s'il s'adresse aux Personnes concernées.

5.1.12. Le Secrétaire général informe les actionnaires et le Conseil d'administration de l'utilisation des données sur une base semestrielle.

5.1.13. Tout collaborateur du Groupe auquel le Secrétaire général estime nécessaire de prêter assistance dans le traitement, le stockage et la gestion des Données personnelles des actionnaires et du Conseil d'administration de chacune des Sociétés du Groupe, des bénéficiaires du Groupe et des administrateurs, dirigeants et cadres supérieurs des Sociétés du Groupe reconnaît avoir été informé de la présente Politique et s' y conformer. Les listes des personnes qui sont autorisées à manipuler ces Données personnelles seront conservées par le Secrétaire général. Les listes de personnes qui sont dressées par les Secrétaires généraux régionaux ou les conseillers juridiques régionaux (selon le cas) pour traiter, stocker et gérer les Données personnelles relatives aux Sociétés du Groupe gérées par la

Région sont tenues à jour par les Secrétaires généraux régionaux ou les conseillers juridiques régionaux (selon le cas). Les Collaborateurs qui manipulent ces Données à caractère personnel ou qui considèrent devoir traiter ces Données à caractère personnel doivent obtenir l'accord de leur Responsable hiérarchique pour le faire et en informer le Secrétaire général du Groupe ou le Directeur des Affaires juridiques, ainsi que le Responsable de l'entité ou de la Région (selon le cas). Ces listes doivent être transmises au Secrétaire général du Groupe sur une base semestrielle.

5.1.14. Le Président-Directeur général et le Directeur financier du Groupe sont tous les deux autorisés à élaborer et à approuver les procédures, directives, délégations et modèles internes nécessaires pour assurer la mise en œuvre des clauses 5.1.6 – 5.1.13 inclusivement.

Données personnelles sensibles

Le personnel des Ressources Humaines et le personnel médical de la Société (le cas échéant) sont les seuls autorisés à traiter les Données personnelles sensibles afin de respecter l'obligation légale des Sociétés du Groupe de répondre aux demandes des gouvernements et d'assurer la santé et la sécurité au travail des collaborateurs de la Société. Avant le traitement des Données personnelles sensibles le Délégué à la protection des données régional doit effectuer une vérification nécessaire à établir si ce traitement affectera les droits et les libertés de la Personne concernée.

5.1.15. Seules les Données personnelles sensibles suivantes peuvent être traitées par les Sociétés du Groupe :

a) appartenance religieuse aux fins du prélèvement de l'impôt à la source[3] ;

b) dossiers médicaux[4].

5.1.16. Le personnel des Ressources humaines assurera ce traitement conformément aux exigences réglementaires applicables.

5.1.17. Les dossiers médicaux ne peuvent être traités que par des professionnels de la santé agréés conformément aux exigences légales.

5.1.18. Les Données personnelles sensibles ne sont accessibles aux Collaborateurs que si c'est autorisé par le droit du travail local et strictement en conformité avec le principe de nécessité de service. Seules les Sociétés du Groupe qui doivent traiter ce type de données conformément aux exigences légales locales applicables peuvent avoir accès aux Données personnelles sensibles.

Données personnelles liées à l'informatique

5.1.19. Chaque Société du Groupe peut traiter des Données à caractère personnel dans le cadre de l'utilisation du système informatique au quotidien qui permet aux Collaborateurs et à des tiers d'échanger des e-mails, d'accéder au site Internet, de stocker des fichiers/données et d'utiliser des applications logicielles et de créer, d'utiliser et de stocker les messages de diagnostique et les fichiers journaux si cela est nécessaire ou autorisé par les lois applicables.

5.1.19. Si les lois et règlements locaux requièrent une autorisation (par exemple, par une autorité locale de protection des données ou une autre autorité locale) pour le traitement des Données à caractère personnel mentionnées au point 5.1.19 ci-dessus (par exemple pour la surveillance informatique des Collaborateurs), la Société du Groupe doit obtenir cette autorisation et/ou ce consentement en temps utile.

[3] *En relation par exemple avec la Suisse*

[4] *Applicable aux divisions opérationnelles qui fournissent des services médicaux de leurs spécialistes ou qui effectuent ou recueillent des résultats de tests médicaux (p. ex., dépistage d'alcool ou de drogues, etc.).*

5.1.20. Lors du traitement des Données personnelles liées à l'informatique, les Sociétés du Groupe doivent respecter les normes applicables en matière de respect de la vie privée, telles que le secret de la correspondance ou des communications électroniques privées.

