



Le Livre Blanc de l'agence rgpd

Une expertise du réseau
Bras Droit des Dirigeants

2025



Pourquoi le RGPD a-t-il été adopté ?

La protection de la vie privée est un **droit fondamental** reconnu par la Déclaration Universelle des Droits de l'Homme de 1948.

Ce droit inclut la **protection du domicile**, la **confidentialité des correspondances**, le **secret médical** mais également la **protection des données personnelles**. Toute personne doit pouvoir contrôler ses informations privées et savoir ce qui en est fait.

Le développement du numérique a entraîné **l'émergence de pratiques malveillantes** portant atteinte aux données personnelles des citoyens.

En réaction à ce constat, la Loi informatique et liberté a été promulguée en France en 1978.

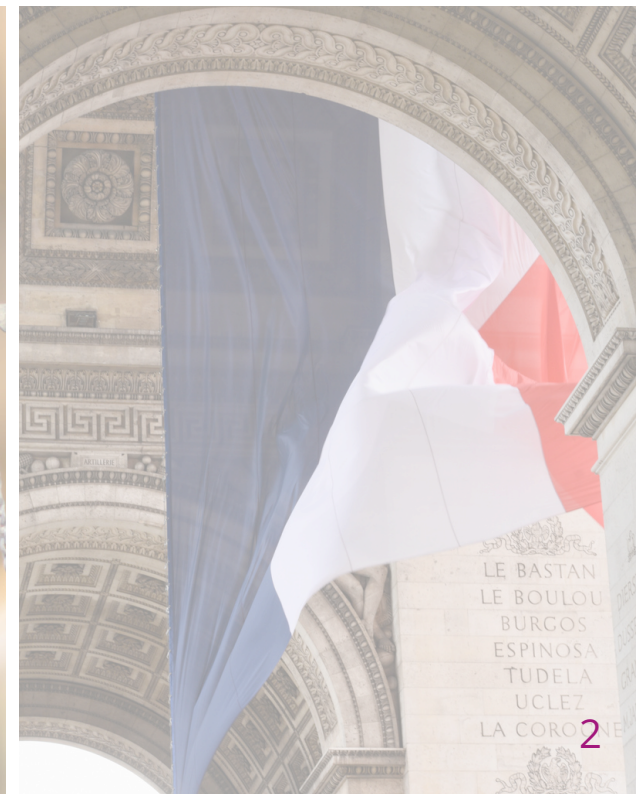
Le sujet devenant de plus en plus préoccupant, **le Règlement Général sur la Protection des Données (RGPD)** a été adopté en 2016 au niveau européen. Puis différents textes de lois plus spécifiques ont suivi.

Le RGPD harmonise le droit de l'ensemble des Etats membres pour permettre une **meilleure circulation des données** au sein de l'Union européenne (UE). Cette réglementation est **applicable depuis le 25 mai 2018**.

Êtes-vous concerné(e) ?

Le RGPD est applicable aux organismes **publics et privés** qui collectent et traitent des données personnelles. Il concerne **toutes les structures basées sur le territoire d'un Etat membre de l'UE** ou traitant des données personnelles de personnes physiques situées sur le territoire d'un Etat membre de l'UE.

Afin de leur permettre de conserver le **contrôle** sur leurs informations, le RGPD accorde également des **droits** aux personnes dont les données sont traitées.



Qu'est ce qu'un traitement ? Qu'est qu'une donnée à caractère personnel ?

Un **traitement** correspond à toute **opération** réalisée sur une ou plusieurs **données à caractère personnel**

Une **donnée à caractère personnel** est une information se rapportant à **une personne physique identifiée ou identifiable, directement ou indirectement**



Exemples de traitements de données personnelles

Il est souvent difficile de déterminer ce qui peut être un traitement de données personnelles ou non.

Voici quelques exemples :

- Collecter des informations sur un client pour un rendez-vous ;
- Traiter des candidatures pour un recrutement ;
- Faire un formulaire sur un site internet pour être contacté ;
- Accéder à la géolocalisation du véhicule d'un employé ;
- Disposer d'extraits de casier judiciaire ;
- Récolter des informations d'un compte bancaire pour un paiement ;
- Installer un dispositif de vidéosurveillance ;
- Faire une photographie où une ou des personnes apparaissent ;
- Disposer d'informations sur les hobbies ou la vie familiale d'une personne.

