PUBLIC

ROQUETTE
Offering the best of nature™

Privacy & Data Protection

COMMENT ASSURER LA PROTECTION DES DONNÉES PERSONNELLES AU QUOTIDIEN

Protection des Données et de la Vie rivée

Guide de Bonne Conduite

GROUPE ROQUETTE

Legal & Compliance

Défis clés de la conformité chez Roquette

Sous la responsabilité de la direction générale, le champ d'application de la conformité et sa gestion au sein de Roquette représentent un élément clé de la direction « Legal & Compliance » du Groupe, que l'on appelle « Compliance Office ».

Le Compliance Office demeure responsable du Code de Conduite de Roquette, de sa mise à jour et de sa mise en œuvre.

Il couvre également les trois principaux domaines suivants :

- Sécurité financière,
- Éthique professionnelle,
- Protection des Données et de la Vie Privée.

Par conséquent, un Programme de conformité a été élaboré et évolue afin d'assurer l'irréprochabilité juridique et financière de nos activités.

Quel est le rôle de la conformité ?

La conformité a pour rôle d'inculquer des **valeurs éthiques** et de mettre en place des mesures conformément aux **exigences légales**, aux **standards** et aux **bonnes pratiques**.

Notre Programme facilite la mise en place des procédures qui garantissent la conformité aux règles applicables à Roquette.

Nos quatre valeurs – **authenticité, excellence, innovation, bien-être** – constituent la clé de voûte sur laquelle reposent nos activités **au quotidien**.

Gardez à l'esprit qu'aujourd'hui, l'entreprise durable est éthique.
Et la société de demain sera transparente.

Pensez global
Agissez local

Édito

Les principes de la Protection des Données et de la Vie Privée font partie des standards exposés dans notre Code de Conduite.

Tous les collaborateurs, ainsi que les tiers avec lesquels Roquette travaille, ont un droit à la Vie Privée. C'est pourquoi Roquette s'engage à protéger leurs données personnelles.

Les données personnelles sont des informations qui permettent d'identifier, directement ou indirectement, une personne physique (nom, date de naissance, numéro de sécurité sociale, photo, adresse e-mail, ID d'ordinateur, etc.).

La Protection des Données Personnelles constitue un droit fondamental qui garantit le respect de la Vie Privée

La Protection des Données Personnelles permet à chaque individu de contrôler le recueil, le traitement, l'utilisation et la distribution de ses données.

Ces dernières doivent être utilisées de façon juste à des fins spécifiques, explicites et légitimes et doivent être conservées uniquement pendant la durée nécessaire aux finalités de traitement.

En Europe, le traitement des données personnelles est régi par le Règlement Général sur la Protection des Données (RGPD), entré en vigueur le 25 mai 2018.

Étant donné que les législations relatives à la Protection de la Vie Privée et aux données personnelles varient d'un pays à l'autre, et que notre entreprise est présente à l'international, Roquette a adopté une Politique Groupe concernant la protection des données personnelles. Cette Politique s'applique à tous les employés du Groupe dans le monde.

Ce Guide explique les bonnes conduites à tenir dans nos activités quotidiennes pour respecter les principes de la Protection des Données Personnelles et les exigences de notre Politique.

Jennifer GODIN, Data Protection Officer

Déléguée à la protection des données

Sommaire

Objet

Qu'est-ce que la Politique de Protection des Données et de la Vie Privée ?

Le Groupe Roquette a établi une Politique de Protection des Données Personnelles et de la Vie Privée (la « Politique ») afin d'aborder au mieux les questions relatives ce sujet, conformément à son image, à ses intérêts et aux lois et réglementations applicables en la matière.

Cette Politique définit les principes et les exigences relatifs à la protection des informations personnelles et expose les règles que tous les employés, responsables, directeurs et parties tierces agissant pour le compte de Roquette doivent respecter en matière de Protection des Données et de la Vie Privée.

Les principes et les règles de cette Politique relative à la Protection des Données Personnelles sont détaillés dans une plateforme documentaire à trois niveaux :

- Engagement de la direction : Code de conduite.
- Règles internes : Directives et Manuel sur la Protection des Données Personnelles dans Q-Docs.
- Documentation sur le Système de Management de la Protection des Données (SMPD) : procédures, directives, méthodologies, formations, etc.

Toute la documentation respecte les lois et règlementations relatives à la Protection des Données.

Qu'est-ce que le Guide de Bonne Conduite sur la Protection des Données et de la Vie Privée ?

Le Guide de Bonne Conduite sur la Protection des Données et de la Vie Privée (le « Guide ») nous aide à mettre en place et à respecter notre Politique relative à la Protection des Données et de la Vie Privée.

Il présente, de façon simplifiée, les règles et les bonnes pratiques qui respectent les directives et les exigences des lois et règlementations applicables à notre Groupe en terme de Protection des Données.

Il se divise en thématiques inspirées du Code de Conduite, dont la « Protection des Données et de la Vie Privée » compte parmi les sujets relatifs à la conformité.

Description

A qui s'applique le Guide de Bonne Conduite sur la Protection des Données et de la Vie Privée ?

La Politique et le Guide constituent une base commune à toutes les entités mondiales. Ils s'appliquent :

- À tous les employés, directeurs et responsables (« les Employés »)
- À toutes les parties tierces agissant pour le compte de Roquette, telles que :
  - Les sous-traitants, dont les consultants, les indépendants et le personnel intérimaire
  - Les stagiaires
  - Le personnel détaché d'une entité non rattachée à Roquette
  - Les travailleurs saisonniers
  - Les autres représentants
  - Et toutes les parties tierces employées ou payées par Roquette.

Où pouvons-nous trouver le Guide de Bonne Conduite sur la Protection des Données et de la Vie Privée ?

Tous les employés et parties tierces agissant pour le compte de Roquette doivent comprendre et respecter les principes de la Protection des Données et de la Vie Privée contenus dans notre documentation, et notamment dans le présent Guide.

Le Guide est à portée de main sur :

https://fr.roquette.com/protection-des-donnees.

Ce Guide, diffusé dans le cadre d'une communication dédiée, s'accompagne d'un kit et de formations en ligne sur les Principes de la Protection des Données et de la Vie Privée (définis par les standards internationaux et les exigences spécifiques du RGPD).

Cette formation est incluse dans le Programme d'intégration sur la Protection des Données.

Responsabilités

Qui est responsable de la mise en œuvre des principes opérationnels ?

La confidentialité des données concerne – et est de la responsabilité de - tous les salariés de notre entreprise.

Nous avons tous la responsabilité de respecter les principes opérationnels décrits dans la documentation sur le SMPD fournie par le Compliance Office et le Réseau de la Protection des Données. Ce Guide facilite cette mise en œuvre et améliore notre niveau de conformité.

Comment nous assurer que nous prenons la bonne décision ?

Le Guide est conçu pour nous aider à faire face à la plupart des situations dans notre vie professionnelle qui pourraient poser des problèmes liés à la vie privée. Cependant, il ne peut pas prévoir toutes les situations auxquelles nous pourrions faire face dans l'exercice de nos activités professionnelles. En cas de doute, à tout moment, quant à l'attitude à adopter, nous devons faire preuve de discernement et nous poser les questions suivantes :

- Est-ce conforme à la loi ?
- Cela donne-t-il une bonne image de moi et de la société ?
- En parlerais-je à un ami, à la famille ou à un collègue ?
- Serais-je à l'aise si cela était rendu public ?

Si la réponse à l'une de ces questions est « Non », nous ne devrions pas prendre cette décision. En cas de doute, nous devons nous adresser à la Data Protection Officer du Groupe ou à tout autre contact approprié (voir coordonnées de contact dans la section « Questions et inquiétudes »).

Que se passe-t-il si nous ne respectons pas les principes de la Protection des Données et de la Vie Privée ?

Le non-respect des principes peut avoir des effets négatifs sur la société. Les conséquences peuvent être très graves, autant pour la société que pour les personnes impliquées (sanctions disciplinaires, amende, peine d'emprisonnement, atteinte à la réputation, etc.).

Tout signal de violations des principes, avérées ou présumées, sera pris au sérieux. Nous examinerons cela immédiatement, de manière juste et en accord avec les exigences légales. En fonction de la nature de la violation de données, des sanctions disciplinaires peuvent être appliquées, conformément aux lois locales et aux réglementations de la société.

Tous les employés sont tenus de coopérer pleinement à toute vérification. Roquette assurera la confidentialité des personnes impliquées.

Questions et inquiétudes

Les employés, toute partie tierce agissant pour le compte de Roquette et toute autre partie prenante sont encouragés à signaler les situations préoccupantes, ce qui aidera Roquette à prévenir et réduire tout préjudice à la société.

Quels types de situations peuvent être signalés ?

Peuvent être signalées toute situation et toute violation, avérée ou présumée, des principes de la Protection des Données et de la Vie Privée, des réglementations de la société ou des lois applicables.

A qui faut-il s'adresser ?

En cas de violation de données, veuillez contacter le Délégué à la Protection des données de Roquette à dpo@Roquette.com. Et/ou reporter un incident via notre formulaire web « Privacy Alert ».

Si vous devez signaler une violation potentielle de la conformité, vous pouvez contacter votre point de contact habituel ou signaler un problème par l'intermédiaire du dispositif Speakup©. Toutes les alertes reçues par l'intermédiaire de ce dispositif sont traitées de manière confidentielle, dans le respect des lois et réglementations en vigueur.

SpeakUp®

Roquette ne tolère aucune forme de représailles à l'encontre d'un employé ou d'un tiers qui signale, en toute bonne foi, une violation potentielle ou réelle des principes de confidentialité et de protection des données ou des lois applicables.

Par conséquent, si l'émetteur d'une alerte professionnelle doit s'identifier, son identité doit être traitée de manière confidentielle par l'organisation, afin d'éviter tout risque de représailles, de discrimination ou de mesures disciplinaires à son encontre pour avoir dénoncé les faits.

Respect des lois et des réglementations

Chacun de nous, dans chaque entité du Groupe, est tenu de respecter les lois et les réglementations en vigueur sur la Protection des Données.

Dans le cas où les réglementations locales sont plus strictes que la Politique et le Guide, ces premières prévaudront.

Le cas échéant (absence de législation locale ou législation moins restrictive), nos bonnes pratiques internes prévaudront dans la mesure autorisée par la loi.

Nous considérons que :

- Nous devons adopter aussi vite que possible toutes les réglementations locales applicables.
- Chacun de nous doit savoir que toute violation de lois et réglementations peut être passible de sanctions civiles et/ou pénales, autant pour la personne impliquée que pour la société.
- La protection des personnes physiques en ce qui concerne le traitement des données personnelles constitue un droit fondamental.
- Les principes et les règles relatifs à la protection des personnes physiques concernant le traitement de leurs données personnelles doivent, indépendamment de leur nationalité ou lieu de résidence, respecter leurs libertés et droits fondamentaux, en particulier leur droit à la Protection des Données Personnelles.
- Le droit à la Protection des Données Personnelles n'est pas un droit absolu. Il doit être apprécié par rapport à sa fonction dans la société et pondéré au regard des autres droits fondamentaux, selon le principe de proportionnalité.

Quel pays dispose d'une législation spécifique ou d'une autorité de Protection des Données Personnelles ?

Consultez cette carte pour avoir une vision d'ensemble : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde.

Nos responsabilités :

- Nous devons, en toutes circonstances, respecter toutes les lois et réglementations applicables sur la Protection des Données dans les pays où nous opérons et toutes les règles en vigueur dans chaque lieu où se trouve la société.

- Dans le cadre de nos activités professionnelles, nous devons signaler tout comportement que nous considérons comme allant à l'encontre des lois et réglementations applicables sur la Protection des Données (par ex. : RGPD) à notre Data Protection Officer à dpo@Roquette.com et le dispositif confidentiel d'alerte Roquette : Speakup©.

- Nous devons mettre en place des mesures de Protection des Données Personnelles appropriées et proportionnelles au contexte tout en facilitant la conformité aux autres lois et réglementations. Inversement, nos actions visant à être en conformité aux lois et réglementations applicables au Groupe doivent respecter les règles et les bonnes pratiques pour la Protection des Données Personnelles (exemple : dans le cadre du programme de conformité en matière de lutte contre les pots-de-vin et la corruption, nous devons garantir la protection du lanceur d'alerte par des mesures de confidentialité et de protection de ses données personnelles).

Êtes-vous concerné(e) par le Reglement general sur la protection des donnees (RGPD) ?

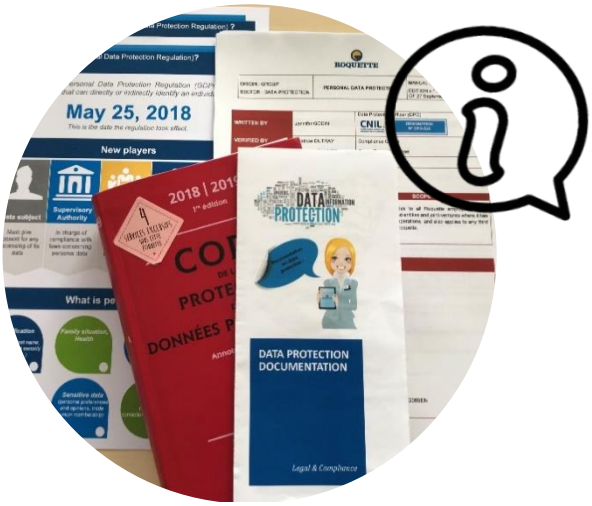
Vous entrez dans le cadre du RGPD en tant que **sous-traitant des données** (1) ou **responsable de traitement** (2) :

- si vous êtes établi(e) dans un pays de l'UE ;
- ou, le cas échéant, si vos « activités de traitement ont un lien avec
  - l'offre de biens ou de services à des personnes concernées au sein de l'UE ;
  - ou le suivi de leur comportement, dans la mesure où celui-ci a lieu au sein de l'UE ».

Texte officiel : Article 3 du RGPD au sujet du champ d'application territorial

(1) et (2) : Voir définitions à la page 38.

