Directives générales Groupe pour l'adoption d'une Politique de protection des données personnelles

Novembre 2019

Le respect de la vie privée et de la protection des données personnelles constitue une préoccupation essentielle, mais aussi un vecteur de confiance, pour le Groupe Veolia qui a décidé d'adopter des directives générales s'imposant à toutes les entités qui le composent en vue de fixer des règles communes de protection des données personnelles.

Les entités qui ne satisfont pas les critères matériels ou géographiques d'application du RGPD devront appliquer les Normes Groupe Minimales telles qu'énoncées dans "le RGDP pour les entités du Groupe localisées hors de l'UE" ("Entités du Groupe hors RGPD") annexées à ces Directives générales.

1. Champs d'application

Chacune des Entités du Groupe concernée par le RGPD doit se doter d'une politique de protection des données personnelles.

La Politique de protection des données de Veolia Environnement SA constitue un standard commun à toutes les entités du Groupe concernées par le RGPD ; ce standard s'impose à chacune de ces entités dès qu'elles en reçoivent communication sauf pour celles des entités qui seraient amenées à adopter une version modifiée sous réserve que de telles modifications :

- sont requises pour tenir compte :
  - des lois locales, notamment celles relatives aux relations sociales ou à la protection des données à caractère personnel, ainsi que
  - des décisions impératives de l'autorité de régulation compétente chargée, dans le pays de l'entité, de veiller à la protection des données personnelles contenues dans les fichiers ou traitements, aussi bien publics que privés,
  - des spécificités de l'activité de l'entité concernée,
- aient été validées, préalablement à leur adoption, par le Directeur de la conformité du groupe ou par la ou les personnes qu'il aura mandatée(s) à cet effet.

2. Règles d'or ("Golden rules")

Chaque Entité du Groupe concernée par le RGPD devra intégrer à sa Politique de protection des données personnelles au moins ces six règles d'or pour que chaque personne amenée à collecter et traiter des données personnelles pour son compte :

- respecte le RGPD en s'assurant que les données personnelles sont collectées, utilisées et partagées dans le respect des droits des personnes concernées et du concept de "*privacy by design*" pour la protection des données dès la conception du traitement ;

- soit transparente et claire avec les personnes concernées sur les finalités du traitement envisagé, sur la finalité et les modalités de sa mise en oeuvre ainsi que sur les destinataires avec lesquels ces données seront éventuellement partagées ; recherche le consentement des personnes physiques concernées chaque fois que possible et n'agisse sans leur consentement que dans les cas prévus

par le RGPD ou la loi ou lorsque leur consultation préalable est impossible ou présente un risque particulier ;

- recherche un avis en cas de doute sur la façon de traiter les données personnelles, échange avec d'autres spécialistes, demande un avis juridique ou recueille l'avis de l'autorité de régulation compétente et conserve une trace de ses décisions ;
- prenne la décision de collecter, d'utiliser ou de partager des données personnelles en tenant compte de l'intérêt de la personne physique pour ne traiter que les données nécessaires, pertinentes, adéquates, proportionnées, justes, opportunes et sécurisées, pour une durée limitée aux besoins du traitement ;
- s'assure que les données personnelles ne sont partagées qu'avec ceux auxquels l'accès est nécessaire pour rendre le service attendu et atteindre l'objectif du traitement ;
- s'assure que les mesures de sécurité proportionnelles aux risques ont été prises en vue de préserver la disponibilité, la confidentialité et l'intégrité des traitements.

3. Délégué à la Protection des Données ("Data Protection Officer" ou DPO)

Chaque zone du Groupe Veolia désigne un Correspondant à la Protection des Données de zone ("Zone Personal Data Correspondant" ou Zone PDC), y compris dans les pays dans lesquels Veolia est présent mais où le RGPD n'a pas vocation à s'appliquer : le Zone DPC devient l'interlocuteur du Groupe pour la zone sur tous les sujets liés aux données personnelles et veille au respect des présentes directives pour sa zone.

En France, un DPO est désigné pour chaque Business Unit (BU).

Le Zone PDC ou les DPO de BU disposent de la faculté de s'adjoindre un ou plusieurs DPOs (ou correspondants) locaux si l'organisation de la zone ou de la BU ou la loi applicable l'impose ; il peut également s'attacher des collaborateurs ou "Data Protection Managers" (DPM) pour l'assister dans sa mission.

Le Zone DPC agira comme DPO des entités de sa zone ou comme DPM local à défaut avoir procédé à leur désignation.

Tout Zone PDC agit de manière indépendante ; il rapporte sur ces sujets au Responsable de la conformité (Local CCO) de la zone à laquelle il appartient ou, à défaut, aux plus hauts niveaux de la hiérarchie de la zone.