Attention : certaines données sont considérées comme sensibles. Leur recueil est interdit sauf exception.



Il s'agit notamment de :

- L'origine raciale et ethnique ;
- Les opinions ou politiques ;
- Les convictions religieuses, philosophiques ou l'appartenance syndicale ;
- Les données biométriques afin d'identifier la personne de manière unique ;
- Les données concernant la santé ;
- Les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ;
- Les informations relatives aux condamnations pénales et infractions ;
- Le numéro de sécurité sociale.

Principe de Licéité et Loyauté

Pour être licite, le traitement doit être fondé sur une des 6 bases légales. La loyauté implique le respect des engagements pris envers les personnes concernées à propos du traitement (Art 5 RGPD).

Principe de transparence

Les personnes concernées doivent être informées des conditions du traitement. Cette information doit être concise, transparente, compréhensible et accessible (Art 5-12-13-14 RGPD).

Principe de Finalité

Le traitement doit être effectué dans un objectif déterminé. Celui-ci doit être explicite, légitime et limité (Art 5 du RGPD)

Quelles sont les grands principes du RGPD ?

Le RGPD pose des grands principes qui guident le RT tout au long du traitement

Durée de conservation limitée

Les données ne doivent pas être conservées pour une durée excédant celle nécessaire à la réalisation de l'objectif justifiant le traitement. (Art 5 RGPD)

Principe de minimisation et d'exactitude

Doivent être traitées uniquement les données pertinentes au regard des finalités pour lesquelles elles sont traitées (ART 5 RGPD). Toutes les données inexacts doivent être effacées ou rectifiées (Art 5 RGPD)

Principe de Sécurité

Le RT et le ST doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques et aux besoins. (Art 5 RGPD)

Quels sont les principaux acteurs du RGPD?

Le Responsable de Traitement (RT)

Le RT est l'acteur principal du traitement. Il détermine les **finalités** et les **moyens** du traitement et est responsable vis-à-vis personnes concernées et à la CNIL.

Le RT doit veiller au respect du RGPD par son personnel et les sous-traitants qu'il sollicite.

Le contrat de sous-traitance permet d'encadrer les obligations de chacun.



Le Sous-Traitant (ST)

Le ST traite les données à caractère personnel **pour le compte du RT.**

Le RGPD s'appliquant à l'ensemble de la chaîne économique, si le ST fait appel à un prestataire, il doit veiller à ce que son ST applique les obligations qu'il doit lui-même respecter.



Le Délégué à la protection des données (DPO)

Le DPO a pour mission de **conseiller** les acteurs du traitement, de **contrôler** le respect de la réglementation, de **coopérer** avec l'autorité de contrôle et d'être le **point de contact** des personnes concernées.

Le DPO peut être **interne** à l'entreprise ou **externalisé**.



La personne concernée (PC)

La PC est la **personne dont les données personnelles sont traitées.**

Elle dispose de droits :

- Sur ses données (droit d'accès, de rectification, d'oubli, de portabilité)
- Sur les traitements (droit de limitation, de retrait du consentement, d'opposition).



Focus : Comment encadrer les transferts vers des pays en dehors de l'UE ?

Le RGPD est un texte européen, mais s'applique au delà de l'Union Européenne.