Autres données personnelles

5.1.21. Les Collaborateurs peuvent également traiter les données à caractère personnel conformément aux politiques et procédures de Sécurité de l'information et à la Politique d'utilisation acceptable. L'objet et la portée de ce traitement sont décrits plus en détail dans ces politiques.

Transparence, notification et droits des Personnes concernées

5.2. La plupart des Données à caractère personnel reçues par les Sociétés du Groupe sont fournies directement par la Personne concernée. Lors de la collecte de données à caractère personnel, chaque Personne concernée, si la loi locale l'exige, doit être informée de ce qui suit[5] :

5.2.1. la raison sociale de la Société du Groupe (ou des Sociétés du Groupe) est (sont) en train de collecter les informations en tant que Responsable du contrôle des données ;

5.2.2.2. les noms et les coordonnées des Délégués à la protection des données régional ou du Représentant externe que la Personne concernée peut contacter avec les demandes liées à ses Données à caractère personnel ;

5.2.3. l'objet (les objets) de ce Traitement et son (leur) fondement juridique ;

5.2.4. les intérêts légitimes réalisés (le cas échéant) ;

5.2.5. Le Groupe ou les tiers (désignés séparément ou ensemble avec des noms communs tels que « les Sociétés du Groupe » ou « les autorités locales ») qui recevront les Données à caractère personnel pour les traiter ultérieurement à leurs fins indépendantes (afin d'éviter toute ambiguïté par la présente il est expliqué que la divulgation des informations sur les Responsables du traitement des données n'est pas obligatoire) ;

5.2.6. Si le Responsable du traitement des données est une personne de l'UE ou de Suisse et, le cas échéant, que le Responsable du traitement des données a l'intention de transférer les Données à caractère personnel au destinataire hors de l'Union Européen/de l'EEE, et :

- si ce tiers assurera un niveau suffisant de sécurité des Données à caractère personnel en conformité avec les normes de l'UE (c'est-à-dire s'il y a la décision de la Commission européenne sur la sécurité suffisante), et (dans la négative),

- la référence aux mesures de sécurité appropriées ou pertinentes, approuvées par un Délégué à la protection des données afin d'assurer la sécurité du transfert, le moyen d'obtenir leurs copies ou le lieu de leur délivrance; et

- le nom et les coordonnées du Délégué à la protection des données régional ou du Représentant externe que la Personne concernée peut contacter avec les demandes liées à ses Données à caractère personnel ;

5.2.7. le délai de conservation des Données à caractère personnel ou, si c'est impossible, les critères utilisés pour établir ce délai ;

5.2.8. Si le Responsable du traitement des données est une personne de l'UE ou de Suisse, il doit respecter les droits légaux de la Personne condernée ; par exemple, en Union européenne, il s'agit des droits de :

- demander l'accès à ses Données personnelles, de les rectifier et de les supprimer ;

[5] *Ces renseignements peuvent faire partie d'un modèle de contrat ou de demande d'emploi, etc.*

- exiger l'imposition des limites de Traitement des données de la Personne concernée (sous certaines conditions) ;

- s'opposer à tout moment au Traintement (sous certaines conditions). Les Personnes concernées ont le droit de s'opposer à tout moment, pour des raisons impérieuses et légitimes liées à sa situation particulière, au traitement de ses Données à caractère personnel, sauf si la loi l'exige. Ils ont le droit de s'opposer gratuitement au traitement de leurs Données à caractère personnel à des fins de marketing direct ;

- transférer les Données à caractère personnel sur d'autres plateformes, et

- porter plainte auprès les autorités compétentes en matière de protection des données.

5.2.9. Si les Données à caractère personnel sont collectées auprès d'un tiers, les Sociétés du Groupe doivent informer la Personne concernée de la nature des Données personnelles, de leur source et, les cas échéant, de l'obtention des données des sources publiques dans un délai raisonnable qui ne doit pas néanmoins excéder un mois après l'obtention des Données à caractère personnel.

Toutefois, l'obligation d'informer la Personne concernée dans un tel cas peut ne pas s'appliquer si celle-ci a déjà reçu cette information.

5.2.10. Les demandes des Personnes concernées relatives à leurs droits devraient être adressées au Délégué à la protection des données régional. La réponse devrait être envoyée aux Personnes concernées dans le délai d'un mois. Toutefois, si la demande s'avère être compliquée ou que les Sociétés du Groupe reçoivent un grand nombre de demandes, ce délai peut être prolongé de deux mois.