4. Données des Clients

Lorsque l'activité d'une entité l'amène à collecter les données personnelles de clients, personnes physiques, qu'il s'agisse de clients directs ou de bénéficiaires d'un service public, cette entité devra préciser dans sa Politique de protection des données personnelles les précautions particulières qu'elle met en œuvre à leur bénéfice.

5. Sécurité

L'entité doit prendre des mesures, y compris avec ses sous-traitants, pour assurer que la sécurité des données personnelles traitées est adaptée à la sensibilité des données et des risques liés au traitement.

A cet effet, les entités devront se conformer à la politique adoptée par la Direction de la sûreté Groupe "PO-TSE 11 *Veolia GDPR Security policy* " qui constitue une annexe à la Data Privacy Policy, telle que ponctuellement amendée.

Addendum aux Directives générales pour une Politique Groupe de Protection des Données Personnelles
- Applicable aux Entités du Groupe hors RGPD -

Chaque Entité du Groupe hors RGPD doit se doter d'une politique de protection des données personnelles prenant en compte les "Golden Rules" et basée, dans la mesure du possible, sur les standards communs aux Entités du Groupe concernées par le RGPD, posés par la Politique de Protection des données de VE SA, en complément des lois qui leur sont applicables. Les Entités du Groupe hors RGPD devront en particulier, sous réserve des lois et règlements locaux plus contraignants (***voir résumé dans le tableau joint***) :

- mettre en oeuvre un Registre des traitements relatifs à la gestion de :
  - i) leurs employés (traitements et salaires, gestion de carrière, protection de la santé, dotation d'équipements et outils professionnels),
  - ii) la relation contractuelle avec leurs clients (services et biens fournis, données de facturation),
  - iii) la relation contractuelle avec les fournisseurs (gestion des contrats, données de facturation),

- identifier dans le registre la liste des données collectées et leurs destinataires; s'interdire de partager les données personnelles lorsque cela n'est pas imposé par la loi ou rendu nécessaire pour satisfaire les objectifs du traitement ; dans la mesure du possible, adapter leurs contrats pour sécuriser les données partagées,

- limiter les données collectées à ce qui est strictement nécessaire pour satisfaire la finalité du traitement et supprimer toute donnée non pertinente ; s'abstenir de conserver des donnée pour une durée indéterminée; s'abstenir de traiter des données sensibles lorsque cela n'est pas impératif,

- informer les personnes physiques concernées que la collecte sera minimisée à ce qui est nécessaire à la finalité du traitement et que des mesures de sécurité seront prises conformément aux normes de la Direction de la sûreté Groupe. Une telle information peut se faire par le site internet ou de toute autre manière que l'Entité du Groupe hors RGPD juge appropriée et conforme aux lois locales,

- dans la mesure du possible, rendre l'information accessible qu'une personne a été désignée à laquelle toute personne physique concernée par une collecte de données pourra s'adresser en cas de question sur ledit traitement.

	Entités Groupe concernées par RGPD	**Entités groupe hors RGPD**
Désigner un DPO	X	*optionnel* *(au min un DPC ou un DPM)*
Adopter une politique de protection des données conforme à celle de VESA	X	
Adopter une politique de protection des données		X
Mettre en œuvre un registre des traitements de l'entité	X	X
Mettre en œuvre un outil d'AIPD	X	
Réaliser les AIPD lorsque des données sensibles sont collectées	X	
Dans le Registre : ● être transparent sur les finalités	*détail de toutes les finalités*	*finalité principale*
● minimiser les données personnelles collectées	X	X
● lister les données personnelles collectées	*toutes*	*catégories*
● définir une durée de conservation adéquate	*durée strictement limitée*	*durée raisonnable*
● identifier les destinataires	*tous (directs & indirects)*	*les principaux*
● décrire le flux des données	X	
● documenter tous les transferts de données entre des entités UE/hors UE	*toujours*	*quand un risque est identifié*
Rechercher, s'il y a lieu, le consentement de la personne physique avant de collecter ses données	*chaque fois* *(sauf les cas de l'art. 6.1 RGPD)*	*si faisable ou approprié*
Informer la personne physique concernée de la mise en oeuvre du traitement	X	X
Informer la personne physique concernée de ses droits	*fournir toutes informations sur les droits (accès, suppression, portabilité…)*	
Adopter des mesures de sécurité pour protéger les données personnelles	*fournir la preuve de l'art. 32 du RGPD & se conformer aux politiques Groupe de sécurité*	*Mettre en oeuvre les politiques Groupe de sécurité*
Revoir les contrats	*insérer les clauses appropriées et les annexes requises par le RGPD dans*	*pour les nouveaux contrats insérer les clauses de protection des*

	les contrats (nouveaux ou en cours)	*données personnelles et prévenir leur utilisation inappropriée*