

Politique de
protection
des données
personnelles
Périmètre Europe

sommaire

| | |
|---|---|
| 1. Objectifs | 3 |
| 2. Champ d'application | 3 |
| 2.1 Entités, collaborateurs et sous-traitants soumis à la Politique..... | 3 |
| 2.2 Données personnelles et traitements concernés par la Politique | 3 |
| 3. Pilotage & Gouvernance | 4 |
| 3.1 Au niveau du Groupe | 4 |
| 3.1.1 Gouvernance Groupe | 4 |
| 3.1.2 Délégué Groupe à la protection des données (DPO Groupe) | 4 |
| 3.2 Au niveau des BU..... | 4 |
| 4. Principes de protection énoncés par le RGPD | 5 |
| 4.1 Principe de responsabilité (<i>Accountability</i>) | 5 |
| 4.2 Finalités déterminées, explicites et légitimes..... | 5 |
| 4.3 Pertinence, proportionnalité et minimisation des données personnelles collectées | 5 |
| 4.4 Licéité du traitement de données personnelles..... | 5 |
| 4.5 Transparence et droit à l'information | 6 |
| 4.6 Droit d'accès, de rectification, de limitation, d'effacement et d'opposition | 6 |
| 4.7 Classification, niveau de confidentialité et sécurité des données personnelles | 6 |
| 4.8 Intégration de la protection des données personnelles dans la gestion des projets | 6 |
| 4.9 Analyse d'impact relative à la protection des données personnelles | 6 |
| 4.10 Relations avec les sous-traitants..... | 7 |
| 4.11 Transferts des données personnelles en dehors de l'UE..... | 7 |
| 4.12 Durée de conservation limitée | 7 |
| 5. Mise en œuvre opérationnelle | 7 |
| 5.1 Sensibilisation et formation | 7 |
| 5.2 Mise à disposition de procédures et livrables | 7 |
| 5.3 Traçabilité des événements de sécurité | 8 |
| 5.4 Gestion des incidents de sécurité et des violations de données personnelles..... | 8 |
| 5.5 Examen de conformité, contrôles, audits et sanctions | 8 |

Le respect des droits fondamentaux et des règles de protection des données personnelles fait partie intégrante des valeurs éthiques du Groupe.

Le Règlement Général sur la Protection des Données (« **RGPD** »)¹ applicable dans l'ensemble des Etats membres le 25 mai 2018, renforce les droits des personnes physiques sur leurs données personnelles grâce à un régime harmonisé des principes de protection au sein de l'Union européenne.

Le RGPD prévoit un nouveau principe de « responsabilité » (*Accountability*) des acteurs du secteur privé et du secteur public, à charge pour ces derniers de démontrer qu'ils ont mis en œuvre les mesures appropriées, afin de garantir le respect des règles de protection.

Ces nouvelles exigences se matérialisent notamment par la désignation d'un délégué à la protection des données (« **DPO** »), la tenue d'un registre afin de documenter la conformité des traitements de données personnelles et la mise en œuvre de mesures de sécurité renforcées.

Ne pas respecter ces règles peut conduire à de lourdes sanctions pécuniaires² et à dégrader l'image de SUEZ.

Face à ces nouveaux enjeux, le Groupe a décidé de se doter d'une politique (la « **Politique** ») destinée à garantir la protection des données personnelles des collaborateurs, des clients et des fournisseurs, dans le respect de sa Charte éthique.

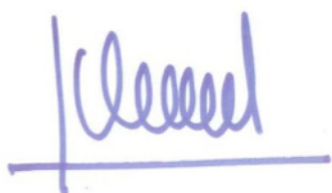
La protection des données personnelles constitue un atout au service de notre transformation digitale et contribue à pérenniser la confiance de nos collaborateurs, de nos clients et de nos partenaires.

Il s'agit d'un enjeu significatif pour l'exercice durable de nos activités.

Le DPO Groupe, rattaché à la Direction juridique, est en charge de faire appliquer cette Politique au nom du Secrétaire Général.

Je demande donc à l'ensemble des collaborateurs de se mobiliser pour garantir sa bonne application.

Jean-Louis CHAUSSADE
Directeur Général

A handwritten signature in blue ink, appearing to read 'JL CHAUSSADE', is written over a horizontal blue line.