Principes de la Protection des Données



Les données personnelles doivent être :

- sécurisées.
- exactes et à jour.
- traitées loyalement et licitement.
- traitées à des fins limitées.
- adéquates, pertinentes et non excessives.
- conservées pendant une période limitée et déterminée.
- traitées conformément aux droits des personnes concernées.
- protégées par des mesures juridiques appropriées en cas de transfert vers d'autres pays.

Vos droits :

Conformément à la législation et aux réglementations applicables, vous avez le droit d'accéder à vos informations personnelles, de les rectifier et de vous opposer à leur traitement pour motif légitime. Vous disposez également du droit d'effacer vos données pour motif légitime, du droit à leur portabilité et de limiter leur traitement.

Pour exercer ces droits, veuillez compléter le formulaire disponible à l'adresse : Roquette.com/Protection des données.

Pour toute question, veuillez contacter la Data Protection Officer (dpo@Roquette.com).

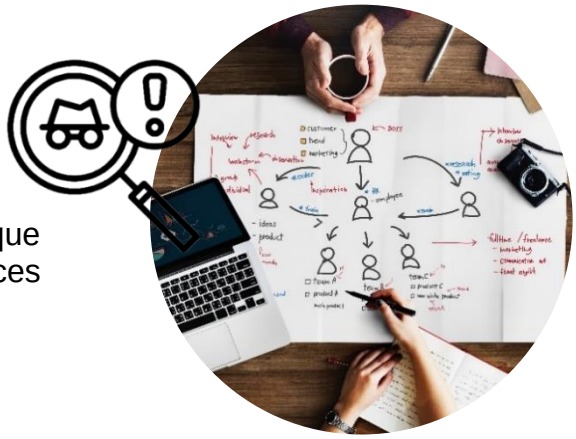
Nos responsabilités :

Nous devons :

- Respecter la législation locale et les règles de la Politique du Groupe concernant la Protection des Données Personnelles.
- Signaler tout nouveau traitement ou changement à la Data Protection Officer.
- Renoncer à utiliser, divulguer ou conserver des données à caractère personnel, sauf à des fins spécifiques, légitimes et nécessaires.
- Garantir que les personnes concernées ont bien été informées de la collecte de leurs données personnelles.
- Protéger ces données lors de leur collecte, de leur traitement, de leur utilisation, de leur divulgation, de leur stockage ou de leur transfert.
- Garantir la sécurité et la confidentialité des données traitées.
- Conserver des données uniquement pendant la durée nécessaire aux fins du traitement et respecter les lois applicables.
- Contacter la Data Protection Officer en cas d'incident de sécurité impliquant des données à caractère personnel.

Nos collaborateurs sont formés !

Risques sur la vie privée



Qu'est-ce qu'un risque sur la vie privée ?

Un risque correspond à un scénario hypothétique décrivant un événement redouté et toutes les menaces qui permettraient sa survenue.

Plus spécifiquement, il explique :

- comment les origines d'un risque (par ex. : un employé qui reçoit un pot-de-vin d'un concurrent)
- peuvent exploiter les vulnérabilités des actifs de support (par ex. : le système de gestion de fichiers qui permet la manipulation de données)
- dans le cadre de menaces (par ex. : mauvaise utilisation par envoi d'e-mails)
- et déclencher la survenue d'événements redoutés (par ex. : accès illégitime à des données personnelles)
- concernant les données personnelles (par ex. : fichier client),
- ce qui entraîne des répercussions sur la vie privée des personnes concernées (par ex. : sollicitations indésirables, sentiments d'intrusion dans la vie privée, problèmes d'ordre personnel ou professionnel).

Effet de l'incertitude sur la confidentialité

La gravité représente l'ampleur d'un risque. On l'estime principalement selon l'ampleur des répercussions potentielles (aux niveaux **physique**, **matériel** et **moral**) sur les personnes concernées, en tenant compte des contrôles existants, planifiés ou supplémentaires.

Exemple :

Le risque le plus important représenté par le système d'alerte professionnelle pour le lanceur d'alerte : le risque de représailles, de discrimination ou sanctions disciplinaires appliquées contre cette personne pour avoir dénoncé les faits.

Nous considérons que :

Les droits de chacun s'appliquent en totalité, indépendamment du niveau de risque dans le traitement.

Cependant, nous devrons moduler notre respect de la Protection des Données en fonction du niveau de risque que représentent nos opérations de traitement de données personnelles pour les libertés et droits fondamentaux des individus.

Le RGPD donne une plus forte impulsion à cette pratique. Par conséquent, les opérations de traitement qui génèrent des risques plus faibles pour les libertés et droits fondamentaux des individus entraînent généralement des obligations de conformité moins nombreuses, tandis que celles « à haut risque » exigeront des obligations de conformité supplémentaires, comme les Analyses d'impact relatives à la Protection des Données (AIPD) (1).

Nos responsabilités :

L'analyse des risques est fondamentale. Dans le cadre du RGPD, la prise en compte des risques sous-tend la responsabilité de l'entreprise et tous les traitements de données.

Nous devons procéder à des analyses de risques dans le cadre des AIPD pour les traitements à haut risque, ainsi qu'en rapport avec de nombreuses autres exigences du RGPD dont la sécurité des données, les notifications d'infraction de la sécurité et des données, la Protection des Données dès la conception, l'intérêt légitime, la limitation des finalités et le traitement loyal.

(1) : Voir définition à la page 58.

Risques en cas de non-conformité

Les personnes morales et physiques qui ne respectent pas la loi et la réglementation sur la Protection des Données (par ex. RGPD) s'exposent à des sanctions et des peines financières, sous forme de :

Sanctions pénales :

- Peine d'emprisonnement.
- Amende pour les entités légales.

Sanctions civiles :

- Dommages-intérêts civils.

Sanctions administratives :

- Notification formelle.
- Avertissement.
- Injonction.
- Limitation de traitement temporaire ou définitive.
- Retrait d'une certification ou injonction à retirer une certification.
- Suspension des transferts de données.
- Injonction à cesser le traitement ou retrait de l'autorisation de traitement.
- Publicité des sanctions imposées.
- Sanctions sans avis formel préalable (caractère urgent).
- En fonction du manquement, une amende administrative.

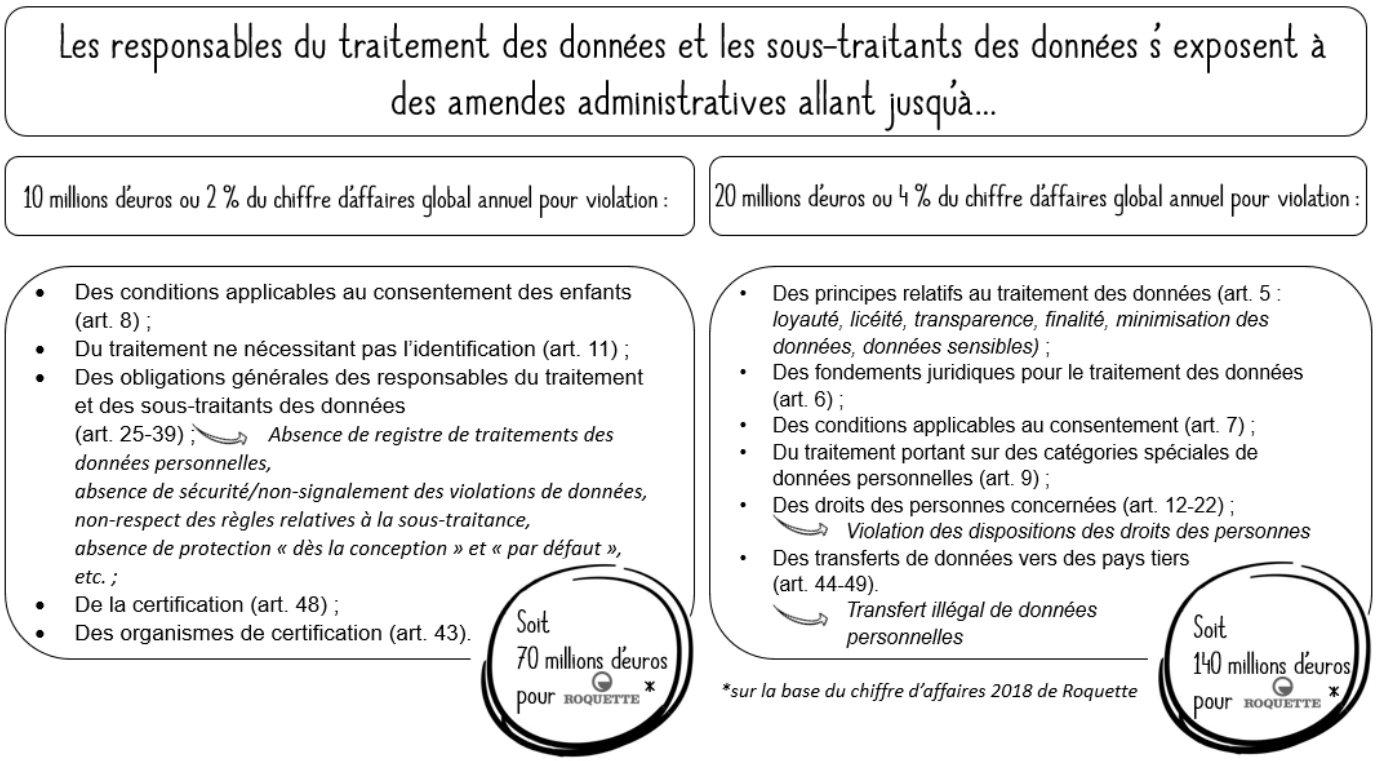
Peines financières conséquentes :

- Perte de revenus découlant de l'atteinte à leur réputation.

Quel est le plafond des amendes administratives prévu par le RGPD ?

Les amendes revêtent un caractère davantage facultatif qu'obligatoire. Elles s'appliquent au cas par cas et doivent être « efficaces, proportionnées et dissuasives ».

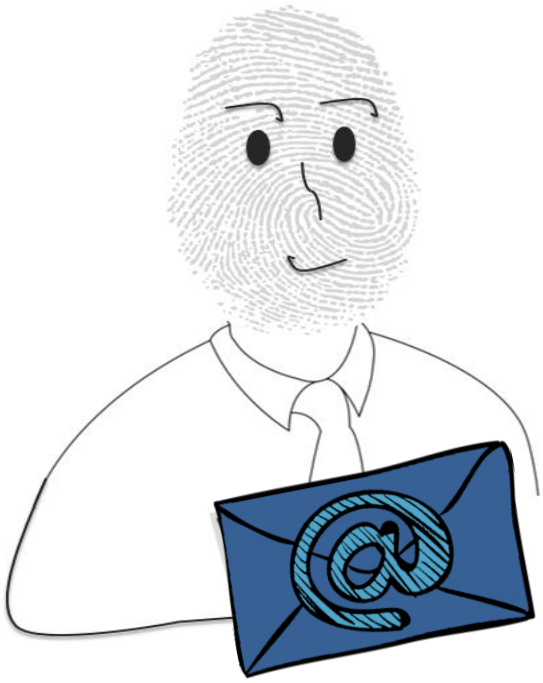
Leur montant repose sur les articles spécifiques de la réglementation que l'entreprise a violée.



Quelles peuvent être les sanctions pénales ?

Quelques exemples de la législation française :

- Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est passible de cinq ans d'emprisonnement et de 300 000 euros d'amende (Art. 226-18 du Code pénal).
- Afin de garantir un véritable droit et une véritable protection du lanceur d'alerte, la loi anti-corruption (Sapin II) punit sévèrement toute entrave à une alerte. La confidentialité entourant l'alerte est un élément essentiel de la réglementation. Ainsi, le fait de divulguer des éléments confidentiels de l'alerte (identité du lanceur d'alerte, de la personne mise en cause, informations fournies à l'appui du signalement), sauf à l'égard de l'autorité judiciaire, est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.



1 Nos standards quant à nos RELATIONS AVEC LES PERSONNES CONCERNÉES

Culture de la confidentialité

La **Protection des Données** est un ensemble de lois, de réglementations et de bonnes pratiques régissant le recueil et l'utilisation d'informations personnelles au sujet d'individus.

Les **données personnelles** désignent toute information liée à une personne physique identifiée ou identifiable.

Le terme « **Privacy** » renvoie au traitement des informations personnelles de manière confidentielle et respectueuse de la Vie Privée.

Qui est concerné ?

Le respect de la confidentialité et Protection des Données Personnelles concerne – et est de la responsabilité de - tous les salariés de notre entreprise.

Pourquoi est-ce important ?

Le mauvais traitement des informations peut avoir de graves répercussions pour les entreprises, leurs salariés et leurs clients.

Tout manquement à la confidentialité est susceptible de provoquer des pénalités financières illimitées, une mauvaise presse, une atteinte à notre réputation, une perte de confiance de la part de nos clients, une perte de chiffre d'affaires et, pour les salariés, des réclamations, voire des plaintes en cas de manquement à la confidentialité de leurs informations personnelles et la perspective d'une action disciplinaire dans les autres cas. Il est dans l'intérêt de chacun de nous de traiter les informations de manière appropriée.

Nous considérons que :

- Tous les employés de Roquette doivent être sensibilisés à leurs rôles et à leurs responsabilités en matière de Protection des Données Personnelles. Cette sensibilisation vise à renforcer la culture du respect de la confidentialité et de la Protection des Données Personnelles au sein de Roquette.

[DDPG001EN – Règle 1]

Il est nécessaire de former les employés à la mise en œuvre de la Politique relative à la Protection des Données.

[DDPG001EN – Règle 2]

RESPECT DE LA VIE PRIVÉE

C'est notre responsabilité !

Nous avons besoin des informations personnelles de nos clients et de nos salariés pour exercer correctement notre activité.

Ils nous font confiance pour que nous prenions soin de ces informations clés.

Chacun de nous est tenu de respecter les lois relatives à la Protection des Données.

C'est notre réputation !

Les réputations se font difficilement et se ruinent facilement.

Traiter les données de nos clients et salariés avec soin et respect est essentiel à la protection de notre réputation.

VOUS êtes notre meilleure protection contre les atteintes à notre réputation.