Décisions automatisées[6]

5.3. Aucune évaluation ou décision concernant une Personne concernée qui l'affecterait de manière significative ne sera basée uniquement sur un traitement automatisé/électronique des Données à caractère personnel, à l'exception des cas où :

5.3.1. cette décision soit prise dans le cadre de la conclusion ou de l'exécution d'un contrat, pour autant que la demande introduite par la Personne concernée ait été satisfaite ou qu'il existe des mesures appropriées pour sauvegarder les intérêts légitimes de la Personne concernée, telles que des dispositions permettant à la Personne concernée de faire valoir son point de vue ; ou

5.3.2. la décision ne soit autorisée par la loi qui précise également les mesures de sauvegarde des intérêts légitimes d'une Personne concernée.

Les Personnes concernées ont le droit d'exiger la participation d'une personne à tout tratement de données automatisé.

Conservation des données

5.4. Les Collaborateurs doivent conserver les Données à caractère personnel, électroniques et papier, conformément aux Politiques des Sociétés du Groupe concernées, et, le cas échéant, d'après le calendrier des délais de conservation des données, approuvé par le Président-Directeur général du Groupe figurant en Annexe A. Le Président-Directeur général est habilité par le Conseil à approuver et à apporter des changements dans le calendrier des délais de conservation des données proposés par le conseiller juridique en chef, toutefois en concertation avec le Délégué à la protection des données.

Sécurité et confidentialité

[6] *Parmi les exemples de décisions automatisées, mentionnons l'examen automatisé des soumissions initiales ou l'examen automatisé des questionnaires destinés aux candidats à l'emploi.*

5.5. Des mesures techniques et organisationnelles appropriées pour protéger les Données à caractère personnel de la destruction accidentelle ou illicite ou la perte accidentelle, l'altération, la divulgation ou l'accès non autorisés devraient être mises en œuvre et maintenues par chaque Société du Groupe conformément aux politiques et procédures de Sécurité de l'information.

5.6. En cas de destruction accidentelle ou illicite, de perte accidentelle, d'altération, de divulgation ou d'accès non autorisé à des Données à caractère personnel, les Sociétés du Groupe se conforment aux procédures établies par les lois applicables, par les politique et les procédures de la Société du Groupe en matière de protection des données et aux instructions des autorités compétentes en matière de protection des données. Si le Responsable du traitement des données est une Société du Groupe de l'UE :

- elle doit informer immédiatement le Responsable du contrôle des données de la fuite des Données personnelles lorsqu'elle est découverte, et

- si le Délégué à la protection des données le juge nécessaire, il doit avertir l'autorité locale compétente de la fuite des Données personnelles sans retard excessif et dans le délai de 72 heures si possible. Cet avertissement doit inclure toutes les informations exigées par les lois locales relatives à la protection des données. De surcoît, si, selon toute probabilité, la fuite des Données personnelles engendrera un risque élevé à l'égard des droits et des libertés de la Personne concernée, le Responsable du contrôle des données doit informer les Peronnes concernées de la fuite des Données personnelles sans retard excessif hors des dérogations légales documentées.

Partage des Données à caractère personnel au sein des Sociétés du Groupe

5.7. ERG est une société internationale et devra occasionnellement échanger des Données à caractère personnel entre ses filiales et sociétés affiliées.

5.8. Les Données personnelles ne seront divulguées à d'autres Sociétés du Groupe que conformément à la présente Politique. Lorsqu'elles sont traitées par toutes les Sociétés du Groupe, la protection des Données à caractère personnel est garantie par le respect des mesures de sécurité organisationnelles et techniques strictes communes définies dans les politiques et procédures de Sécurité de l'information et dans la présente Politique.

5.9. Des clauses contractuelles types devraient être utilisées pour permettre un éventuel transfert de données à caractère personnel entre les Sociétés du Groupe.

Partage des Données à caractère personnel avec les Responsables du traitement des données

Partage de Données à caractère personnel par les Sociétés du Groupe situées dans l'UE avec des sous-traitants de traitement de données situés dans l'UE ou dans des pays assimilés

5.10. Si une Société du Groupe basée dans l'UE souhaite partager des Données à caractère personnel avec un Responsable du traitement de données basé dans l'UE, l'EEE ou dans un pays reconnu par la Commission européenne comme assurant un niveau de protection adéquat[7], les conditions suivantes doivent être remplies avant le transfert des données :

5.10.1. il doit exister un contrat écrit entre la Société du Groupe et le Responsable du traitement des données ; et

[7] La Commission européenne a jusqu' à présent reconnu Andorre, l'Argentine, l'Australie, le Canada (organisations commerciales), la Suisse, les Îles Féroé, Guernesey, Israël, l'île de Man, Jersey, la Nouvelle-Zélande, l'Uruguay (voir *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm* pour des informations actualisées).