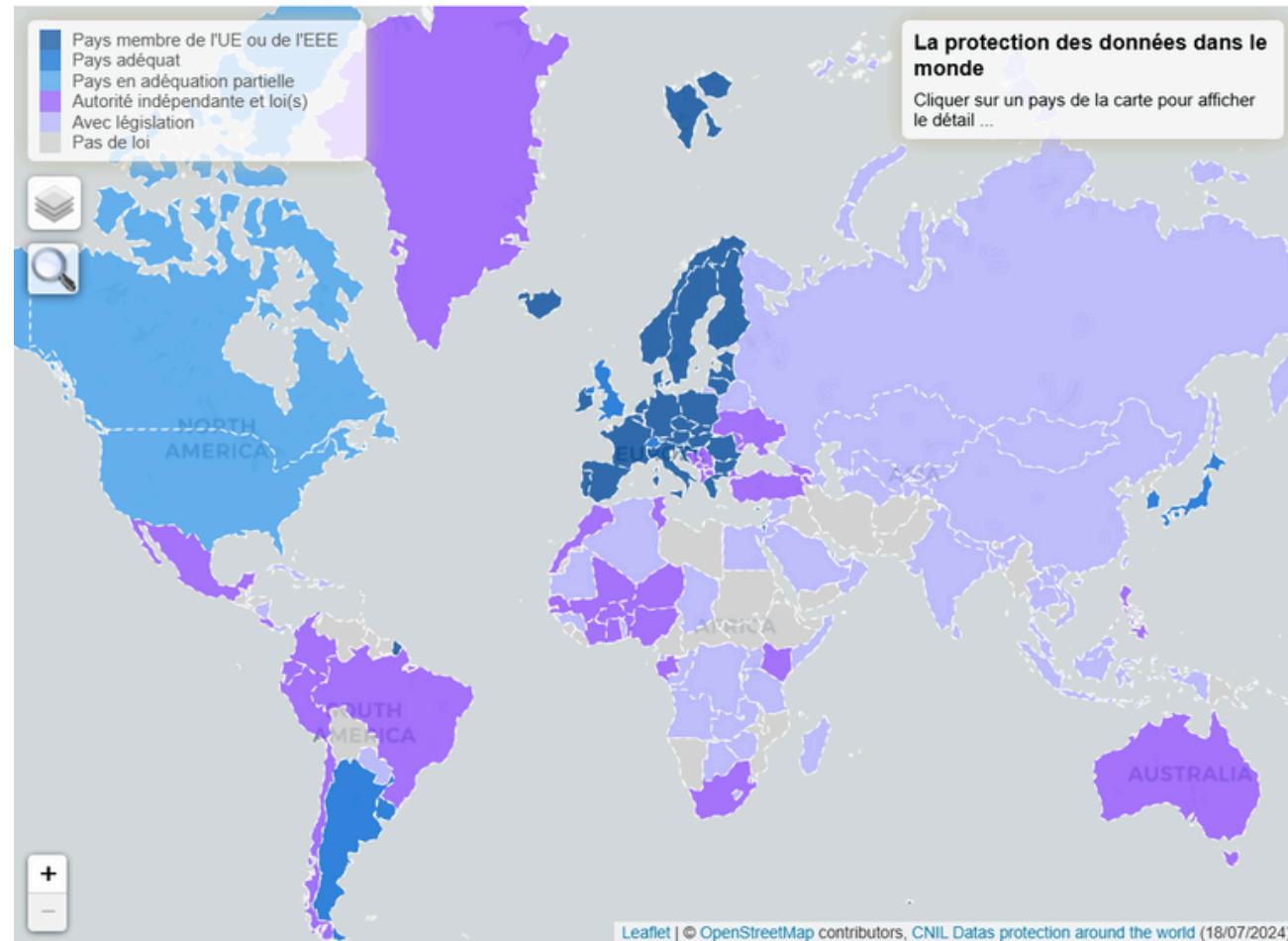
En tant que responsable de traitement, **vous devez encadrer les transferts de données que vous ou vos sous-traitants pourraient effectuer vers des pays en dehors de l'UE.**

En fonction du niveau d'adéquation du pays, des mesures complémentaires de sécurisation du traitement doivent être prises.

D'autres pays tiers ont adopté des législations sur la protection des données de leurs citoyens. C'est le cas du Brésil avec la **LGPD**, ou de la Californie avec le **Data Consumer Privacy Act** depuis 2020. Il est important de se conformer à ces législations si vous devez traiter des données provenant de ces pays.

Cependant, ce n'est pas parce qu'un pays dispose d'une législation qu'il est forcément adéquat aux yeux de l'UE.

Afin de savoir quels pays sont considérés comme adéquats ou non, la CNIL a mis en place une **carte interactive**.



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

Comment puis-je assurer au mieux la mise en conformité de mon entité ?