C'est une question de respect !

Les choix de nos clients et salariés quant à l'utilisation de leurs données personnelles doivent être respectés si nous voulons préserver la confiance qu'ils nous accordent.

C'est entre nos mains !

Nous sommes tous responsables de la sécurité et de la confidentialité des données personnelles des clients et salariés.

Une attention particulière doit être portée à toute information devant être adressée ou emportée hors site.

Nos collaborateurs sont formés !

- Code de Conduite – Protection des Données et de la Vie Privée - p. 42 – 43.
- Pour les nouveaux venus : Plusieurs informations et une formation en ligne sur la Protection des Données sont fournies lors de l'intégration globale.
- Pour les employés : Les formations sont disponibles sur l'intranet..
- Pour les Coordinateurs de Protection des Données : Des documents sont partagés sur notre Communauté « Data Protection Network ».
- Pour tous : Plus d'informations disponibles sur notre intranet > Protection des données.

Traitement des données personnelles

Le **traitement des données personnelles** désigne toute opération ou tout ensemble d'opérations effectuées sur des données personnelles ou des ensembles de données personnelles, que ce soit par des moyens automatisés ou non, comme la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou l'altération, la récupération, la consultation, l'utilisation, la divulgation par transmission, la dissémination ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la restriction, la suppression ou la destruction.

Vous devrez connaître l'exigence en matière de Protection des Données (et relative au RGPD) selon laquelle vous devez disposer d'une « base légale » pour la collecte de données personnelles. En fonction de la législation locale, il peut y avoir différents fondements juridiques.

Quelle est ma « base légale » pour le traitement des données personnelles ?

Vous devez être capable de répondre clairement à la question suivante :

« Comment avez-vous obtenu ma/mon/mes [élément(s) de donnée] et qu'est-ce qui vous autorise à en disposer ? »

Plus spécifiquement, cela signifie que vous devez respecter au moins l'une des six bases légales pour traiter des données. Dans le cadre du RGPD, vous ne pouvez pas traiter de données, sauf :

1. Consentement
2. Contrat
3. Obligation légale
4. Intérêts vitaux
5. Mission d'ordre public
6. Intérêt légitime

Licéité, loyauté et transparence

Nos responsabilités :

Nous devons appliquer des règles pour garantir un traitement licite des données personnelles.

Règles	Référence Q-Docs	Référence RGPD
• Agir avec licéité, équité et transparence en collectant des données	DDPG002EN – Règle 1	Art. 5 1. a)
• Montrer que le consentement des personnes concernées a été respecté (si nécessaire)	DDPG002EN – Règle 2	Art. 7
• Respecter les finalités définies durant la collecte des données	DDPG002EN – Règle 3	Art. 5 1. b)
• Limiter les informations collectées dans les formulaires papier ou numériques au strict minimum	DDPG002EN – Règle 4	Art. 5 1. c)
• Limiter la conservation des données au strict minimum	DDPG002EN – Règle 5	Art. 5 1. e)
• Prendre les mesures nécessaires pour transférer des données personnelles vers des pays tiers ou des organismes internationaux	DDPG002EN – Règle 6	Art. 44 à 50

Nos collaborateurs sont formés !

Droits des personnes concernées

Une **personne concernée** désigne une personne physique qui peut être identifiée, directement ou indirectement, notamment par l'intermédiaire de son nom, son numéro d'identification, son adresse, ses identifiants informatiques, ou tout autre élément spécifique à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.

Qu'est-ce qu'une « personne concernée » ?

Ce terme technique désigne tout individu dont les données personnelles précises sont traitées.

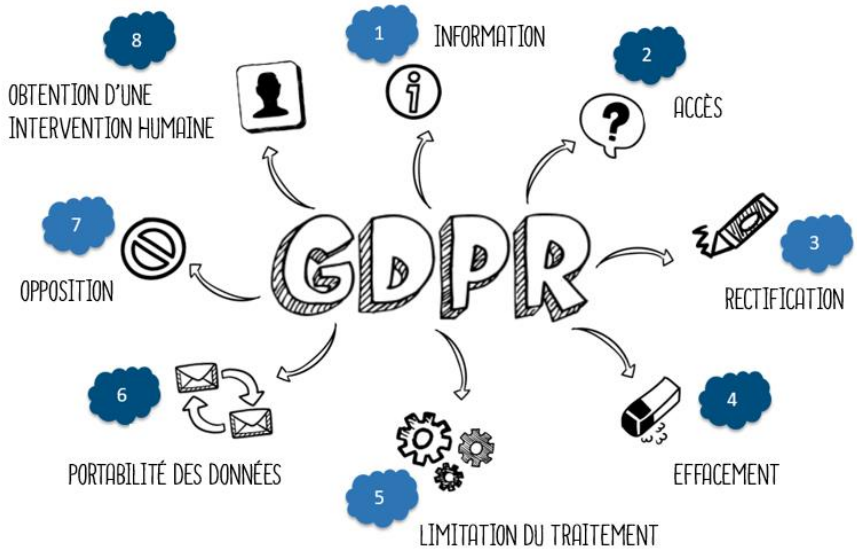
Qu'est-ce qu'une demande d'accès par la personne concernée ?

Les lois sur la Protection des Données en vigueur accordent aux individus, entre autres droits principaux, celui d'accéder à leurs informations personnelles.

Un individu peut vous envoyer une « demande d'accès », vous demandant de lui communiquer les données personnelles que vous détenez à son sujet et de lui fournir une copie de ces informations. Dans la plupart des cas, vous devez répondre à une demande d'accès valide dans un délai de 30 (*) jours calendaires suivant sa réception.

(*) : Cette période peut varier en fonction de la loi applicable ou de la nature de l'opération de traitement des données.

Quels sont les autres droits des personnes concernées ?



Nos responsabilités :

Nous devons appliquer des règles pour garantir les droits des personnes concernées.

Règles	Référence Q-Docs	Référence RGPD
• Vérifier que les mentions légales respectent les obligations	DDPG006EN Règle 1	Art. 12
• Permettre aux personnes concernées d'exercer leur droit d'accès	DDPG006EN Règle 2	Art. 15
• Permettre aux personnes concernées d'exercer leur droit de rectification	DDPG006EN Règle 3	Art. 16
• Permettre aux personnes concernées d'exercer leur droit à la portabilité des données	DDPG006EN Règle 4	Art. 20
• Permettre aux personnes concernées d'exercer leur droit à l'effacement (« droit à l'oubli »)	DDPG006EN Règle 5	Art. 17
• Permettre aux personnes concernées d'exercer leur droit à la limitation du traitement	DDPG006EN Règle 6	Art. 18
• Signaler toute rectification ou tout effacement des données personnelles ou toute limitation du traitement	DDPG006EN Règle 7	Art. 19
• Contrôler les prises de décision individuelles automatisées, y compris le profilage	DDPG006EN Règle 8	Art. 22

Nos collaborateurs sont formés !

Mention d'information

Le droit d'être informé(e) sur l'utilisation de ses données personnelles

Nous sommes tenus de vous informer, en tant que collaborateur, ainsi que les tiers avec lesquels Roquette travaille, de l'utilisation de vos/leurs données personnelles.

Nous devons fournir des informations détaillées sur les aspects suivants :

- Raison(s) pour laquelle/lesquelles Roquette utilise vos/leurs données.
- Type(s) de données que Roquette utilise.
- Durée de conservation de vos/leurs données.
- Votre/leur droit à l'information.
- Origine(s) des données.
- Notification de transfert de vos/leurs données par Roquette à des tiers, dont vos/leurs noms et les motifs du transfert.
- Notification de transfert des données à une autre juridiction, dont le pays impliqué et ce qu'il adviendra des données.
- Utilisation des données par Roquette à des fins de profilage (type de traitement automatisé dans lequel les données personnelles sont utilisées à des fins d'analyse ou de prédiction comme les performances au travail, la situation économique, la santé).
- Moyen(s) de contacter la DPO.
- En cas de situation préoccupante, votre/leur droit de porter plainte auprès de l'autorité de contrôle.

C'est ce qu'on appelle **Mention d'information** .

Nous devons vous/leur fournir des informations sur la confidentialité et la Protection des Données au moment où Roquette les collecte. Il en va de même si Roquette obtient vos/leurs données via une autre source. Cela doit se faire sous forme d'une mention d'information.

C'est ce qu'on appelle le **droit à l'information**.

Règle	Référence Q-Docs	Référence RGPD
• Vérifier que les mentions légales respectent les obligations	DDPG006EN Règle 1	Art. 12

Exemple :

- Mention d'information relative au site Web de Roquette, disponible sur : https://fr.roquette.com/protection-des-donnees.

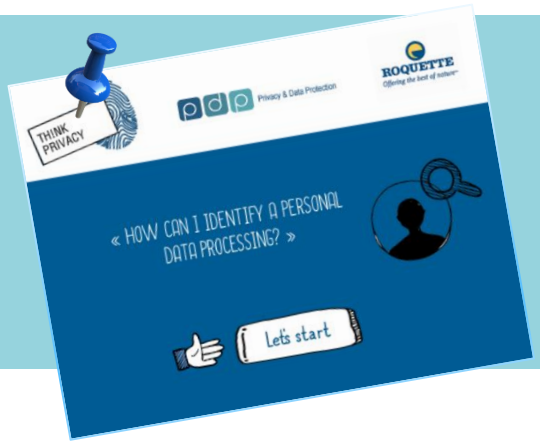
Dans quels cas Roquette est-elle dispensée de vous/les informer de ses activités ?

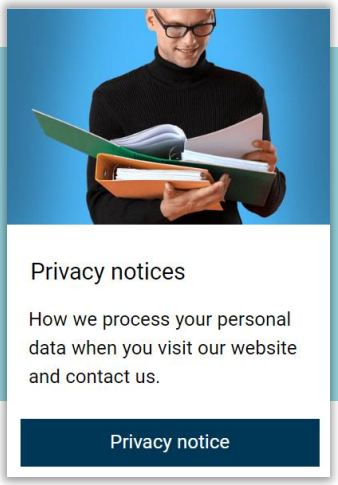
Si nous devons en général vous/leur fournir une note d'information sur la confidentialité, nous n'y sommes pas tenus, notamment dans les situations suivantes :

- vous disposez/ils disposent déjà de la mention d'information sur la confidentialité et la Protection des Données Personnelles sur chaque ligne et aucun changement n'est à signaler ;
- vous/leur donner la mention d'information sur la confidentialité et la Protection des Données Personnelles est impossible ou demanderait des « efforts disproportionnés » ;
- vous/leur donner la mention d'information sur la confidentialité et la Protection des Données Personnelles rendrait impossible l'utilisation de vos/leurs données ou nuirait gravement aux motifs de leur utilisation.

Remarque : Lorsque des mesures provisoires s'avèrent nécessaires pour prévenir la dissimulation ou la destruction de preuves, ces informations peuvent être émises après l'adoption desdites mesures.

Nos collaborateurs sont formés !





Minimisation des données

Qu'est-ce que le principe de minimisation des données ?

Ce que dit le RGPD – Article 5(1)(c) :

> « 1. Les données à caractère personnel doivent être :
>
> (c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données). »

Les formulaires papier ou numériques conçus par les Fonctions Globales pour collecter des données personnelles ne doivent contenir que des champs d'information strictement nécessaires aux finalités du traitement afin d'éviter la collecte de données non justifiées par ce traitement.

Nos responsabilités :

Nous devons nous assurer que les données personnelles que nous traitons sont :

- adéquates – suffisantes pour atteindre comme il faut la finalité que vous avez déclarée ;
- pertinentes – ont un lien rationnel avec cette finalité ;
- et limitées à ce qui est nécessaire – vous ne détenez pas plus que ce dont vous avez besoin pour cette finalité.

Règle	Référence Q-Docs	Référence RGPD
• Limiter les informations collectées dans les formulaires papier ou numériques au strict minimum	DDPG002EN – Règle 4	Art. 5 1. c)

Liste de vérification :

- ☑ Nous ne collectons que les données personnelles dont nous avons réellement besoin au regard de nos finalités spécifiques.
- ☑ Nous disposons de suffisamment de données personnelles pour atteindre ces finalités.
- ☑ Nous examinons périodiquement les données que nous détenons, et supprimons ce dont nous n'avons pas besoin.
- ☑ Nous devons identifier le nombre minimum de données personnelles dont nous avons besoin au regard des finalités pour lesquelles nous les collectons. Nous devons disposer de ces informations, mais pas plus.

Le principe de responsabilité signifie que vous devez être capable de prouver que vous utilisez des processus appropriés pour vous assurer de ne collecter et de ne détenir que les données personnelles dont vous avez besoin.

Gardez également en tête que le RGPD dispose que les individus ont le droit de compléter toute information incomplète qui est inadéquate au regard des finalités pour lesquelles vous l'avez collectée, en exerçant leur droit de rectification.
Ils peuvent également exiger de votre part de supprimer toute donnée qui n'est pas nécessaire aux finalités pour lesquelles vous l'avez collectée, en exerçant leur droit à l'effacement (droit à l'oubli).

Nos collaborateurs sont formés !

Sécurité des données

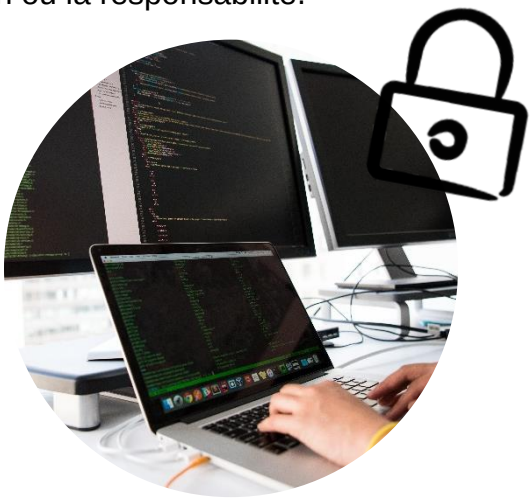
La **cyber-sécurité** est une activité transversale dont la mise en œuvre assure le partage et l'utilisation de données à un niveau adapté et garanti de protection des informations et des actifs connexes :

- **Confidentialité** : garantit la confidentialité et la non-divulgation des informations à des personnes ou entités inappropriées,
- **Intégrité** : garantit l'exactitude et l'exhaustivité des informations et des méthodes de traitement,
- **Disponibilité** : veille à ce que les utilisateurs autorisés aient toujours accès aux informations, aux applications et aux services lorsque cela est nécessaire,
- **Traçabilité** : désigne la capacité de conserver des suivis pertinents et, si nécessaire, des preuves des opérations réalisées dans nos systèmes. La traçabilité couvre également les objectifs juridiques comme la non-répudiation ou la responsabilité.