¹ Règlement (UE) n°2016/679 du Parlement européen et du Conseil du 27/04/2016 relatif à la protection des personnes physiques à l'égard du traitement de leurs données personnelles et à la libre circulation de ces données, abrogeant la Directive 95/46/CE, publié le 04/05/2016 au Journal Officiel de l'Union.

² Sanctions financières pouvant s'élever jusqu'à 4 % du chiffre d'affaires annuel mondial du Groupe relatif à l'exercice précédent ou à 20 millions d'Euros, le montant le plus élevé étant retenu.

1. Objectifs

La présente Politique, validée par le Comité de Direction, définit les règles de protection que SUEZ et les entités du Groupe doivent mettre en œuvre pour traiter les données personnelles³ en Europe.

La Politique comprend l'ensemble des principes qui visent à garantir la mise en œuvre de traitements de données personnelles licites, loyaux et transparents. Elle établit des règles de gouvernance qui précisent les rôles et responsabilités des acteurs de la protection des données personnelles.

Il est demandé à chaque collaborateur, ainsi qu'à toute personne ou entité extérieure au Groupe qui réalise des traitements⁴ de données personnelles d'adopter un comportement conforme aux principes définis ci-après.

Pour toute demande relative à l'exercice des droits d'accès et de rectification, pour toute question ou réclamation en lien avec le traitement de leurs données personnelles, les collaborateurs doivent consulter leur DPO local, soit par courrier, soit par e-mail, à l'adresse dédiée indiquée sur l'intranet de leur BU.

Pour toute question relative aux modalités d'application de la Politique ou toute autre question, le DPO Groupe peut être contacté à l'adresse suivante : privacy@suez.com

2. Champ d'application

2.1 - Entités, collaborateurs et sous-traitants soumis à la Politique

La présente Politique s'applique aux entités juridiques exerçant leurs activités sur le territoire de l'Union européenne (« UE »), que le traitement de données personnelles soit réalisé ou non dans l'UE.

La présente Politique s'applique à tous les collaborateurs, même occasionnels et à tous les sous-traitants⁵ (*data processors*), au sens du RGPD, qui traitent des données personnelles.

Dès lors qu'une réglementation nationale requiert des standards de protection des données personnelles plus élevés que ceux prévus par le RGPD, cette réglementation nationale prime sur la Politique.

Les entités juridiques du Groupe qui sont soumises à des réglementations nationales spécifiques adoptent, si nécessaire, des documents d'application complémentaires, dans le respect de la présente Politique.

2.2 - Données personnelles et traitements concernés par la Politique

La Politique vise les données personnelles présentes sur tout support papier ou dématérialisé, qui sont hébergées ou traitées notamment :

- sur tout support informatique : serveur dans un data center ou dans le cloud, un poste de travail ou un smartphone ;
- via des applicatifs, bases de données ou entrepôts de données ;
- via des portails exposés sur internet ou sur l'intranet ;
- via des objets communicants ou smart grids ainsi que les projets de digitalisation.

La Politique s'applique à tous les traitements qui portent sur les données personnelles des collaborateurs, clients, fournisseurs ou partenaires collectées, utilisées ou transférées par les entités du Groupe.

³ « Donnée personnelle » désigne toute information relative à une personne physique identifiée ou identifiable, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

⁴ « Traitement de données personnelles » désigne toute opération appliquée à des données personnelles, telle que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, la diffusion ou toute autre forme de mise à disposition, le rapprochement, l'interconnexion, la limitation, l'effacement ou la destruction.

⁵ « Sous-traitant » désigne toute personne, physique ou morale, qui traite les données personnelles pour le compte d'une entité du Groupe.

3. Pilotage & Gouvernance

Chaque collaborateur doit se conformer à la présente Politique.

Les représentants légaux des entités juridiques du Groupe s'assurent de la diffusion de la Politique au sein de leur périmètre et de leurs équipes. Ils sont garants de sa mise en œuvre, avec l'assistance du DPO Groupe et de son réseau de DPO locaux.

Le DPO Groupe met en place une gouvernance visant à décliner les mesures organisationnelles prévues par le RGPD et à permettre un déploiement efficace de la Politique. Cette gouvernance est précisée dans un guide spécifique sur la gouvernance des données personnelles (la « **Gouvernance** »).