5.10.2. ce contract doit être rédigé d'après le modèle l'Autorisation d'utilisation des données personnelles (ou comporter des clauses équivalentes), approuvée par le Groupe et étant à la disposition du Délégué à la protection des données en Europe.

Partage de Données à caractère personnel par les Sociétés du Groupe situées dans l'UE avec des sous-traitants de traitement de données situés en dehors de l'UE ou dans des pays assimilés

5.11. Si une Société du Groupe basée dans l'UE souhaite partager des Données à caractère personnel avec un Responsable du traitement des données situé en dehors de l'UE, de l'EEE ou dans un pays qui n'est pas reconnu par la Commission européenne comme assurant un niveau de protection adéquat, le Collaborateur responsable doit s'assurer de ce qui suit :

5.11.1. ce traitement des données est effectué en conformité avec les clauses de l'Accord intérieur du Groupe ;

5.11.2. en l'absence d'un tel Accord intérieur du Groupe, les Sociétés du Groupe doivent conclure un contract écrit rédigé d'après le modèle l'Autorisation d'utilisation des données personnelles (ou comporter des clauses équivalentes), approuvée par le Groupe et étant à la disposition du Service juridique du Groupe ;

5.11.3. tous les transferts de Données à caractère personnel doivent être sécurisés et réalisés dans le respect de la législation applicable relative aux transferts internationaux de données ;

5.11.4. les Sociétés du Groupe concernées qui exportent les Données à caractère personnel doivent (i) avoir conclu un ensemble de Clauses contractuelles standard sous une forme approuvée par la Commission européenne avec le Responsable du traitement des données préalablement au transfert des Données à caractère personnel ; et (ii) effectuer les formalités ou dépôts potentiels requis par sa législation locale.

Partage des Données à caractère personnel par les Sociétés du Groupe situées en dehors de l'UE

5.12. Si une Société du Groupe établie en dehors de l'UE souhaite partager des Données à caractère personnel avec un Responsable du traitement des données situé en dehors de son pays d'origine, un avocat général local doit s'assurer que le transfert est effectué dans le plein respect des lois et réglementations locales régissant la protection des données et les transferts internationaux des données à caractère personnel.

Données à caractère personnel des Collaborateurs qui quittent une Société du Groupe

5.13. Lorsqu'un Collaborateur quitte une Société du Groupe, celle-ci doit procéder comme suit :

5.13.1. donner à chaque Collaborateur sortant la possibilité de faire des copies de ses Données à caractère personnel privées stockées dans ses boîtes aux lettres électroniques, ordinateurs d'entreprise et appareils informatiques mobiles.

5.13.2. désactiver l'adresse électronique du Collaborateur dès que raisonnablement possible après son départ.

Programme de formation

5.14. Tous les Collaborateurs qui ont un accès permanent et (ou) régulier aux Données à caractère personnel suivront une formation sur la collecte et le traitement des Données à caractère personnel ou sur le développement des outils utilisés pour traiter les Données à caractère personnel de façon périodique.

5.15. Tous les autres Collaborateurs recevront une formation sur la présente Politique au moment de leur adhésion à l'entreprise et au besoin par la suite.

6. Réponse aux questions, préoccupations et demandes de renseignements

6.1 Si un Collaborateur a des questions ou des préoccupations concernant la protection des données, il doit contacter son Délégué à la protection des données.

6.2 Si une Personne concernée estime que ses données ne sont pas traitées conformément à la présente Politique, elle doit faire part de ses préoccupations au Délégué à la protection des données concerné.

6.3 Si un Collaborateur reçoit une plainte d'une Personne concernée en dehors du groupe, cette plainte doit être transmise sans délai au Délégué à la protection des données concerné.

6.4 Le Délégué à la protection des données doit examiner la plainte de façon confidentielle. Si le Délégué à la protection des données n'est pas disponible, le conseiller juridique en chef local examinera et enverra la plainte au Délégué à la protection des données dès qu'il sera disponible.

6.5 Les Sociétés du Groupe doivent avertir le Délégué à la protection des données de la région et ouvrir sans délai une enquête sur toute allégation de violation de la présente Politique.