Les actifs de renseignements personnels incluent les éléments suivants :

- Documents papier (textes, cartes, photos, etc.),
- Informations numériques dans un environnement de travail,
- Informations numériques dans un environnement mobile,
- Savoir-faire et compétences professionnelles (détenus par les individus ou partagés oralement),
- Articles physiques (échantillons, souches, modèles, etc.).

[DSUG006EN] Directive sur la gestion de la cyber-sécurité



La **pseudonymisation** désigne le traitement des données personnelles de sorte que celles-ci ne puissent plus être attribuées à une personne concernée précise sans recourir à des informations supplémentaires, pour autant que ces dernières soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles pour garantir que les données personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable.

L'**anonymisation** désigne le processus qui altère les données personnelles de façon irréversible, de sorte qu'une personne concernée ne puisse plus être identifiée, directement ou indirectement, que ce soit par le responsable de traitement (1) seul ou en collaboration avec une autre partie.

Le **chiffrement** correspond à la méthode de conversion de texte brut ou de tout autre type de donnée de format lisible en une version encodée qui ne peut être décodée que par une autre entité ayant accès à une clé de déchiffrement. Il s'agit là d'une des méthodes les plus importantes pour assurer la sécurité des données, plus particulièrement la protection de bout en bout des données transmises par le biais de réseaux.

(1) : Voir définition à la page 38.

Nous considérons que :

Afin de préserver la sécurité et de prévenir tout traitement constituant une violation des lois et réglementations sur la Protection des Données, Roquette et nos sous-traitants doivent évaluer les risques inhérents au traitement et mettre en œuvre des mesures pour réduire ces risques, comme le **chiffrement** ou la **pseudonymisation**.

Nos responsabilités :

Nous devons appliquer des mesures de sécurité lors de la manipulation de tout type de données personnelles, mais ce que nous mettons en place dépend de circonstances qui nous sont propres. Nous avons besoin de nous assurer de la confidentialité, de l'intégrité et de la disponibilité des systèmes et des services que nous utilisons pour traiter des données personnelles. Ceci peut inclure, entre autres, les politiques de sécurité des informations, les contrôles d'accès, le suivi de sécurité et les plans de rétablissement.

Des mesures de sécurité appropriées doivent être prises tout au long du cycle de vie des données personnelles et par tous les acteurs.

Règles	Référence Q-Docs	Référence RGPD
• Application et examen des mesures de sécurité définies dans la politique et les directives relatives à la sécurité	DDPG007EN Règle 1	Art. 32
• Intégration de l'examen de la sécurité des informations et de la Protection des Données dans les projets	DDPG007EN Règle 2	Art. 32
• Sécurité, Protection des données et de la vie privée dès la conception et par défaut	DDPG007EN Règle 3	Art. 25
• Intégration des clauses de sécurité des informations et de Protection des Données avec les sous-traitants	DDPG007EN Règle 4	Art. 32

Nos collaborateurs sont formés !

Classification des informations personnelles

Le traitement des données personnelles sensibles et de certaines catégories spécifiques de données personnelles est interdit, sauf dans certains cas particuliers.

Ces traitements requièrent des mesures de protection en termes de :

Marquage, Accès, Transmission, Transport, Copie et impression, Stockage et archivage, Destruction.

La **classification** vise à identifier les actifs d'informations sensibles, quels qu'en soient la nature et le support, et à spécifier, si nécessaire, les mesures de protection qui s'imposent pour réduire les risques en cas de divulgation non désirée.

Le niveau de **classification de confidentialité** est directement lié à l'impact évalué d'une divulgation d'informations non désirée.

[DSUG001EN] Directive sur la protection des informations

Classification des protections des informations	Types de données personnelles	Catégories de données personnelles
Niveau 1 = ROQUETTE RESTREINT Définition : type d'information dont la divulgation publique à grande échelle n'est pas recommandée	Données personnelles communes	État civil, identité, données d'identification
		Vie personnelle (habitudes de vie, situation de famille, hors données sensibles)
		Vie professionnelle (CV, formation initiale et formation professionnelle continue, distinctions)
		Informations économiques et financières (revenus, situation financière, situation fiscale)
		Données de connexion (adresses IP, journaux d'événements)
		Données de localisation (voyages, données GPS, données de géolocalisation de téléphone portable)
Niveau 2 = ROQUETTE CONFIDENTIEL Définition : type d'information dont la divulgation peut considérablement nuire aux intérêts du Groupe	Données personnelles considérées comme sensibles	Numéro de sécurité sociale
		Données biométriques
		Données bancaires
Niveau 3 = ROQUETTE SECRET Définition : type d'information dont la divulgation peut gravement nuire aux intérêts du Groupe	Données personnelles sensibles au sens prévu par la Loi « Informatique et libertés »	Opinions philosophiques, politiques, religieuses et syndicales, vie sexuelle, données relatives à la santé, origine raciale ou ethnique
		Infractions, condamnations, mesures de sécurité

Nos responsabilités :

Règles	Référence Q-Docs	Référence RGPD
• Respecter le cadre légal pour le traitement des données personnelles sensibles	DDPG004EN Règle 1	Art. 9
• Interdire le traitement de données relatives aux condamnations pénales et aux infractions	DDPG004EN Règle 2	Art. 10
• Limiter l'accès aux données relatives à la santé uniquement aux professionnels de santé en ayant l'autorisation	DDPG004EN Règle 3	Art. 9
• Interdire l'utilisation du numéro d'identification national comme unique identifiant	DDPG004EN Règle 4	Art. 87
• Restreindre l'accès aux données bancaires et leur utilisation	DDPG004EN Règle 5	Art. 9
• Restreindre l'accès aux données sensibles uniquement aux personnes en ayant l'autorisation	DDPG004EN Règle 6	Art. 9
• Mener des analyses d'impact relatives à la vie privée des personnes concernées impliquées dans le traitement des données sensibles	DDPG004EN Règle 7	Art. 35
• Limiter l'utilisation du champ de commentaire aux informations générales	DDPG004EN Règle 8	Bonnes pratiques

Quelques astuces pratiques...

Exemples de mesures de protection à prendre pour chaque catégorie d'actifs d'informations classifiés (papier, numérique, savoir-faire, physique).

Conservation des données

Le besoin croissant de dématérialiser les opérations et l'échange d'informations entre le Groupe, nos clients et nos partenaires commerciaux, ainsi que les exigences législatives et réglementaires, ont assujetti Roquette à de nombreuses obligations en termes de durée de conservation des données et de politiques de gestion des dossiers.

Sur la base de nos activités, Roquette acquiert et traite une grande quantité de données sensibles relatives à notre stratégie, nos résultats financiers, notre développement commercial ou nos engagements, **ainsi que des données personnelles relatives à nos clients, partenaires commerciaux et membres du personnel**.

Les informations envoyées ou reçues par Roquette en rapport avec nos activités doivent être conservées durant une période de conservation minimale, bien que rien ne nous empêche de les archiver pendant de plus longues périodes, **sauf si elles contiennent des données personnelles**.

Ce délai, durant lequel les autorités administratives et compétentes peuvent procéder à des post-inspections, varie en fonction de la nature des informations à conserver et des exigences légales pertinentes.

Les durées de conservation infinies ou indéterminées sont interdites.

RGPD, Art. 5.1. E)

« Limitation de la conservation »

Les données personnelles doivent être conservées sous une forme qui permette l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles les données personnelles sont traitées.

Les données personnelles peuvent être conservées pendant plus longtemps dans la mesure où elles seront traitées uniquement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques soumises à une mise en œuvre des mesures techniques et organisationnelles appropriées, nécessaires pour garantir les droits et libertés de la personne concernée.

Nos responsabilités :

- En tant que responsable de traitement des données, Roquette doit définir des périodes de conservation spécifiques et adéquates pour chaque catégorie de données personnelles collectées et traitées.
- Avant la mise en œuvre du traitement des données personnelles et avec l'aide du Coordinateur de la Protection des Données, le chef du projet doit spécifier, dans notre registre, la durée de conservation des données.
- Nous devons conserver des données personnelles uniquement pendant la durée nécessaire aux fins du traitement et respecter les lois applicables.

Règle	Référence Q-Docs	Référence RGPD
• Limiter la conservation des données au strict minimum	DDPG002EN – Règle 4	Art. 5 1. E)

À cet égard, les Fonctions Globales, les GBU et les régions s'engagent à respecter les Règles de conservation des informations de la société et à maintenir les procédures associées en condition opérationnelle.

Exemple :

À l'issue d'un processus de recrutement, nous devons supprimer les informations concernant les candidats non retenus, à moins qu'ils n'acceptent de rester dans notre « vivier » pendant une période limitée (2 ans).

Nos collaborateurs sont formés !

2 Nos standards quant à nos RELATIONS AVEC LES SOCIÉTÉS AFFILIÉES et LES SOUS-TRAITANTS

Qualification du sous-traitant des données et du responsable de traitement

Le **responsable de traitement** désigne la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui, seul ou avec l'aide d'autres entités, détermine les finalités et les moyens du traitement des données personnelles.

Le **coresponsable de traitement** désigne un ou plusieurs responsables du traitement supplémentaires dont le rôle est de déterminer conjointement les finalités et les moyens du traitement. En tout état de cause, chaque responsable de traitement reste chargé du respect de toutes les obligations des responsables de traitement dans le cadre du RGPD.

Le **sous-traitant des données** désigne une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui traite des données personnelles pour le compte du responsable de traitement.

Qui est sous-traitant des données au sens du Règlement Général sur la Protection des Données ?

(Article 4 du RGPD – Définitions).

Une très grande variété de prestataires de services a la qualité de sous-traitant au sens juridique du terme. Les activités des sous-traitants peuvent concerner une tâche bien précise (sous-traitance d'envoi de courriers) ou être plus générales et étendues (gestion de l'ensemble d'un service pour le compte d'un autre organisme telle que la gestion de la paie des salariés, par exemple).

Sont notamment concernés par le RGPD :

- les prestataires de services informatiques (hébergement, maintenance, etc.), les intégrateurs de logiciels, les sociétés de cyber-sécurité ou les entreprises de service du numérique (anciennement sociétés de services et d'ingénierie en informatique, SSII) qui ont accès aux données,
- les agences de marketing ou de communication qui traitent des données personnelles pour le compte de clients,
- et plus généralement, tout organisme offrant un service qui implique un traitement de données à caractère personnel pour le compte d'un autre organisme,
- une autorité publique ou une association peut également être amenée à recevoir une telle qualification.

Dans la mesure où ils n'ont pas accès aux données à caractère personnel ou ne les traitent pas, les éditeurs de logiciels et les fabricants de matériels (badgeuses, matériel biométrique ou matériel médical, par ex.) ne sont pas concernés.

Exemple de qualification de sous-traitant et de responsable de traitement :

Une entreprise A offre un service d'envoi de courriers de prospection commerciale en utilisant les fichiers clients d'autres entreprises B et C.

L'entreprise A est un sous-traitant des entreprises B et C dans la mesure où elle traite les données clients nécessaires à l'envoi des courriers pour le compte et sur les instructions des entreprises B et C.

Les entreprises B et C sont responsables de traitement de gestion de leurs clients, incluant l'envoi de courriers de prospection commerciale.

L'entreprise A est par ailleurs responsable de traitement s'agissant de la gestion du personnel dont elle est l'employeur, et de la gestion de ses clients dont font partie les entreprises B et C.

Une entreprise A offre un service d'envoi de courriers de prospection commerciale en utilisant les fichiers clients des entreprises B et C.

Textes officiels

- Article 4 du RGPD pour les définitions de « responsable de traitement » et de « sous-traitant »
- Article 28.10 du RGPD sur la notion de « responsable de traitement »

Nos collaborateurs sont formés !

Clauses de Protection des Données

Quand est-il nécessaire d'avoir un contrat et pourquoi est-ce important ?

Lorsqu'en tant que responsable de traitement, nous faisons appel à un sous-traitant des données pour traiter des données personnelles en notre nom, il faut conclure un contrat écrit entre les parties.
Le contrat est important dans la mesure où il permet aux deux parties de comprendre nos responsabilités et obligations.

Les contrats qui prévoient des clauses spécifiques de Protection des Données et/ou un accord de Protection des Données entre Roquette, en tant que responsable de traitement, et ses sous-traitants des données garantissent la bonne compréhension des obligations et responsabilités des deux parties. Les contrats nous aident également à respecter le RGPD et à prouver aux individus et aux régulateurs notre conformité à celui-ci, comme le veut le principe de responsabilité.

Quelles sont nos responsabilités et nos obligations en tant que responsable de traitement faisant appel à un sous-traitant des données ?

Nous ne devons recourir qu'aux sous-traitants des données pouvant apporter suffisamment de garanties quant aux mesures techniques et organisationnelles appropriées qu'ils vont mettre en œuvre pour nous assurer que leur traitement respectera les exigences du RGPD et protégera les droits des personnes concernées.

En tant que responsable de traitement, il nous incombe principalement de veiller au respect général du RGPD et des autres lois relatives à la confidentialité des données en vigueur et de prouver cette conformité. En cas de manquement à ces obligations, nous pouvons être tenus de nous acquitter de dommages et intérêts dans le cadre de poursuites judiciaires ou être passibles d'amendes, d'autres sanctions ou de mesures correctives.

Quelles sont les nouveautés introduites par le RGPD ?

Plutôt qu'un simple moyen de prouver le respect des principes de Protection des Données (mesures de sécurité appropriées), la mise en place de contrats écrits entre les responsables de traitement et les sous-traitants des données est une exigence du RGPD.