3.1 - Au niveau du Groupe

3.1.1 - Gouvernance Groupe

La mise en œuvre et le respect de la Politique sont supervisés par le Comité de Protection des Données (« **CPD** »), où siègent le DPO Groupe et le Chief Information Security Officer du Groupe (« **CISO** », rattaché à la Direction des Systèmes d'Information) et qui est placé sous l'autorité du Secrétaire Général du Groupe.

Chaque année, le CPD établit le bilan de ses activités, qui est présenté par le Secrétaire Général au Comité Ethique et Développement Durable du Conseil d'administration de SUEZ, ainsi que la proposition de plan d'actions pour l'année à venir. Les attributions et les modalités de fonctionnement du CPD sont précisées dans la Gouvernance.

3.1.2 - Délégué Groupe à la protection des données (DPO Groupe)

Le DPO Groupe rapporte hiérarchiquement au Directeur Juridique Groupe, au sein du Secrétariat Général. Les principales missions du DPO Groupe sont celles prévues par l'article 39 du RGPD et sont précisées dans la Gouvernance.

Au titre de ses principales missions, le DPO Groupe conçoit et supervise l'application de la présente Politique et coordonne le réseau des DPO locaux.

3.2 - Au niveau des BU

Selon le RGPD, chaque entité juridique est responsable des traitements de données personnelles qu'elle met en œuvre. Il revient donc aux représentants légaux de ces entités de s'assurer de la bonne application de la Politique par les collaborateurs, dans le respect du RGPD.

Des DPO locaux sont désignés sous la responsabilité des représentants légaux des entités et sont fonctionnellement rattachés au DPO Groupe.

Les DPO locaux définissent et contrôlent la conformité au RGPD et à la Politique, dans leur périmètre.

Les DPO locaux ou, à défaut, les représentants légaux apportent aide et conseils aux collaborateurs qui les interrogent ou qui leur font part de leurs préoccupations en matière de protection des données personnelles et veillent à ce que les collaborateurs adoptent des pratiques conformes à la Politique, au RGPD et aux réglementations nationales applicables.

4. Principes de protection énoncés par le RGPD

4.1 - Principe de responsabilité (*Accountability*)

En vertu du principe de responsabilité prévu par le RGPD, chaque entité doit :

- être en mesure de documenter à tout moment la manière dont elle assure la protection des données personnelles ;
- mettre en œuvre les mesures techniques et organisationnelles appropriées afin de pouvoir démontrer que chaque traitement de données personnelles est conforme au RGPD et à la législation nationale applicable.

En pratique, ce principe est mis en œuvre au travers des mesures suivantes :

- désignation d'un DPO, lorsque cette désignation est rendue obligatoire en vertu du RGPD ou de la réglementation nationale applicable ;
- tenue d'un registre interne des traitements de données personnelles reprenant la cartographie des traitements effectués par les entités ;
- analyses d'impact relatives à la protection des données personnelles, dans les cas obligatoires prévus par le RGPD ;
- protection des données personnelles dès la conception de tout nouveau projet concerné ;
- mise en œuvre par les entités de procédures appropriées, en cas de risques générés par les traitements de données personnelles liés à leurs activités.

4.2 - Finalités déterminées, explicites et légitimes

Les données personnelles doivent être traitées de manière licite, loyale et transparente. Elles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec les finalités d'origine.

Chaque entité doit porter une attention particulière au traitement des catégories particulières de données personnelles (données sensibles) qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques ou biométriques, les données concernant la santé, la vie ou l'orientation sexuelle d'une personne.

Chaque entité ne pourra traiter ce type de données personnelles qu'avec le consentement explicite de la personne concernée ou dans les cas expressément autorisés par les législations nationales et le RGPD.

4.3 - Pertinence, proportionnalité et minimisation des données personnelles collectées

Les données personnelles traitées par les entités doivent être exactes, pertinentes et limitées aux finalités pour lesquelles elles sont collectées.

4.4 - Licéité du traitement de données personnelles

Chaque entité demeure garante de la licéité des traitements de données personnelles qu'elle réalise.

Un traitement de données personnelles licite, au sens du RGPD, doit répondre à l'un des fondements suivants :

- respect d'une obligation légale à laquelle l'entité est soumise ;
- exécution d'un contrat auquel la personne concernée est partie ;
- intérêts légitimes poursuivis par l'entité, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée ;
- consentement exprès de la personne concernée pour une ou plusieurs finalités spécifiques, dans les cas prévus par le RGPD.