Une mise en conformité porte sur plusieurs domaines bien distincts :

Juridique



Organisationnel



Processuel



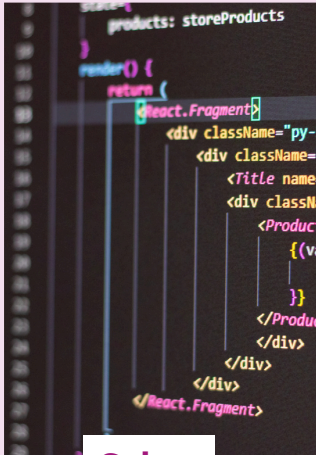
Le recensement



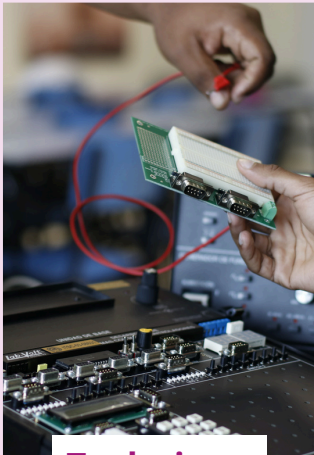
Le tri



Cyber



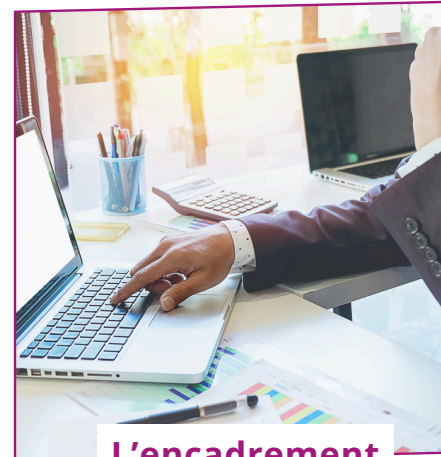
Technique



Informatique



L'encadrement



La sécurisation



Cependant, être en conformité à un instant "T" ne suffit pas. La conformité est une notion qui s'évalue dans la durée. Il est donc indispensable de développer des méthodes permettant une protection des données à caractère personnel de manière constante. La mise en conformité est une démarche active et continue.

Quelles mesures peuvent être mises en place ?



Organisation et documentation

- Recenser tous les traitements de données
- Déterminer les finalités, bases légales, durées de conservation, ...
- Tenir un registre des violations de données
- Mettre en place une procédure de déclaration à la CNIL et d'information des personnes concerné



Sécurité informatique et physique

- Avoir une politique de mots de passe
- Protéger les équipements avec des antivirus, VPN, ...
- Protéger les réseaux informatiques et les serveurs
- S'assurer que les documents contenant des données personnelles soient dans une zone fermée à clé
- Installer un dispositif de badges d'entrée ou de limitation d'accès



Conformité et droits des personnes

- Mettre en place une procédure de réponse à l'exercice des droits des personnes concernées
- Informer les personnes concernées du traitement de leurs données
- Encadrer les transferts de données vers l'étranger



Sensibilisation

- Former ses salariés sur la protection des données

Mais ce ne sont pas les seules ! Enormément de critères sont à prendre en compte en fonction de votre structure et de vos traitements.

Quels sont les risques en cas de non respect des dispositions ?

Impact sur les personnes concernées :

Tout incident de sécurité ayant un impact sur les données personnelles traitées représente un risque pour les droits et libertés des personnes concernées. Selon la gravité du risque, le responsable de traitement peut avoir l'obligation de le notifier à la CNIL dans les **72h**.

Sanctions :

Le RGPD a renforcé les sanctions prévues. En cas de non-respect du RGPD, des amendes administratives peuvent être prononcées, pouvant atteindre les **20 Millions d'€ ou 4% du CA annuel**. Des sanctions pénales peuvent également être prononcées, pouvant atteindre **5 ans d'emprisonnement et/ ou 300 000€ d'amende**.

Exemple de manquements constatés par la CNIL :

Un géant de la navigation a écopé d'une amende de 50 Millions d'euros pour manque de transparence.

Une importante compagnie Aérienne a dû déboursé plus de 200 Millions d'euros suite aux négligences de l'entreprise ce qui a entraîné le vol de données personnelles de passagers.

Une entreprise allemande a été condamnée à payer 9,55 Millions d'euros pour ne pas avoir su protéger les données de ses clients dans le cadre de son service client téléphonique.