Ces contrats doivent désormais prévoir des clauses minimales spécifiques. Ces clauses ont pour vocation de garantir que le traitement effectué par un sous-traitant des données respecte toutes les exigences du RGPD, en plus de celles relatives à la conservation des données personnelles de façon sécurisée.

Règles	Référence Q-Docs	Référence RGPD
• Intégration des clauses de sécurité des informations et de Protection des Données avec les sous-traitants	DDPG007EN Règle 4	Art. 32
• Sécurité des sous-traitants des données	DSUG016EN	

Que faut-il inclure dans le contrat ?

Les contrats doivent mentionner :

- ☑ l'objet et la durée du traitement ;
- ☑ la nature et la finalité du traitement ;
- ☑ le type de données personnelles et les catégories de personnes concernées ;
- ☑ et les obligations et les droits du responsable de traitement.

Les contrats doivent également prévoir des modalités ou clauses spécifiques concernant :

- ☑ le traitement, effectué uniquement sur les instructions documentées du responsable de traitement ;
- ☑ le devoir de confidentialité ;
- ☑ les mesures de sécurité appropriées ;
- ☑ le recours aux sous-traitants ultérieurs des données ;
- ☑ les droits des personnes concernées ;
- ☑ l'aide apportée au responsable de traitement ;
- ☑ les dispositions de fin de contrat ;
- ☑ et les audits et inspections.

Nos employés sont formés !

- Guide sur la Protection des Données pour les contrats de sous-traitance en conformité au RGPD.
- Modèle de clauses contractuelles de sous-traitance disponible sur notre système de Privacy Management : OneTrust@Roquette > Module Vendor Risk Management.

Accord de transfert des données

Un **transfert de données** désigne toute communication, copie ou transit de données personnelles (hébergement de serveurs, envoi de pièces jointes par e-mail, outils d'accès à distance, partage d'écran, etc.) à des fins de traitement dans d'autres pays n'ayant pas les mêmes lois sur la Protection des Données Personnelles applicables.

Nous vivons dans un monde plus connecté que jamais. Le transfert de données à l'international occupe une place essentielle dans les opérations commerciales quotidiennes de Roquette à l'échelle mondiale. À titre d'exemple, nous stockons des données personnelles des employés dans un service cloud hébergé à l'étranger et partageons des données personnelles des employés et des clients entre nos filiales implantées dans le monde entier.

Comment le RGPD et autres lois sur la Protection des Données en vigueur affectent ces transferts de données à l'international ?

Nos responsabilités :

Tout transfert de données personnelles qui fait l'objet d'un traitement ou est destiné à un traitement après transfert vers un pays tiers ou un organisme international ne doit être effectué que si :

- La législation locale l'autorise et/ou l'autorité de contrôle a décidé que le pays tiers, un territoire ou un ou plusieurs secteurs spécifiques au sein de ce pays tiers, ou l'organisme international en question garantit un niveau adéquat de protection ou a donné son autorisation, et/ou
- Une mesure juridique a été prise (par ex. : Règles d'entreprise contraignantes ou clauses contractuelles types pour le transfert de données personnelles vers des sous-traitants des données établis dans des pays tiers en vertu de la Directive 95/46/CE du Parlement européen et du Conseil, etc.).

Règle	Référence Q-Docs	Référence RGPD
• Prendre les mesures nécessaires pour transférer des données personnelles vers des pays tiers ou des organismes internationaux	DDPG002EN – Règle 6	Art. 44 à 50

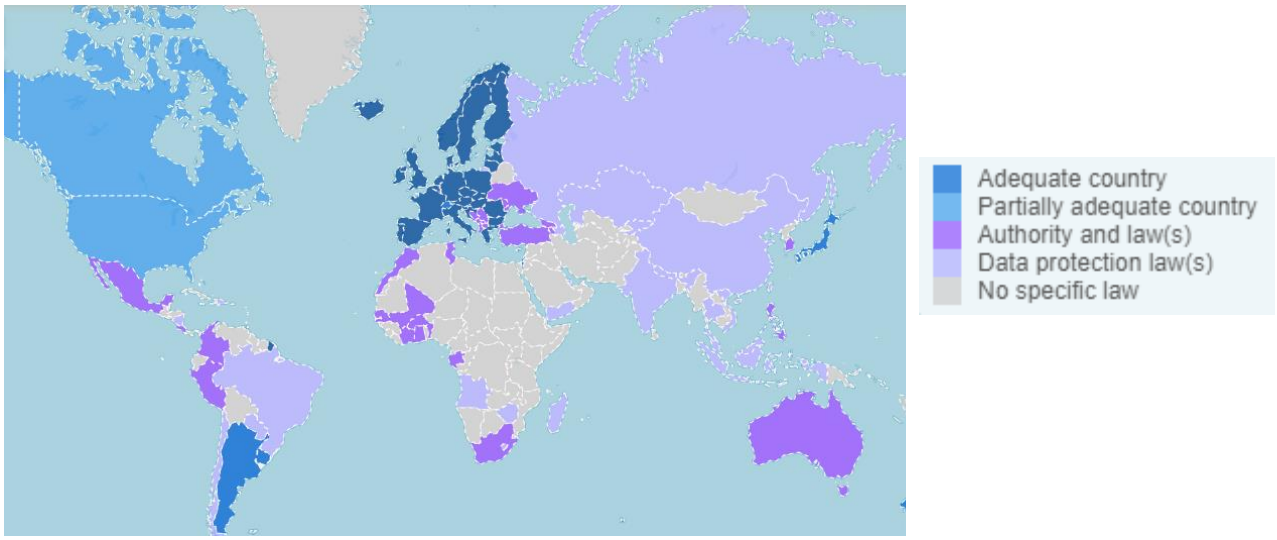
Dans tous les cas, veuillez d'abord contacter la DPO.

Dans quel pays transférer des données personnelles et à quelles conditions ?

Consultez cette carte pour avoir une vision d'ensemble :

https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde.

Cette carte vous permet de visualiser le niveau de Protection des Données pour chaque pays.



Nos collaborateurs sont formés !

- Section sur le Data Transfert Agreement, y compris notre modèle Data Processing Agreement.
- FAQ pour résoudre les problèmes posés par l'entrée en vigueur de la Décision de la Commission européenne sur les clauses contractuelles types pour le transfert des données personnelles vers des sous-traitants des données établis dans des pays tiers.

3 Nos standards quant à nos RELATIONS AVEC notre RÉSEAU et les AUTORITÉS DE CONTRÔLE

Data Protection Officer

Le Groupe a désigné une Data Protection Officer.

Le **Data Protection Officer** (DPO) nous aide à contrôler la conformité interne, nous informe et nous conseille sur nos obligations relatives à la Protection des Données, apporte des conseils en matière d'Analyses d'impact relatives à la Protection des Données (AIPD) et sert d'interlocuteur pour les personnes concernées et l'autorité de contrôle.

Le DPO doit agir de manière indépendante, justifier d'une expertise en matière de Protection des Données, disposer des ressources adéquates et rendre compte au niveau le plus haut de la hiérarchie.

Le DPO peut nous aider à prouver notre conformité au RGPD et participe au renforcement de notre responsabilité.

Tâches du DPO	Référence Q-Docs	Référence RGPD
• Notre DPO a pour mission de contrôler la conformité au RGPD et aux autres lois sur la Protection des Données ainsi qu'à nos politiques de Protection des Données, d'organiser des campagnes de sensibilisation, d'assurer des formations et de réaliser des audits	MDPG001EN Manuel sur la Protection des données personnelles	RGPD Article 39 Tâches du Data Protection Officer
• Nous tiendrons compte des conseils de notre DPO et des informations qu'elle fournit sur nos obligations en matière de Protection des Données		
• Lors de la réalisation d'une AIPD, nous demandons conseil auprès de notre DPO qui contrôle également le processus		
• Notre DPO agit en qualité d'interlocutrice pour les autorités de contrôle		
• Dans l'accomplissement de ses missions, notre DPO tient dûment compte du risque associé aux opérations de traitement compte tenu de la nature, du champ d'application, du contexte et des finalités du traitement		

La DPO du Groupe a été désignée auprès de la CNIL par le CEO pour prendre ses fonctions le 25 mai 2018, date d'application du RGPD.

Responsabilité du DPO :

- Notre Data Protection Officer, Jennifer Godin, représente une interlocutrice facilement accessible pour nos employés, les individus et l'autorité de contrôle.
- Nous avons publié les coordonnées de la DPO et les avons communiquées aux autorités de contrôle.
  - ☑ https://fr.Roquette.com/protection-des-donnees
  - ☑ Intranet > Protection des Données
  - ☑ Espace collaboratif > Réseau de la Protection des Données

Contactez la DPO en cas de :

- ☑ Traitement des données personnelles
- ☑ Requêtes des personnes concernées
- ☑ Violation de données personnelles
- ☑ Besoin de conseil ou d'assistance

Une interlocutrice unique : dpo@Roquette.com ou jennifer.godin@Roquette.com

Nos collaborateurs sont formés !

Protection des Données : Réseau…

Les coordinateurs fonctionnels (« Privacy Coordinators ») et les DPO locaux forment un réseau qui permet à la Data Protection Officer du Groupe, respectivement, de mettre en œuvre les règles relatives à la Protection des Données Personnelles dans chaque Fonction Globale et de respecter les exigences des lois et réglementations pertinentes en matière de Protection des Données dans les pays où Roquette exerce ses activités.

Les DPO/Coordinateurs locaux exécutent au minimum les tâches suivantes :

- Informer et conseiller au niveau local sur les obligations conformément à la Politique relative à la Protection des Données Personnelles de Roquette définie par la DPO Groupe et les exigences des lois locales applicables en matière de Protection des Données ;
- Contrôler le respect de la législation locale, d'autres législations et réglementations applicables en matière de Protection des Données, si nécessaire, avec l'aide de la DPO Groupe et aux politiques relatives à la Protection des Données Personnelles ;
- Fournir des conseils au niveau local sur demande concernant l'analyse d'impact relative à la Protection des Données et contrôler ses performances ;
- Coopérer avec l'autorité de contrôle locale ;
- Agir en qualité d'interlocuteur pour la DPO Groupe sur des problèmes concernant le traitement et la consulter, le cas échéant, pour tout autre sujet ;
- Rendre compte de ses activités à la DPO Groupe pour contribuer à améliorer le système de gestion de la Protection des Données du Groupe.

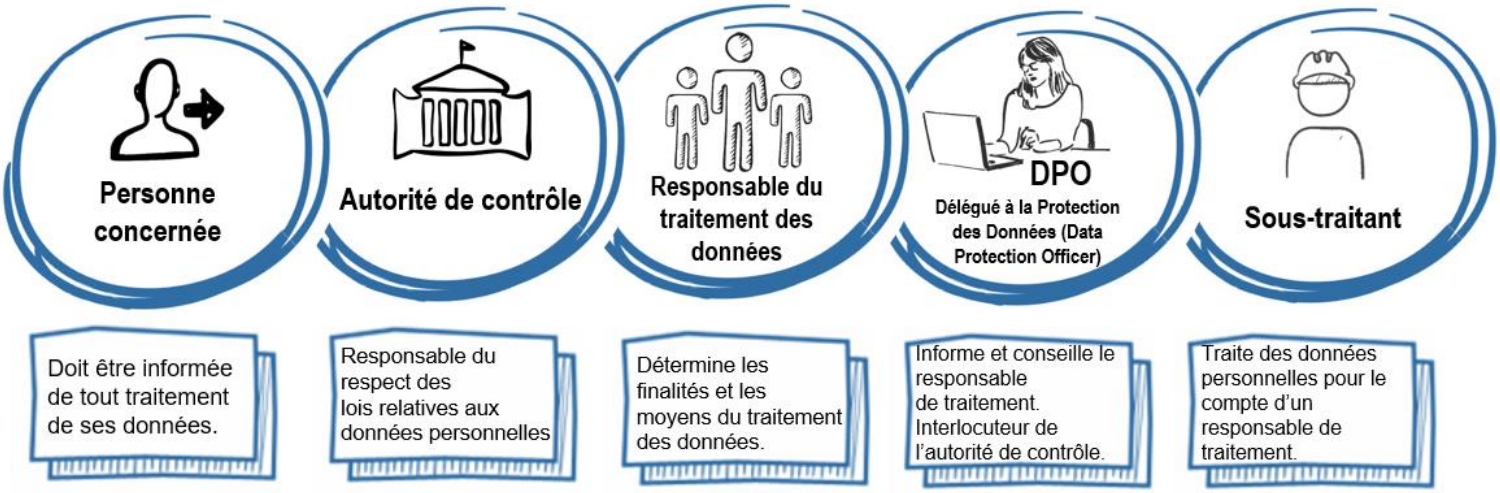
Nos collaborateurs sont formés !

Notre séminaire annuel PDP est le lieu de rencontre de notre réseau de contributeurs à la protection des données et de la vie privée.