4.5 - Transparence et droit à l'information

Chaque entité doit veiller à informer les personnes concernées par les traitements de données personnelles, au moyen des mentions exigées par le RGPD, sur tout support permettant une communication concise, transparente, intelligible et aisément accessible.

Lorsque la collecte est effectuée directement auprès de la personne concernée, l'information doit intervenir au moment où les données personnelles sont obtenues.

Lorsque la collecte est effectuée de manière indirecte (ex : achat de fichiers), l'information des personnes doit être effectuée dans un délai raisonnable ne dépassant pas un mois à compter de la collecte et, dans tous les cas, au plus tard lors de la première communication avec la personne concernée ou avant toute communication à un tiers.

4.6 - Droit d'accès, de rectification, de limitation, d'effacement et d'opposition

Les personnes concernées par les traitements de données personnelles disposent d'un droit d'accès, de rectification, de limitation des données personnelles qui les concernent, d'un droit à l'effacement des données personnelles (droit à l'oubli), d'un droit d'opposition au traitement et d'un droit à la portabilité de leurs données personnelles, dans les conditions prévues par le RGPD.

Elles peuvent exercer ces droits à tout moment. Les modalités de réponse à l'exercice de ces droits sont précisées par les DPO locaux.

Chaque entité doit s'assurer que les personnes concernées par ses traitements de données personnelles sont effectivement en mesure d'exercer leurs droits.

4.7 - Classification, niveau de confidentialité et sécurité des Données personnelles

Les données personnelles sont classées conformément à la « Politique de classification de l'information et de protection de la confidentialité de SUEZ », qui est consultable sur l'intranet de SUEZ (Rubrique Politiques et procédures).

Les documents contenant des données personnelles courantes sont à classer au niveau « interne ».

Les documents contenant des catégories particulières de données personnelles (données sensibles), sont à classer au niveau « confidentiel ».

En outre, chaque entité doit prendre les mesures nécessaires en fonction de la nature des données personnelles, du contexte et des finalités du traitement de données personnelles, de façon à garantir un niveau de sécurité adapté aux risques identifiés.

Le niveau de sécurité doit permettre de garantir la confidentialité, l'intégrité et la disponibilité des données personnelles et de limiter tout risque de destruction, de perte, d'altération, de divulgation et d'accès non autorisé aux données personnelles.

Les données personnelles traitées doivent être protégées conformément aux Directives Sécurité et à la Gouvernance Sécurité des systèmes d'information, consultables sur l'intranet de SUEZ (Rubrique Politiques et procédures).

4.8 - Intégration de la protection des données personnelles dans la gestion des projets

La protection des données personnelles doit être intégrée dans la gestion des projets et, dès leur conception, pour les nouveaux services.

4.9 - Analyse d'impact relative à la protection des données personnelles

Chaque entité du Groupe, agissant comme responsable de traitement⁶, procède à une analyse d'impact relative à la protection des données personnelles avant la mise en œuvre de tout nouveau traitement de données personnelles, lorsque les critères prévus par le RGPD sont réunis, en particulier en cas de traitements à grande échelle de catégories particulières de données personnelles (données sensibles) ou de recours à de nouvelles technologies.

⁶ « Responsable de traitement » désigne la personne physique ou morale, le service ou l'organisme qui, seul ou conjointement avec d'autres, détermine la finalité ou les moyens du traitement.

4.10 - Relations avec les sous-traitants

Les entités du Groupe qui confient la collecte, l'utilisation ou le traitement de données personnelles à des sous-traitants, au sens du RGPD, demeurent responsables de la protection de ces données. Ces entités doivent veiller à ce que les sous-traitants offrent des garanties suffisantes au regard de la présente Politique et du RGPD. Tout contrat conclu avec chaque sous-traitant doit définir ses obligations, y compris les mesures de sécurité et de confidentialité, conformément aux exigences du RGPD.