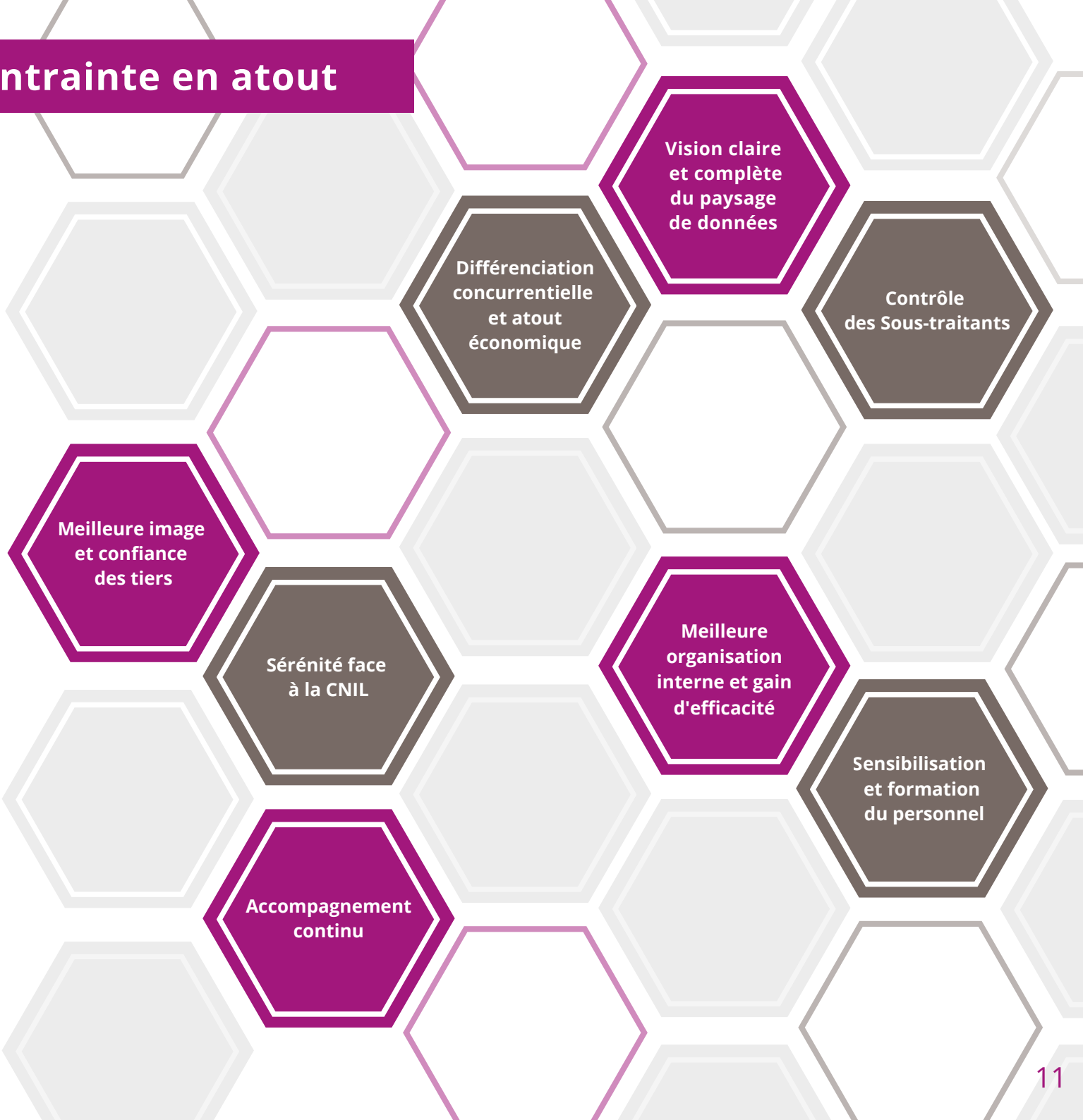
Transformez une contrainte en atout

Ce règlement est souvent perçu comme une contrainte pour les entités concernées. Pourtant, il peut constituer une **réelle valeur ajoutée**.