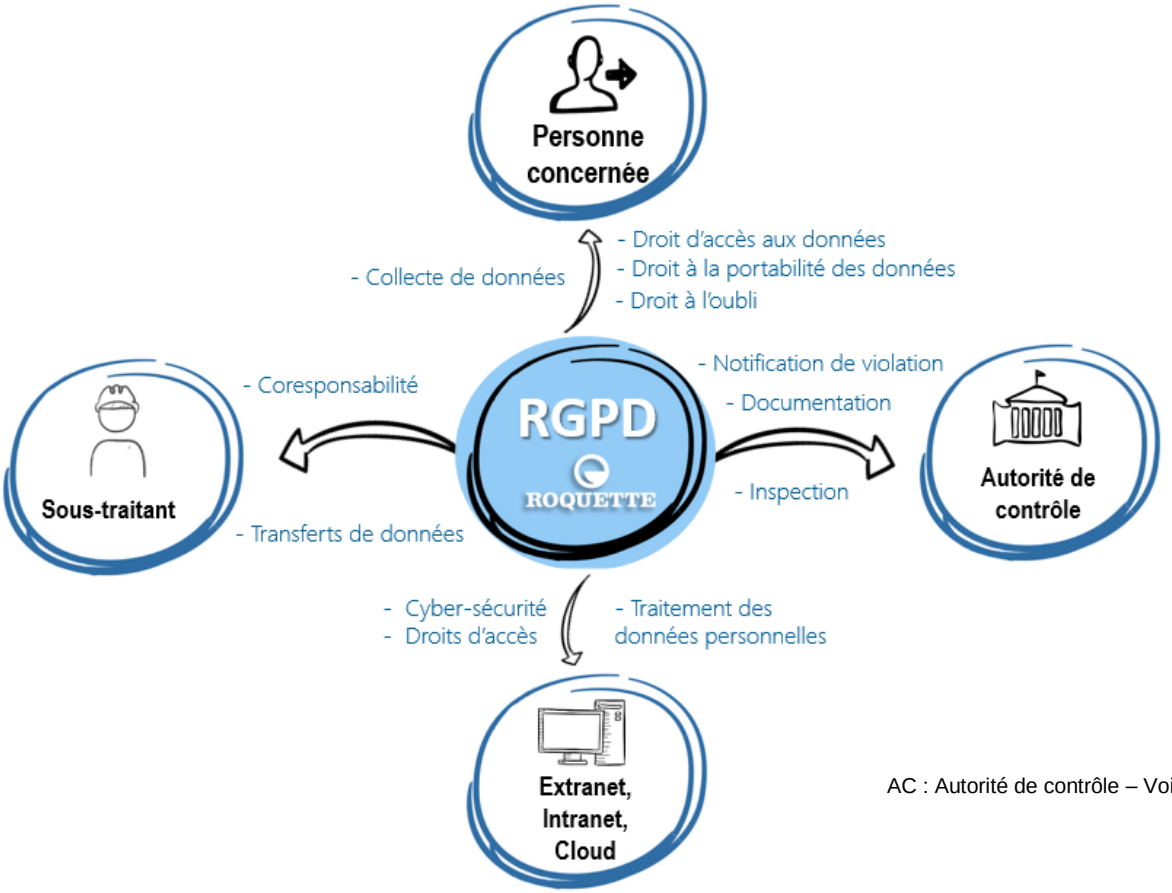
.

et acteurs

Quels sont les nouveaux acteurs ?



Quelles sont les relations entre ces acteurs ?



AC : Autorité de contrôle – Voir page 50

Autorités de contrôle

De nombreux pays disposent d'une loi sur la Protection des Données et d'une

Autorité de Protection des Données (APD)

indépendante. Ces autorités réglementent la vie privée et la liberté d'information de façon indépendante au niveau national. Elles promeuvent et défendent les droits des personnes concernées à accéder aux informations détenues par les organismes et à faire protéger leurs informations personnelles.

Quel est le rôle d'une autorité de contrôle dans le cadre du RGPD ?

Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de contrôler l'application des lois relatives aux données personnelles et à la vie privée afin de protéger les libertés et droits fondamentaux des personnes concernées à l'égard du traitement des données personnelles et de faciliter le libre flux de ces données au sein de l'UE.

Dans le cadre du RGPD, tous les États membres de l'UE disposent d'une Autorité de Protection des Données, qui sert en général d'interlocuteur privilégié pour les acteurs au sein de cet État membre.

Pour veiller à l'application du RGPD de manière cohérente dans l'ensemble de l'UE, chaque autorité de contrôle doit travailler en collaboration avec ses homologues étrangères et la Commission européenne.

Chaque autorité de contrôle doit, sur son territoire, favoriser la sensibilisation du public et sa compréhension des risques, règles, garanties et droits en matière de traitement des données personnelles.

C'est également auprès d'elles que les organismes introduisent une réclamation en cas de violation d'une législation sur la Protection des Données et demandent conseil, posent des questions spécifiques et/ou sollicitent de l'aide.

En résumé, les responsabilités des autorités de contrôle (AC) consistent à :

- Garantir l'application des règles, y compris par l'infliction d'amendes,
- Clarifier l'application des règles, si besoin est, par ex. par le biais de directives,
- Promouvoir une culture du dialogue avec tous les acteurs, y compris les entreprises,
- Coopérer ensemble.

CNIL : Commission Nationale de l'Informatique et des Libertés.

Autorité chef de file

- L'autorité de contrôle sous laquelle se place l'établissement principal du responsable de traitement ou du sous-traitant des données doit agir en qualité d'autorité chef de file. Elle doit coopérer avec les autres autorités concernées.

- Il n'est pertinent de désigner une autorité de contrôle chef de file que lorsque le traitement transfrontalier de données à caractère personnel est effectué par un responsable de traitement ou un sous-traitant des données.

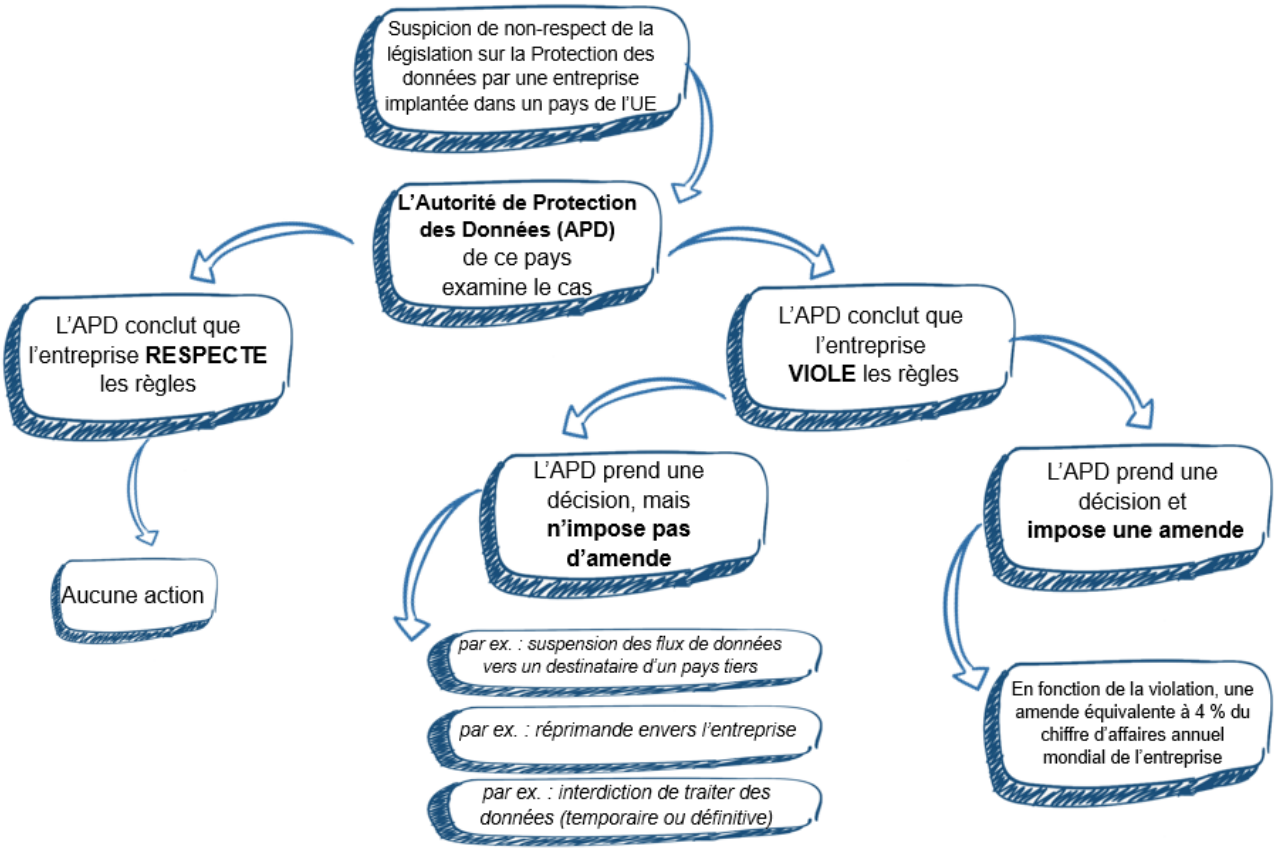
Comment désigner l'« autorité de contrôle chef de file » ?

Déterminer le lieu de l'administration centrale du responsable de traitement principal dans l'UE. L'autorité de contrôle du pays où se situe le lieu de l'administration centrale est l'autorité chef de file du responsable de traitement.

---

*La **CNIL** est l'autorité de contrôle chef de file de Roquette*

Comment fonctionne le mécanisme de sanctions du RGPD en pratique ?



Gouvernance

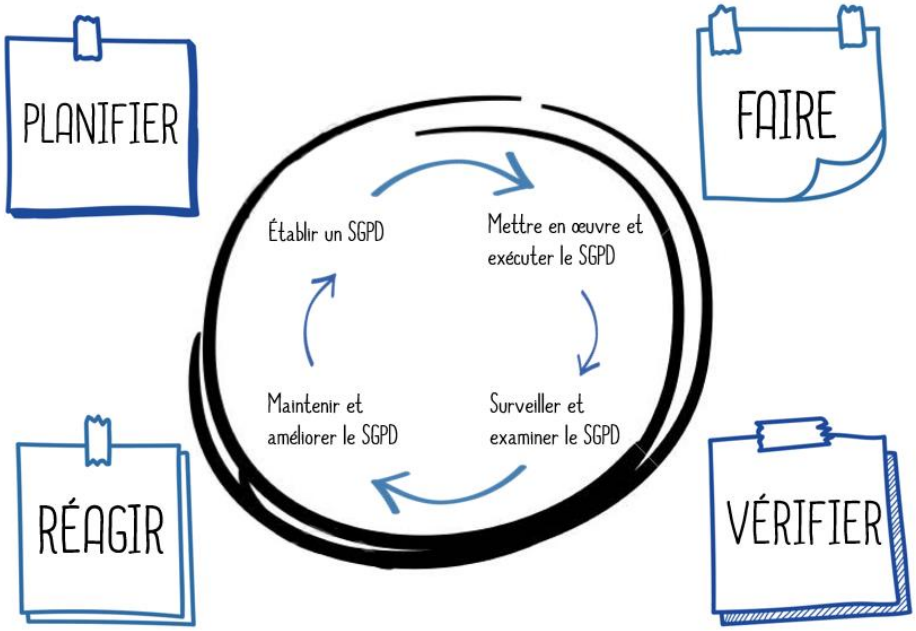
« La **Gouvernance de Protection des Données** s'articule principalement autour de la Data Protection Officer, de ses coordinateurs par site et par fonction, du Directeur général en qualité de Responsable de traitement des données, des Responsables de Fonctions Globales en qualité de responsable de la mise en œuvre du traitement des données personnelles et des sous-traitants en qualité de Sous-traitant des données. » [MDPG001EN]

Nous adoptons une approche procédurale pour l'établissement, la mise en œuvre, le fonctionnement, le contrôle, l'examen, l'entretien et l'amélioration du **S**ystème de **M**anagement de la **P**rotection des **D**onnées personnelles (**SMPD**) de Roquette.

Le processus et l'approche de la gestion de la Protection des Données Personnelles définis au sein de cette gouvernance encouragent leurs utilisateurs à souligner l'importance de :

1) la compréhension des exigences en matière de Protection des Données de Roquette et du besoin d'établir des directives et des procédures pour la Protection des Données ;
2) la mise en œuvre et l'exécution de contrôles pour gérer les risques en matière de Protection des Données de Roquette dans le cadre des risques commerciaux d'ordre général de Roquette ;
3) le suivi et l'examen des performances et de l'efficacité du SMPD ;
4) et l'amélioration continue qui repose sur des mesures objectives.

Nous adoptons le modèle "Planifier-Faire-Vérifier-Réagir" (PFVR) que nous appliquons pour structurer l'ensemble des processus du Système de Management de la Protection des Données (SMPD).



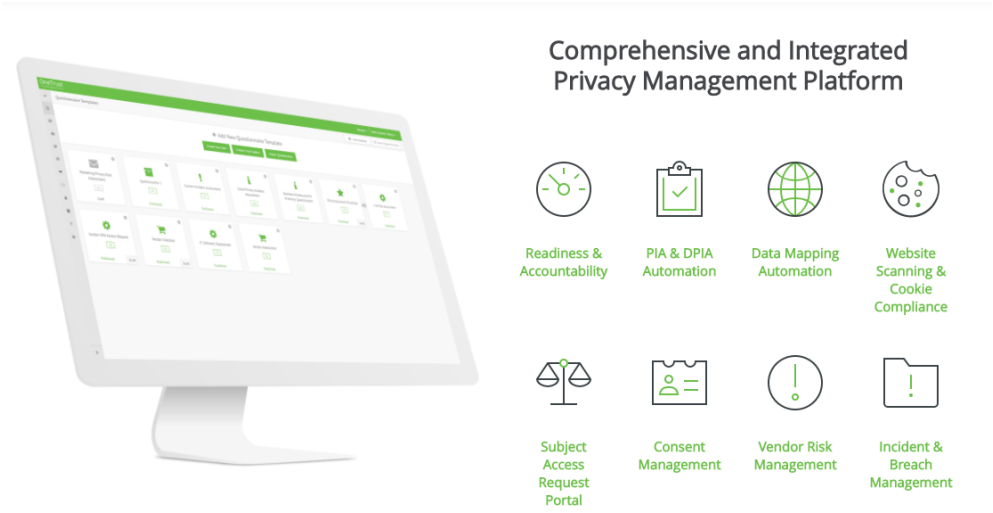
Notre approche :

Notre programme de conformité au RGPD est axé sur les points suivants :

- Compréhension de la façon dont notre entreprise recueille, stocke, utilise et transfère des données pour être en conformité,
- Création d'une culture de la conformité dans notre entreprise,
- Réalisation d'analyses d'impact relatives à la confidentialité,
- Préparation à une infraction de données,
- Allocation de ressources au programme de Protection de la Vie Privée,
- Mise en œuvre d'un système de gestion de la Protection des Données (Planifier – Faire – Vérifier – Réagir).