4.11 - Transferts des données personnelles en dehors de l'UE

Les transferts de données personnelles en dehors de l'UE ne peuvent intervenir que dans les cas suivants :

- le pays de destination des données personnelles est considéré comme présentant un niveau de protection adéquat, selon les conditions fixées par la Commission européenne ;
- le destinataire des données personnelles peut justifier de garanties appropriées permettant l'exercice effectif des droits des personnes, au sens du RGPD ;
- dans les conditions dérogatoires prévues par le RGPD : consentement explicite de la personne concernée, caractère nécessaire du transfert pour l'exécution d'un contrat ou pour des motifs d'intérêt public, transfert nécessaire à la constatation, à l'exercice ou à la défense de droits en justice, ou à la sauvegarde des intérêts vitaux de la personne concernée.

4.12 - Durée de conservation limitée

Il incombe à chaque entité du Groupe de ne pas conserver les données personnelles traitées au-delà de la durée nécessaire au regard des finalités pour lesquelles ces données sont traitées, dans le respect de chaque la législation nationale applicable.

Lorsque les données personnelles ne sont plus nécessaires aux finalités légitimant leur traitement, elles doivent être effacées ou rendues anonymes.

5. Mise en œuvre opérationnelle

Le réseau des DPO, les Directions des Systèmes d'Information, les Responsables Sécurité des Systèmes d'Information et la filière Juridique assistent les entités dans la mise en œuvre de la Politique.

Les actions suivantes sont mises en œuvre afin d'atteindre ses objectifs :

5.1 - Sensibilisation et formation

Les DPO locaux ou, à défaut, les représentants légaux des entités, doivent s'assurer que leurs collaborateurs ont les connaissances suffisantes pour remplir leurs obligations au titre du RGPD et de la réglementation applicable, en fonction de leur degré d'implication dans les traitements de données personnelles.

Compte-tenu des enjeux associés à la protection des données personnelles, l'ensemble du personnel concerné participe aux actions de sensibilisation organisées par le DPO Groupe et par les DPO locaux.

5.2 - Mise à disposition de procédures et livrables

La Politique est déployée par l'intermédiaire de méthodologies, procédures, sensibilisations adaptées aux spécificités des réglementations nationales applicables.

Le Groupe publie régulièrement des guides thématiques destinés à diffuser les bonnes pratiques et à permettre la déclinaison opérationnelle des objectifs visés par le RGPD.

5.3 - Traçabilité des événements de sécurité

Conformément aux règles de sécurité du Groupe, une traçabilité automatisée des événements de sécurité est mise en place. Chaque entité peut décider des événements à tracer, en fonction du contexte, des supports (tels que postes de travail, équipements de réseau, serveurs), des risques et des exigences de chaque législation applicable.

5.4 - Gestion des incidents de sécurité et des violations de données personnelles

Chaque entité du Groupe met en place une procédure de remontée des incidents de sécurité et de gestion des violations de données personnelles, y compris pour la gestion de crise, en conformité avec le RGPD et les réglementations applicables.

Le DPO Groupe ou le DPO local, selon les cas, et le représentant légal de l'entité sont informés sans délai de toute violation de données personnelles, au sens du RGPD. Si la violation ainsi constatée est susceptible de porter sérieusement atteinte aux droits et libertés des personnes concernées, le DPO avise l'autorité de contrôle compétente (et, si nécessaire, les personnes concernées) dans les meilleurs délais (si possible, 72 heures après en avoir pris connaissance).

5.5 - Examen de conformité, contrôles, audits et sanctions

Les mesures techniques et organisationnelles de mise en conformité des traitements de données personnelles sont testées, analysées et évaluées, afin de vérifier leur efficacité.

Des contrôles internes de conformité au RGPD, aux réglementations locales et à la Politique sont réalisés régulièrement. Les sous-traitants doivent communiquer les informations nécessaires à la démonstration du respect des obligations légales.

La réalisation effective des contrôles internes peut, si nécessaire, faire l'objet de revues par la Direction de l'Audit Interne, avec l'appui éventuel de la DSI du Groupe.

Les résultats de ces contrôles peuvent être communiqués à l'entité concernée et au Comité Ethique et Développement durable. Ils peuvent être mis à disposition de l'autorité de contrôle compétente, conformément au RGPD.

Les mesures correctives adoptées en cas d'insuffisances constatées lors de l'examen de conformité sont documentées et mises à jour régulièrement.

Chaque entité juridique supporte directement les sanctions susceptibles de découler du non-respect du RGPD et des réglementations applicables, du fait de ses traitements de données personnelles.

prêts pour la révolution de la ressource  **suez**