6.6 Les Collaborateurs sont tenus de collaborer aux enquêtes internes liées à d'éventuelles violations de la Politique.

6.7 Afin de permettre au Groupe d'enquêter correctement sur une préoccupation, les allégations de non-conformité ou de violation de la présente Politique devraient inclure suffisamment d'informations concernant l'incident ou la violation.

6.8 Le Groupe traitera de façon confidentielle l'identité de toute personne qui dépose une plainte. Toutefois, dans certaines circonstances, le groupe peut être tenu par la loi de divulguer les informations ou l'identité de la personne qui dépose la plainte ou l'allégation.

6.9 Chaque plainte et toute information relative à une plainte sera conservée sous forme écrite et/ou électronique par le Délégué à la protection des données local concerné jusqu' à ce que la plainte ait été résolue, ou tel que requis par la loi et autrement conformément aux politiques d'une Société du Groupe.

7. Responsabilités

7.1. Le Conseil d'administration est responsable de l'établissement de la présente Politique.

7.2. Le service Conformité de la Région concernée est responsable de :

7.2.1. Fournir des conseils et des avis à la Direction régionale en ce qui a trait à la mise en œuvre de la présente Politique et la supervision de la mise en œuvre de la présente politique.

7.2.2. La surveillance du respect de la présente Politique

7.2.3. Obligation de faire rapport : L'établissement de rapports périodiques sur l'état d'avancement de la mise en œuvre et le respect de la Politique.

7.3. La Direction régionale est responsable de la mise en œuvre efficace de la présente Politique dans ses domaines de responsabilité respectifs et veille à ce que des contrôles adéquats soient mis en œuvre pour en assurer à tout moment la conformité.

7.4. La Direction régionale est chargée de désigner un Délégué à la protection des données et d'approuver et de faire appliquer les politiques et procédures élaborées par le Délégué à la protection des données de chaque Région.

7.5. Il incombe aux Délégués à la protection des données d'établir les responsabilités, les procédures, la formation et les contrôles internes appropriés dans leurs Régions respectives afin d'assurer la mise en œuvre uniforme de la présente politique et le respect de ses exigences.

7.6. Il incombe à la Direction régionale de s'assurer que leurs Collaborateurs et Responsables du traitement des données respectifs utilisés sont mis au courant de la présente Politique et que les Collaborateurs qui traitent des données à caractère personnel ou qui y ont accès reçoivent une formation périodique sur les exigences en matière de protection des données.

8. Surveillance

8.1. Le Directeur des Affaires juridiques et le Délégué à la protection des données devraient, sur une base annuelle, rendre compte au Comité de conformité du Conseil de l'état de conformité à la présente Politique. Les Départements de conformité régionaux devraient rendre des comptes annuels au Directeur des Affaires juridiques aur l'état d'avancement de la mise en conformité avec cette Politique.

8.2. L'Audit interne devra examiner périodiquement le respect de cette Politique et signaler tout manquement et formuler les recommandations adéquates pour la Direction du Groupe et le Comité de conformité du Conseil d'administration.

9. Non-conformité

9.1. Toute non-conformité à la Politique doit être documentée et signalée au Délégué à la protection des données, au Département de conformité ou via la ligne d'assistance téléphonique d'ERG.

9.2. Il incombe à chaque Collaborateur de se conformer aux modalités de la présente Politique. Les collaborateurs qui enfreignent la présente Politique feront l'objet de mesures disciplinaires assujetties à la loi locale, pouvant aller jusqu'à la résiliation de leur contrat de travail.

10. Processus de révision

10.1. La présente Politique d'ERG sera mise à jour périodiquement (mais pas moins d'une fois tous les deux ans) pour tenir compte de tout changement dans l'environnement juridique et technologique ainsi que dans les exigences opérationnelles.

10.2. Toutes les demandes de modification doivent être adressées à l'un des Titulaires de la Politique ou à l'un des Délégué à la protection des données.

10.3. Les modifications importantes apportées à la présente Politique d'ERG doivent être approuvées par le Conseil d'administration ou (dans le cas de l'Annexe A) par le Président-Directeur général.

10.4. La version 4.0 de la présente Politique de ERG entre en vigueur le 25 mai 2018.

version	Date de dernière révision	Approuvé par	Date d'approbation	Commentaires
1.0	24.08.2014	Le Conseil	24.08.2014	
1.0	5.05.2015	Conformité	5.05.2015	
2.0	04.03.2016	Le Conseil	13.03.2016	
3.0	20.08.2017	Le Conseil	27.08.2017	
4.0	02.06.2018	Le Conseil	02.06.2018	