Être conforme au RGPD est un **gage de qualité**, et permet ainsi de **renforcer son image** et la **confiance** de vos clients et partenaires.

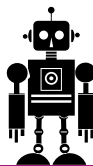
Il offre aussi aux entités concernées l'opportunité de réorganiser leurs activités pour avoir un réel encadrement des responsabilités, une meilleure gestion des données traitées, et ainsi gagner en efficacité.

Il est donc dans votre intérêt de vous assurer de votre conformité RGPD



L'intelligence artificielle est partout : elle nous recommande quoi regarder, anticipe nos besoins, répond à nos questions. Mais derrière cette facilité se cache une complexité juridique et éthique essentielle.

Le RGPD (Règlement général sur la protection des données) ne s'oppose pas à l'IA, il encadre son développement pour éviter les dérives. Voici comment garantir une IA responsable et conforme, que vous soyez développeur, utilisateur ou décideur.



Les technologies d'IA posent des risques concrets :

- **L'effet boîte noire** : si l'algorithme est incompréhensible, l'obligation de transparence prévue par le RGPD concernant les techniques de traitement n'est pas respectée.
- **Les biais cachés** : une IA formée sur des données déséquilibrées peut discriminer sans que cela soit volontaire ; cela viole le principe de traitement équitable.
- **Les fuites involontaires** : les IA génératives peuvent révéler des données sensibles à partir de leurs modèles ; une mauvaise configuration peut exposer des informations confidentielles.

Les réflexes à adopter pour rester conforme

Pour limiter ces risques, voici des actions concrètes :

- **Informier simplement, mais complètement** : pas besoin de jargon technique ; expliquez clairement comment l'IA utilise les données et pour quelle finalité.
- **Sécuriser les données par défaut** : l'anonymisation ou la pseudonymisation doit être intégrée dès les premières étapes du projet.
- **Auditer régulièrement** : vérifiez les performances, les biais et les comportements inattendus ; des tests et corrections doivent être planifiés.
- **Documenter pour mieux protéger** : tenez un registre complet des traitements, des risques identifiés, des mesures de sécurité et des incidents éventuels.
- **Concevoir avec la vie privée en tête** : le "privacy by design" n'est pas un gadget : c'est une méthode pour anticiper les risques au lieu de les corriger après coup.

Rappel utile : plus l'IA est complexe, plus votre responsabilité est grande.

L'IA ne doit pas être une boîte noire pour vous.

Côté utilisateur :

comment rester maître de ses données ?

Voici vos leviers :

- **Ne partagez que le nécessaire** : plus de données = plus de risques ; donnez uniquement ce qui est utile.
- **Lisez les règles** : les politiques de confidentialité peuvent paraître longues, mais elles révèlent comment l'outil gère vos informations.
- **Exigez des garanties** : utilisez des outils d'IA reconnus, conformes au RGPD et vérifiés par des tiers.
- **Utilisez vos droits Accès, rectification, effacement...** Le RGPD vous donne le pouvoir de contrôler ce que l'IA connaît de vous.
- **Restez vigilant** : signalez les usages suspects à l'éditeur ou à la CNIL ; votre vigilance est une barrière essentielle contre les abus.

Une IA responsable, c'est possible !

Le RGPD n'est pas un frein à l'innovation :

c'est un levier pour bâtir une IA digne de confiance. Les entreprises qui intègrent ces principes dès le début conçoivent des outils mieux acceptés, plus durables, et alignés avec les valeurs sociétales.

Conclusion ?

Et si nous vous disions que ce sujet sur l'IA a été rédigé à l'aide de l'IA... vous y croiriez ? 😊

RGPD + Cybersécurité : maîtriser ses traitements, renforcer sa défense

Face à l'explosion des cybermenaces, sécuriser les données n'est plus simplement un bon réflexe : c'est une exigence réglementaire et une responsabilité stratégique. Le RGPD agit comme un pare-feu juridique, en imposant des normes élevées de sécurité, de documentation et de gouvernance. Combiné aux bonnes prat

**Le RGPD :
la base pour une
sécurité cohérente**

La conformité RGPD ne se limite pas à éviter les sanctions : elle permet de cartographier précisément l'ensemble des traitements de données dans une organisation. Cette vision claire des flux, des finalités et des risques est indispensable pour prendre les bonnes décisions techniques et stratégiques en cybersécurité.