Pour atteindre ces objectifs, nous avons, dans le cadre de notre Programme :

- Défini une Politique relative à la Protection des Données, ainsi qu'une Gouvernance et une Documentation associées,
- Géré un projet de conformité au RGPD pour l'examen du traitement, la gestion des violations de données, l'examen de contrats, de clauses relatives à la Protection des Données, d'accord de transfert des données, etc.,
- Mis en œuvre un logiciel de gestion des données personnelles en conformité au RGPD.



Cette plateforme de gestion présente les caractéristiques principales suivantes :

- Tenue du registre du traitement des données (Cartographie des données),
- Gestion des risques associés au traitement (par le biais du PIA, etc.),
- Gestion des requêtes et des droits (d'accès, de rectification, d'opposition, etc.),
- Gestion des incidents et des violations de données,
- Gestion de la documentation relative à la conformité.

Responsabilité

La **responsabilité** compte parmi les principes de la Protection des Données. Nous sommes responsables du respect du RGPD et nous devons être en mesure de prouver notre conformité à ce règlement.

Pourquoi la responsabilité est-elle importante ?

Endosser la responsabilité de ce que nous faisons des données personnelles et apporter la preuve des étapes que nous avons suivies pour protéger les droits des personnes nous permet de mieux respecter les lois et nous offre un avantage concurrentiel. La responsabilité nous donne une véritable occasion de montrer, et de prouver, comment nous respectons la vie privée des personnes. Elle peut nous aider à développer et à entretenir la confiance que les personnes nous accordent.

En outre, si un problème survient, notre capacité à montrer que nous avons activement tenu compte des risques et mis en place des mesures et des garanties contribue à atténuer toute action coercitive qui pourrait être intentée contre nous. Dans le cas contraire, notre incapacité à démontrer de bonnes pratiques en matière de Protection des Données nous expose à des amendes et peut entraîner une atteinte à notre réputation.

Qu'est-ce que l'adoption du principe de responsabilité implique concrètement ?

Le traitement des données personnelles implique un devoir de vigilance et l'adoption de mesures concrètes et pratiques pour sa protection. Respecter le principe de responsabilité signifie :

- documenter et communiquer de façon appropriée toutes les directives, procédures et pratiques relatives à la vie privée (notre « Politique ») ;
- confier la mise en œuvre de la Politique à un individu spécifique au sein de l'entreprise (qui, le cas échéant, peut à son tour déléguer cette tâche à d'autres personnes de l'entreprise) ;
- s'assurer, lors d'un transfert de données personnelles à des tiers, que le destinataire tiers sera tenu de garantir un niveau équivalent de Protection des Données et de la Vie Privée par le biais de clauses contractuelles ou d'autres moyens comme les politiques internes obligatoires (une loi applicable peut contenir des exigences supplémentaires concernant les transferts de données à l'international) ;

- dispenser une formation adaptée pour les membres du personnel du responsable de traitement des données qui auront accès à des données personnelles ;
- mettre au point une gestion efficace des réclamations internes et rectifier les procédures utilisées par la personne concernée ;
- informer les personnes concernées sur les violations de la vie privée susceptibles de leur causer des dommages importants (sauf interdiction, par ex., pendant une collaboration avec les forces de l'ordre) ainsi que sur les mesures prises pour les résoudre ;
- notifier tous les acteurs de la Protection de la Vie Privée pertinents au sujet des violations de la vie privée conformément à certaines juridictions (par ex., les autorités compétentes en matière de Protection des Données) et en fonction du niveau de risque ;
- permettre à la personne lésée d'accéder à des corrections appropriées et efficaces telles que la rectification, l'effacement ou la restitution en cas d'atteinte à la vie privée ;
- et envisager des procédures d'indemnisation dans les cas où il serait difficile, voire impossible, de rétablir le statut de la vie privée de la personne physique à son état initial.

Liste de vérification :

- ☑ Nous sommes tenus responsables du respect du RGPD, au niveau le plus élevé de la hiérarchie et au sein de toute l'entreprise.
- ☑ Nous conservons des preuves des étapes que nous suivons pour respecter le RGPD.

Nous mettons en place des mesures techniques et organisationnelles appropriées, comme :

- ☑ l'adoption et la mise en œuvre de règles sur la Protection des Données ;
- ☑ l'adoption d'une approche « Protection des Données dès la conception et par défaut » ; la mise en place de mesures de Protection des Données tout au long du cycle de vie de nos opérations de traitement ;
- ☑ la mise en place de contrats écrits avec les organismes qui traitent des données personnelles en notre nom ;
- ☑ la tenue de la documentation de nos activités de traitement ;
- ☑ la mise en œuvre de mesures de sécurité appropriées ;
- ☑ l'enregistrement et, si nécessaire, la communication de violations de données personnelles ;
- ☑ la réalisation d'analyses d'impact relatives à la Protection des Données pour les utilisations de données personnelles présentant des risques élevés pour les intérêts des individus ;
- ☑ la désignation d'une Data Protection Officer ;
- ☑ et l'adoption de codes de conduite pertinents et la ratification de schémas de certification (si possible).

- ☑ Nous évaluons et mettons à jour nos mesures relatives à la responsabilité à intervalles appropriés.

Documentation

Qu'est-ce que la documentation ?

Nous devons tenir un registre de nos activités de traitement, qui couvrent des domaines tels que les finalités du traitement, et le partage et la conservation de données : c'est ce que nous appelons la **documentation**.

Il est important de documenter nos activités de traitement : cette exigence légale peut appuyer une bonne gouvernance des données et nous permettre de prouver notre conformité aux autres composantes du RGPD et aux lois relatives à la Protection des Données en vigueur.

Liste de vérification :

Documentation des activités de traitement – exigences

- ☑ En qualité de responsable de traitement des données personnelles que nous traitons, nous documentons toutes les informations applicables en vertu de l'Article 30(1) du RGPD.
- ☑ Nous documentons nos activités de traitement par écrit.
- ☑ Nous documentons nos activités de traitement de façon granulaire avec des liens significatifs entre les différentes informations.
- ☑ Nous examinons régulièrement les données personnelles que nous traitons et mettons à jour notre documentation en conséquence.

Documentation des activités de traitement – bonnes pratiques

- ☑ Nous documentons nos activités de traitement sous format électronique de façon à pouvoir ajouter, supprimer et modifier des informations facilement.

En nous préparant à documenter nos activités de traitement, nous :

- ☑ effectuons des audits d'informations pour connaître les données personnelles détenues par notre entreprise ;
- ☑ utilisons des questionnaires par le biais de nos outils relatifs au numérique, à la sécurité et à la confidentialité, et communiquons avec le personnel de toute l'entreprise pour acquérir une vue plus complète de nos activités de traitement ;
- ☑ et évaluons nos politiques, directives, procédures, contrats et accords pour couvrir des domaines comme la conservation, la sécurité et le partage des données.

Dans le cadre de notre registre des activités de traitement, nous documentons, ou relions à de la documentation, les éléments suivants :

- ☑ les informations requises pour les mentions d'information ;
- ☑ les registres de consentements, si nécessaire ;
- ☑ les contrats entre responsables de traitement et sous-traitants des données ;
- ☑ l'emplacement des données personnelles ;
- ☑ les rapports d'Analyses d'impact relatives à la Protection des Données ;
- ☑ et également les registres de violations de données personnelles ;
- ☑ les registres des demandes d'exercice de droit des personnes concernées.

Où se trouve notre documentation sur la Protection des Données ?

ONE
Fonction Globale
Protection des données

Privacy & Data Protection

« La protection des données concerne - et est de la responsabilité de - tous les salariés de notre entreprise »

Contenu

- Lois et réglementations
- Information et sensibilisation
- Meilleures pratiques et politiques

ONE
Communauté
Réseau de la protection des données

Data Protection Network

« Nous sommes tous des acteurs de la protection des données personnelles »

Contenu

- Politique relative à la protection des données personnelles
- Système de gestion de la protection des données
- Législation locale
- Ressources humaines
- Numérique mondial
- Légalité et conformité
- Audit et contrôle internes
- GBU & Commercial
- Innovation, R&D
- Sécurité Globale
- Assurance et gestion des risques

OneTrust
Logiciel de gestion de la protection de la vie privée

OneTrust
Privacy Management Software
@ ROQUETTE

« Notre outil de gestion de la vie privée dédié à la sécurité de la vie privée et aux risques liés aux tiers »

Modules

CULTURE → CONFORMITÉ → RESPONSABILITÉ

Analyse d'impact relative à la Protection des Données

L'**Analyse d'impact relative à la Protection des Données** (**PIA**) est un processus visant à décrire le traitement, à évaluer sa nécessité et sa proportionnalité, et à faciliter la gestion des risques pour les droits et libertés des personnes physiques associés au traitement des données personnelles en les évaluant et en déterminant les mesures pour y remédier.

L'acronyme « **PIA** » est utilisé indifféremment pour désigner l'**Analyse d'impact sur la vie privée** (**AIPV**) et l'**Analyse d'impact relative à la Protection des Données** (**AIPD**).

Comment réalise-t-on une AIPD ?

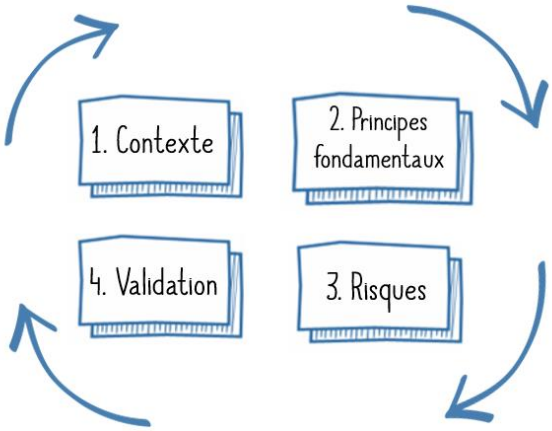
L'approche de conformité mise en œuvre par la réalisation d'un PIA repose sur deux piliers :

1) les **droits et principes fondamentaux**, « non négociables » et imposés par la loi, qu'il faut respecter, indépendamment de la nature, la sévérité et la probabilité des risques ;
2) la **gestion des risques relatifs à la vie privée des personnes concernées**, qui détermine les contrôles techniques et organisationnels appropriés pour protéger les données personnelles.

Approche de conformité basée sur un AIPD

En résumé, pour réaliser une AIPD, il faut :

1) définir et décrire le contexte du traitement des données personnelles à l'examen ;
2) analyser les contrôles garantissant la conformité aux principes fondamentaux : la proportionnalité et la nécessite du traitement, ainsi que la protection des droits des personnes concernées ;
3) évaluer les risques sur la vie privée associés à la sécurité des données et s'assurer qu'ils sont traités correctement ;
4) documenter formellement la validation du PIA à la lumière des faits antérieurs ou décider de réviser les étapes précédentes.



Approche générale de la réalisation d' une AIPD

Puisqu'il s'agit d'un processus d'amélioration continue, il nécessite parfois plusieurs itérations pour obtenir un système de Protection de la Vie Privée acceptable. Il demande également un contrôle des changements dans le temps (au niveau du contexte, des contrôles, des risques, etc.), par exemple tous les ans, ainsi que des mises à jour lorsque se produit un changement significatif.

L'approche doit être mise en œuvre dès la conception d'un nouveau traitement des données personnelles. La mise en œuvre de cette approche dès le départ permet de déterminer les contrôles nécessaires et suffisants à effectuer et, de ce fait, d'optimiser les coûts. Inversement, la mise en œuvre après la création du système et de la mise en œuvre des contrôles peut amener à remettre en question les choix opérés.

Nos responsabilités :

- Si un type de traitement qui utilise notamment les nouvelles technologies présente des risques élevés pour les droits et libertés des personnes physiques, et en tenant compte de la nature, du champ d'application, du contexte et des finalités de ce traitement, Roquette, en qualité de responsable de traitement, doit réaliser une analyse de l'impact des opérations de traitement envisagées sur la Protection des Données Personnelles avant le traitement.
- Le chef du projet doit demander conseil auprès du Data Protection Officer désigné lors de la réalisation d'une Analyse d'impact relative à la Protection des Données.

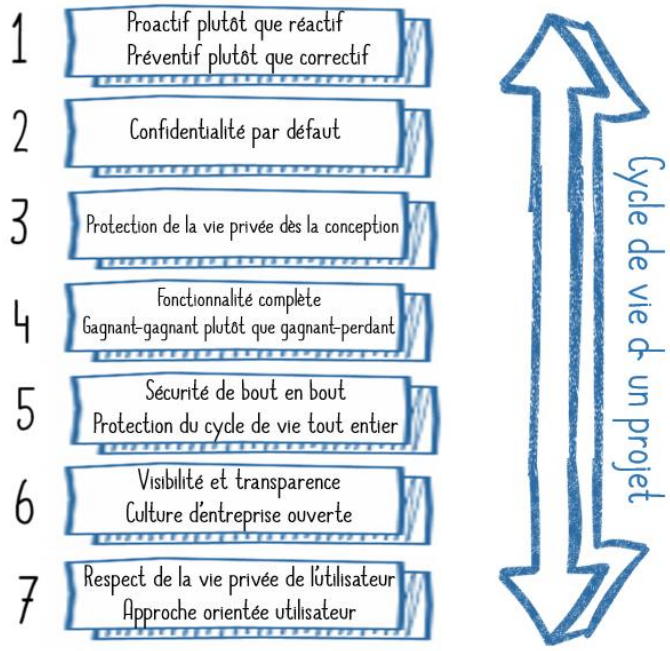
Règles	Référence Q-Docs	Référence RGPD
• Réaliser un PIA en cas de haut risque	DDPG003EN Règle 1	Art. 35
• Contenu d'un PIA	DDPG003EN Règle 2	
• Tâches du DPO en matière de PIA	DDPG003EN Règle 3	
• Examen de PIA	DDPG003EN Règle 4	

Nos collaborateurs sont formés et procédures internes améliorées.

- Formations à propos de Security & Privacy Review dans Projects & Contracts.
- Formation sur notre plateforme de e-learning.
- CNIL Analyse d'impact relative à la Protection des Données, La méthode, Édition février 2018 - https://www.cnil.fr/fr.

