Veolia Environnement SA

Politique de protection des données personnelles

Novembre 2019

1. PRÉAMBULE

Veolia Environnement SA (VESA) prend des engagements forts en faveur de la protection des données personnelles qu'elle entend inscrire au cœur de ses préoccupations.

La présente Politique de protection des données personnelles vise à informer toute personne physique concernée (employés ou candidats, clients, fournisseurs ou partenaires et leurs employés) des mesures ainsi mises en œuvre lorsque VESA collecte des données personnelles dans l'exercice de ses activités.
Elle est susceptible d'évoluer selon les besoins, en raison du contexte légal, en France ou au sein de l'Union européenne, ainsi que des recommandations ou décisions de la CNIL.

Cette politique ne s'applique que pour Veolia Environnement SA ; les entités du groupe Veolia sont par ailleurs tenues d'adopter leur propre politique de protection des données personnelles.

2. DONNÉES COLLECTÉES, FINALITÉS DES TRAITEMENTS ET RÔLE DU DPO

VESA a mis en place dans l'entreprise une organisation responsable de la bonne application et du respect de la présente Politique, sous le contrôle du Directeur groupe de la conformité ("Group CCO").

De plus, VESA prend des mesures pour sensibiliser ses employés à la nécessité de protéger les données personnelles pour qu'une collecte ou un traitement ne s'opère que s'il est nécessaire au regard des finalités envisagées et si ces finalités sont définies de manière à garantir leur caractère licite, déterminé, explicite et légitime.

Les traitements mis en oeuvre par VESA et contenant des données personnelles font l'objet d'une fiche de description complète, intégrée dans le "Registre des traitements" tenu par le Délégué à la Protection des Données de VESA (ou Data Protection Officer - DPO).

Le DPO de VESA veille ainsi à la conformité de la collecte des données personnelles et de leur traitement avec :

- le 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 et à la libre circulation de ces données (RGPD) et
- la loi du loi n° 78-17 du 6 janvier 1978 (French Data Protection Act) relative à l'informatique, aux fichiers et aux libertés modifiée (Loi I&L).

En plaçant le DPO de VESA sous l'autorité du Group CCO, VESA a ainsi voulu garantir son indépendance et placer la protection des données personnelles au centre de la structure organisationnelle de l'entreprise.

3. RÈGLES D'OR

VESA se fonde sur six règles d'or pour que chaque personne amenée à collecter et traiter pour son compte des données personnelles :

- 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.

4. INFORMATION DES PERSONNES PHYSIQUES CONCERNÉES

Conformément au RGPD, VESA s'attache à informer les personnes physiques concernées des droits qui leur sont garantis en les avisant :

- de l'identité du responsable du traitement ;
- de la finalité poursuivie par le traitement ;
- du caractère obligatoire ou facultatif des réponses et des conséquences éventuelles d'un défaut de réponse ;
- des destinataires des données ;
- de leur droit d'accès, de modification et de rectification aux informations qui les concerne, de leur droit d'opposition pour des motifs légitimes, de leur droit de s'opposer à ce que leurs données personnelles soient utilisées à des fins de prospection commerciale ainsi que de leur droit de définir des instructions quant au traitement de leurs données personnelles après leur mort ;
- de la durée de conservation des catégories de données traitées.

5. TRAITEMENTS GROUPE

VESA informe les personnes physiques concernées que les données personnelles objet des traitements recensés dans son registre sont susceptibles d'être rendues accessibles à l'audit interne, à la direction de la conformité ou au DPO, aux commissaires aux comptes, aux personnes en charge du traitement des signalements de comportements violant les règles d'éthique du groupe ainsi qu'à ses avocats ou aux autorités compétentes et, dans certains cas, aux parties prenantes à un projet de fusion ou d'acquisition.

6. DESTINATAIRES DES DONNÉES

VESA est susceptible de partager les données personnelles collectées avec des personnes du groupe Veolia ou avec ses prestataires de services ou avec ses fournisseurs, uniquement dans la limite nécessaire à l'accomplissement des tâches qui leur sont confiées.

VESA veille à ce que ses prestataires et partenaires agissent en conformité avec les lois et règlements applicables en matière de protection de données personnelles mais également à ce qu'ils accordent une attention particulière à la confidentialité de ces données.