➡ **Sans maîtrise des traitements, il est impossible de sécuriser efficacement. Le RGPD structure cette connaissance, et offre au DSI un socle solide pour orienter ses choix technologiques.**

RGPD et cybersécurité ? Des chiffres qui parlent !

ENJEUX	CHIFFRES CLÉS 2024
Sanctions RGPD	87 décisions, 55,2M€ d'amendes
Coût d'une violation	4,3M€ en moyenne par entreprise
Violations quotidiennes	16 par jour (hausse de 29%)
Attaques par rançongiciel	30,2% des entreprises concernés
Risques évités	Jusqu'à 219 M€ grâce au RGPD
Notifications à la CNIL	5 919 violations notifiées
DPO référenciés	34 440 en France

Comment articuler RGPD et cybersécurité ?

ACTION	RÔLE DU DPO	RÔLE DU DSI
Mesure technique (Art. 32 RGPD)	Conseil sur les choix	Mets en œuvre les solutions
Analyse d'impact (AIPD)	Supervise le processus	Fournit les données et mesures
Politiques internes & sensibilisation	Rédige, coordone	Définit les pratiques sécurisées
Tests d'intrusion, journalisation	Documente, suit les écarts	Exécute et analyse les tests
Gestion des incidents	Qualifie le risque, informe la CNIL	Contient l'incident, sécurise les systèmes

RGPD + Cybersécurité : maîtriser ses traitements, renforcer sa défense

Conclusion ?

Grâce au RGPD, les organisations disposent d'une vision claire et documentée des traitements, permettant une cybersécurité alignée sur les vrais enjeux. Ce duo RGPD + cybersécurité ne protège pas seulement des attaques : il renforce la gouvernance, la confiance des clients et la compétitivité sur le long terme.

À RETENIR :
**Conformité = Résilience
+ Maîtrise + Confiance**

"On ne sécurise bien
que ce qu'on comprend
parfaitement."

Courriels professionnels : Les salariés ont le droit de tout savoir ?

En 2025, la jurisprudence renforce **le droit d'accès** des salariés à leurs courriels professionnels. Qu'ils soient licenciés ou démissionnaires, les collaborateurs peuvent désormais récupérer leurs échanges, contenu et métadonnées inclus. Cette évolution majeure rééquilibre les relations de travail et garantit aux salariés les moyens de défendre leurs droits... Mais ce droit est-il sans limite ?

Ce qui change

La Cour de cassation a confirmé le 18 juin 2025 que les messages échangés via la messagerie professionnelle constituent **des données personnelles** au sens du RGPD (article 4) ; le salarié dispose donc **d'un droit d'accès** à leur contenu et aux métadonnées (horodatage, expéditeurs, destinataires) les concernant.

Fondements juridiques

Le droit d'accès du salarié repose sur **l'article 15 du RGPD**, qui permet à toute personne de demander la communication des données la concernant, et sur la définition des données personnelles de **l'article 4 RGPD**, désormais officiellement étendue aux contenus et métadonnées des emails professionnels.

Modalités pratiques

Pour exercer ce droit, il convient d'adresser **une demande écrite** précisant la période visée, les types de messages recherchés ou des mots-clés. L'employeur peut fournir :

- Soit une **copie intégrale** des courriels, à condition de ne pas porter atteinte aux droits des tiers ;
- Soit un **tableau** listant les métadonnées et les données personnelles contenues dans chaque échange, conformément aux recommandations de la CNIL.

La première communication doit être **gratuite** et intervenir **sous un mois**.