Protection de la Vie Privée dès la conception et par défaut

La **Protection de la Vie Privée dès la conception** consiste à intégrer le respect de la vie privée dans la conception, l'exécution et la gestion d'un système, d'un processus commercial ou d'une spécification de conception en particulier.



Qu'est-ce que la Protection des données dès la conception ?

La législation sur la Protection des Données inclut des principes de base concernant la Protection de la Vie Privée des personnes concernées.

La Protection des Données dès la conception et par défaut permet de nous assurer que les systèmes d'informations que nous utilisons respectent ces principes de la Protection des Données et qu'ils protègent les droits des personnes concernées.

Nous considérons que :

Roquette s'appuie sur les systèmes d'informations et les bases de données pour effectuer toute une série de tâches administratives et opérationnelles. La plupart de ces systèmes d'informations traitent des données personnelles. Leur totale conformité à la réglementation revêt donc une importance capitale.

Les entreprises qui prennent les problèmes associés à la Protection des Données au sérieux inspirent confiance.

De vigoureuses mesures de Protection des Données représentent ainsi un avantage concurrentiel.

L'engagement de la direction joue un rôle crucial quant à la décision d'appliquer les principes de la Protection des Données dès la conception dans les approvisionnements et le développement de logiciels de l'entreprise.

La direction doit également s'assurer de fournir suffisamment de ressources pour cette tâche.

Prendre en compte la Protection des Données tout au long du processus de développement est à la fois rentable et plus efficace que d'apporter des changements à un logiciel existant.

Nos responsabilités :

Dans le cadre du RGPD, la Protection des Données dès la conception est, pour la première fois, devenue une obligation légale. Ceci signifie qu'il faut prendre en compte la Protection des Données et de la Vie Privée dans les spécifications de conception et l'architecture des systèmes et technologies de l'information et de la communication.

En qualité de responsable de traitement, Roquette doit se conformer aux exigences régissant la Protection des Données dès la conception durant le développement de logiciels et la commande de systèmes, de solutions et de services.

Il faut également inclure ces exigences en conséquence lorsque nous concluons des contrats avec des fournisseurs et recourrons à des consultants (voir nos standards avec les sous-traitants).

Règle	Référence Q-Docs	Référence RGPD
• Sécurité, Protection des Données et de la Vie Privée dès la conception et par défaut	DDPG007EN Règle 3	Art. 25

Liste de vérification :

- ☑ Examiner l'Analyse d'impact relative à la Protection des Données (AIPD)
- ☑ Éviter, limiter ou minimiser le besoin de collecter et de traiter des données personnelles sensibles
- ☑ Limiter et minimiser l'exposition de fonctionnalités superflues et de données personnelles dans l'interface utilisateur
- ☑ Anonymiser ou pseudonymiser les données personnelles dans la mesure du possible
- ☑ Tous les paramètres de confidentialité doivent être configurés par défaut
- ☑ Le suivi d'un site Web à un autre doit être désactivé par défaut
- ☑ Retirer le consentement via un menu dans le logiciel. Garder à l'esprit que la collecte de données personnelles doit cesser en cas de retrait du consentement
- ☑ Les paramètres doivent apparaître dans un menu où la personne concernée doit activement les « modifier » en toute conscience pour abaisser leur niveau de confidentialité
- ☑ Le suivi d'appareils doit être désactivé par défaut

Nos collaborateurs sont formés !

- Guidelines sur notre Communauté « Data Protection Network ».
- Méthodologie : Examen de la sécurité et de la conformité dans les projets et les contrats.
- Formation sur notre plateforme de e-learning.

Notification de violation de données

Qu'est-ce qu'une violation de données personnelles ?

La **violation de données personnelles** désigne une infraction liée à la sécurité entraînant la destruction, la perte ou l'altération, accidentelles ou illégales, la publication non autorisée des données personnelles transmises, stockées ou traitées de toute autre manière, ou leur accès non autorisé.

*Cela signifie qu'une violation est plus qu'une simple **perte** de données personnelles.*

Exemples :

- Perte d'une base de données client
- Divulgation d'une évaluation des performances des employés

Nos responsabilités :

Nous devons appliquer les règles pour traiter toute violation de données personnelles de façon à limiter son impact sur les personnes concernées et à éviter que ce problème ne se reproduise.

Règles	Référence Q-Docs	Référence RGPD
• Notification d'une violation de données personnelles à la Data Protection Officer	DDPG008EN Règle 1	Art. 33
• Notification d'une violation de données personnelles à l'autorité de contrôle	DDPG008EN Règle 2	
• Communication d'une violation de données personnelles à la personne concernée	DDPG008EN Règle 3	Art. 34

A qui s'adresser en cas de violation de données personnelles ?

Veuillez contacter la Data Protection Officer à dpo@Roquette.com ainsi qu'à l'adresse d'alerte confidentielle de Roquette alert@Roquette.com.

Dans quel délai devons-nous signaler une violation ?

Nous devons notifier une violation auprès de l'autorité de contrôle sans retard injustifié, au plus tard 72 heures après en avoir pris connaissance.

De quelles violations devons-nous informer l'autorité de contrôle compétente ?

Nous ne devons informer l'autorité de contrôle compétente d'une violation que si celle-ci présente un risque pour les droits et libertés des individus. Si nous n'y remédions pas, une telle violation peut porter fortement préjudice aux individus. Par exemple :

- discrimination ;
- atteinte à la réputation ;
- pertes financières ;
- ou perte de confidentialité ou tout autre préjudice majeur d'ordre économique ou social.

Nous devons l'évaluer au cas par cas et devons être en mesure de justifier notre décision de signaler une violation auprès de l'autorité de contrôle.

Quand faut-il notifier les individus ?

Si une violation présente un **risque élevé** pour les droits et libertés des individus, nous devons directement en notifier les personnes concernées sans retard injustifié.

Le devoir de notifier un individu d'une violation ne s'applique pas si :

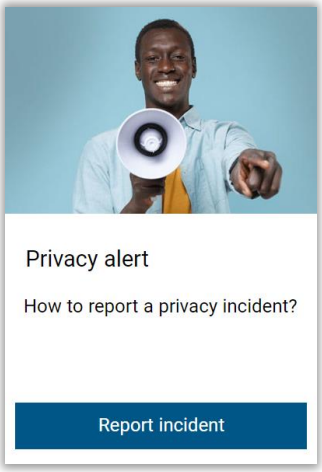
- nous avons mis en œuvre des mesures techniques et organisationnelles appropriées qui ont été appliquées aux données personnelles affectées par la violation ;
- nous avons pris des mesures ultérieures qui préviendront la survenue de tout nouveau risque élevé pour les droits et libertés des individus ;
- cela nécessitait des efforts disproportionnés.

Dans le cas où la communication d'une violation nécessiterait des efforts disproportionnés, nous devons rendre l'information accessible aux individus d'une façon tout aussi efficace (communication publique, par ex.).

Qui contacter en cas de violation de données ?

Veuillez contacter le **Délégué à la Protection des Données** à l'adresse dpo@Roquette.com et/ou signaler l'incident au moyen de notre formulaire web "Alerte vie privée".
Si vous devez signaler une violation potentielle de la conformité, vous pouvez contacter votre point de contact habituel ou signaler un problème à l'aide du dispositif d'alerte confidentiel de Roquette : Speakup©.

SpeakUp



Suivi et examen

Nous considérons que :

Roquette s'engage à :

- ☑ garantir un **suivi** juridique et technologique des exigences en matière de Protection des Données,
- ☑ **examiner** et **améliorer** notre Système de Management de la Protection des Données (SMPD)

afin de prendre en compte les évolutions réglementaires et technologiques ainsi que les contraintes de services internes. [DDPG009EN]

Nos responsabilités :

Règles	Référence Q-Docs	Référence RGPD
• Garantir un suivi et un examen juridiques et technologiques en matière de Protection des Données Personnelles	DDPG009EN Règle 1	Bonnes pratiques
• Surveiller régulièrement la mise en œuvre du SMPD et des directives relatives à la Protection des Données	DDPG009EN Règle 2	
• Examiner régulièrement la politique relative à la Protection des Données Personnelles et la documentation du SMPD	DDPG009EN Règle 3	

Nos collaborateurs sont formés !

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Privacy & Data Protection News

Audit Management
Manage Internal/External Audits

Concevez et soutenez notre programme de Protection de la Vie Privée

Logiciel de recherche réglementaire :

Nous utilisons une plateforme qui fournit une série de solutions de Protection de la Vie Privée conçues pour nous aider à surveiller les développements réglementaires, atténuer les risques et parvenir à une conformité à l'échelle mondiale :

- ☑ Veille réglementaire
- ☑ Comparatifs des traitements transfrontaliers
- ☑ Guides pratiques
- ☑ Portail RGPD
- ☑ Modèles et listes de vérification
- ☑ Service « Analyse d'expert »
- ☑ Recherche juridique

Audit et examen du Système de Management de la Protection des Données :

Nous réalisons des audits internes afin de déterminer si les contributions au SMPD sont :

- ☑ en conformité aux exigences de ce Guide, de la Politique et de la loi ou des réglementations applicables ;
- ☑ effectivement mises en œuvre et tenues à jour ;
- ☑ et effectuées comme prévu.

Nous réalisons un examen de la gestion du SMPD pour nous assurer que le champ d'application reste adéquat et que des améliorations dans le processus du SMPD puissent être identifiées.

Pour ce faire, les contributions sont les suivantes :

- ☑ Objectifs, contrôles, processus et procédures du SMPD ;
- ☑ Résultats d'audits et de contrôles de conformité précédents ;
- ☑ Retour des parties intéressées ;
- ☑ Techniques, produits ou procédures, qui pourraient être utilisés dans l'entreprise pour améliorer les performances et l'efficacité du SMPD ;
- ☑ Statut des actions préventives et correctives ;
- ☑ Vulnérabilités ou menaces non réglées de façon adéquate lors de la précédente évaluation des risques ;
- ☑ Résultats des mesures de l'efficacité ;
- ☑ Actions de suivi en fonction des examens de gestion précédents ;
- ☑ Tout changement susceptible d'affecter le SMPD ;
- ☑ Et recommandations d'amélioration.

Documents de référence

- [Code de conduite] Code de conduite du Groupe Roquette
- [GDPG001EN] Définitions relatives à la protection des données
- [MDPG001EN] Manuel sur la protection des données personnelles
- [DDPG001EN] Directive sur la culture du respect de la vie privée et de la protection des données
- [DDPG002EN] Directive sur la licéité du traitement des données personnelles
- [DDPG003EN] Directive sur l'analyse d'impact relative à la vie privée
- [DDPG004EN] Directive sur le traitement des données sensibles
- [DDPG005EN] Directive sur les registres des activités de traitement
- [DDPG006EN] Directive sur le respect des droits des personnes
- [DDPG007EN] Directive sur la sécurité des données personnelles
- [DDPG008EN] Directive sur la notification d'une violation de données personnelles
- [DDPG009EN] Directive sur l'examen du système de gestion de la protection des données personnelles
- [DSUG001EN] Directive sur la protection des données
- [DSUG006EN] Directive sur la gestion de la cyber-sécurité
- [DSUG016EN] Directive sur la sécurité des sous-traitants

Bibliographie

[Charte européenne] Charte des droits fondamentaux de l'Union européenne, 2010/C 83/02.

[RGPD] 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 abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

[Loi « Informatique et libertés »] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et ses modifications.

[WP29 – Directives] Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable de traitement ou d'un sous-traitant | WP 244 rév.01 (5 avril 2017).

[WP29- Directives] Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement 2016/679 | WP 248 rév.01 (13 octobre 2017).

[WP29- Directives] Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement 2016/679 | WP 253 (21 octobre 2017).

[WP29- Directives] Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement 2016/679 | WP 251 rév.01 (13 février 2018).

[WP29 – Directives] Lignes directrices concernant les Data Protection Officers (DPO) | WP 243 rév.01 (5 avril 2017).

[WP29- Directives] Lignes directrices sur la transparence au sens du règlement 2016/679 | WP260 rév.01 (11 avril 2018).

[WP29- Directives] Lignes directrices sur le consentement au sens du règlement 2016/679 | WP259 rév.01 (11 avril 2018).

[EDPB – Avis] Avis 23/2018 concernant les propositions de la Commission relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale (article 70.1.b) (26 septembre 2018).

[EDPB –Avis] Avis 28/2018 concernant le projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon (5 décembre 2018).

[EDPB – Avis] Avis 14/2019 sur le projet de clauses contractuelles types présenté par l'autorité de contrôle du Danemark (article 28(8) du RGPD) (12 juillet 2019).

[EDPB- Recommandation] Recommendation 01/2019 on the Draft List of the European Data Protection Supervisor Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 39(4) of Regulation (EU) 2018/1725) (10 July 2019) *(en anglais uniquement)*.

[EDPB – EDPS Réponse conjointe] EPDB-EDPS Joint Response to the LIBE Committee on the Impact of the US Cloud Act on the European Legal Framework for Personal Data Protection (Annex) (10 July 2019) *(en anglais uniquement)*.

[EDPB Avis] Opinion 13/2019 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR) (10 July 2019) *(en anglais uniquement)*.

Sources

- Commission Nationale de l'Informatique et des Libertés
    - https://www.cnil.fr/fr
    - Septembre 2019
    - Licence : CC-BY-ND 3.0 FR
- Information Commissioner's Office
    - https://ico.org.uk/
    - Septembre 2019
    - Publié sous Open Government Licence
- Union européenne
    - https://eur-lex.europa.eu
    - 1998-2019
- https://www.iso.org/fr/home.html
- https://www.dataguidance.com/
- https://www.onetrust.com/
- https://www.corporatefiction.fr/
- https://pixabay.com/fr/service/license/

La version anglaise de ce Guide est la version de référence.
Les traductions de ce document sont sujettes à diverses interprétations.
Première édition : Septembre 2019
Document publié par ROQUETTE FRÈRES
Conception éditoriale et graphique : Compliance Office
Photographie : libre de droits


ROQUETTE
Offering the best of nature™