7. CONSERVATION DES DONNÉES

Les traitements de données personnelles collectées par VESA ou pour son compte sont conservés par VESA ou par ses prestataires, notamment sur des plateformes de stockage cloud.

Pour des raisons principalement techniques ou liées à la dimension internationale de VESA, certaines données peuvent ainsi être conservées ou accédées en dehors de l'Union européenne ou de l'Espace Economique Européen (EEE). Dans ce cas, VESA veille à l'instauration de mesures permettant d'assurer un niveau de protection des données personnelles compatible avec les exigences du RGPD, notamment par des mesures physiques, techniques, organisationnelles et procédurales rigoureuses et adaptées pour assurer la disponibilité, la confidentialité et l'intégrité des données personnelles en les modulant selon la nature et la sensibilité des données concernées.

VESA s'attache à limiter la durée de conservation des données personnelles pour le temps nécessaire aux opérations pour lesquelles leur collecte et leur traitement est intervenu, dans le respect de la réglementation applicable. Les données personnelles sont ensuite irréversiblement supprimées ou anonymisées.

8. SÉCURITÉ ET ALERTES

VESA prend des mesures pour assurer que la sécurité des données personnelles qu'elle traite est adaptée selon la sensibilité de ces données et des risques qui y sont attachés. A cet effet, les équipes informatiques concernées ou leurs sous-traitants mettent en oeuvre les exigences de la politique de cybersécurité Veolia et notamment celles relatives à :

- l'identification des risques cyber,
- la mise en oeuvre de protections réseaux adaptées, via des dispositifs de filtrage,
- le maintien en condition de sécurité des différents composants de l'infrastructure et des applications, notamment l'application des mises à jour de sécurité et la mise à niveau des composants pour éviter l'usage de composants hors maintenance,
- le durcissement des composants d'infrastructure tels que les serveurs ou les postes de travail,

- la vérification régulière des vulnérabilités de l'infrastructure ou des applications via une veille et l'utilisation de scanner de vulnérabilité technique ou applicative,
- le cryptage des données au repos quand cela est nécessaire et en transit,
- l'usage des bonnes pratiques de sécurité lors du développement des applications notamment pour les applications de type web, l'utilisation du référentiel OWASP,
- l'attribution des droits des utilisateurs respectant la règle du moindre privilège et le droit d'en connaître,
- la protection des accès par la mise en oeuvre de mécanismes d'authentification forte, par l'utilisation du SSO (*Single Sign On*) basé sur le référentiel d'identité digitale du groupe Veolia et par la revue régulière des comptes,
- la supervision de la sécurité des données personnelles et des applications y accédant notamment via une centralisation et une utilisation des logs,
- la conservation des éléments prouvant la mise en oeuvre des mesures ci-dessus.

En cas d'atteinte aux données personnelles qu'elle détient, Veolia s'impose de réagir sans délai dès qu'elle a connaissance de l'événement pour, d'une part et si nécessaire, informer la CNIL et s'il y a lieu, les personnes concernées et, d'autre part, identifier les défaillances et mettre en place des mesures de sécurité adaptées.

9. DROITS DES PERSONNES PHYSIQUES

Les personnes physiques dont les données personnelles sont collectées disposent, dans les limites de la loi, d'un droit d'accès, de modification, s'il y a lieu de portabilité ainsi que d'un droit à l'oubli portant sur les données personnelles qui les concernent et un droit à la limitation du traitement.
Elles disposent également du droit de faire parvenir au responsable de traitement des directives concernant le sort de leurs données après leur décès.

Pour exercer ces droits, chaque personne concernée par un traitement contenant des données à caractère personnel peut s'adresser par écrit à la personne en charge du traitement au sein de VESA dont l'identité a été portée à sa connaissance lors de la collecte puis au DPO en envoyant un email à l'adresse dpo.vesa@veolia.com.

10. CONTACT

Pour toutes demandes d'information concernant notre politique de protection des données, vous pouvez adresser un courrier au DPO de VESA (dpo.vesa@veolia.com) ou vous adresser au Group CCO.

D'une manière générale, vous pouvez toujours vous adresser à la CNIL (https://www.cnil.fr ou à l'adresse 3, Place de Fontenoy, 75007 Paris).