Accès aux courriels professionnels : les limites

Respect de la vie des tiers	L'employeur doit veiller à ne pas divulguer d'informations concernant d'autres salariés, clients ou partenaires. Avant de transmettre les courriels, il peut occulter ou anonymiser les données relatives à des tiers afin de protéger leur vie privée.
Exclusion des messages strictement personnels	Les courriels identifiés comme strictement personnels (par exemple, comportant la mention « personnel » ou « privé » dans l'objet) ne sont pas concernés par le droit d'accès, sauf en cas de nécessité avérée et sous contrôle du juge. Si l'objet personnel concerne la personne en demande, ce mail a de toute façon vocation à être supprimé dès son départ de la structure si cela n'a pas été fait avant.
Refus des demandes abusives	Les demandes manifestement abusives, trop larges, répétitives ou infondées peuvent être refusées par l'employeur, conformément aux recommandations de la CNIL.
Limitation à la durée de conservation	L'accès est limité aux courriels conservés dans le respect des durées légales de conservation des données. Les messages supprimés ou dont la conservation n'est plus justifiée n'ont pas à être fournis.
Protection des intérêts de l'entreprise	L'employeur peut refuser la communication d'informations sensibles dont la divulgation pourrait porter atteinte à la sécurité.
Recours au DPO ou à la CNIL en cas de doute	En cas de situation complexe ou de conflit d'intérêts, il est recommandé de solliciter l'avis du Délégué à la protection des données (DPO) ou de la CNIL pour garantir un équilibre entre le droit d'accès du salarié et la protection des autres droits fondamentaux.

Importance pour le salarié

Ce droit donne aux salariés des preuves solides pour contester un harcèlement, une discrimination ou un licenciement abusif devant les conseils de prud'hommes. Il participe à un véritable équilibrage des rapports de force entre employeur et collaborateur, en assurant la transparence et la loyauté des échanges professionnels.

Bonnes pratiques à adopter

Il est recommandé aux salariés de trier et d'archiver régulièrement leurs messages, notamment avant toute procédure disciplinaire ou départ de l'entreprise. Transférer ses emails privés vers une messagerie personnelle ou exporter ses dossiers facilite l'exercice ultérieur du droit d'accès. Les employeurs, quant à eux, gagneront à mettre en place une procédure interne claire de gestion des mails par les salariés pour faciliter le traitement de ces demandes dans les délais impartis



Quiz de positionnement

Où en êtes-vous dans votre conformité RGPD ?

1 - Savez-vous ce qu'est un traitement de données à caractère personnel ?	a) ☐ Oui b) ☐ Non
2 - Savez-vous ce qu'est un registre des traitements ?	a) ☐ Oui b) ☐ Non
3 - Connaissez-vous les 8 informations de base à noter dans un registre de traitement ?	a) ☐ Oui b) ☐ Non
4 - Faites-vous attention pour chaque traitement de ne collecter que les données strictement nécessaires, déterminez vous toujours les modalités de leur conservation et destruction ?	a) ☐ Oui b) ☐ Non
5 - Déterminez-vous clairement, notamment par contrat, les responsabilités de chaque acteur (responsable de traitement, sous-traitant, ou coresponsable de traitement) et vérifiez-vous bien que leurs obligations sont remplies ?	a) ☐ Oui b) ☐ Non
6 - L'entrée de vos locaux est-elle verrouillée (code, badge) et encadrez-vous la venue des visiteurs?	a) ☐ Oui b) ☐ Non

7 - Avez-vous une politique d'accès aux données ?	a) ☐ Oui b) ☐ Non
8 - Avez-vous une charte informatique ?	a) ☐ Oui b) ☐ Non
9 - Êtes-vous capable de mettre en place le chiffrement, la pseudonymisation, l'anonymisation de données lorsque cela est nécessaire ?	a) ☐ Oui b) ☐ Non
10 - Sécurisez-vous l'informatique (antivirus, firewall, VPN...) ?	a) ☐ Oui b) ☐ Non
11 - Savez-vous à quoi correspond une violation de données ?	a) ☐ Oui b) ☐ Non
12 - Informez-vous suffisamment les personnes concernées chaque fois que vous traitez leurs données (nature des données traitées, le traitement effectué, l'identité du responsable de traitement, les modalités d'exercice de leurs droits...) ?	a) ☐ Oui b) ☐ Non
13 - Êtes-vous capable de permettre aux personnes concernées d'exercer leurs droits dans les délais requis ?	a) ☐ Oui b) ☐ Non

14 - Sur votre site internet, permettez-vous aux visiteurs de consentir ou non aux cookies, et de retirer leur consentement aussi facilement ?	a) ☐ Oui b) ☐ Non
15 - Transférez-vous des données hors UE ?	a) ☐ Oui b) ☐ Non
16 - Si oui, êtes-vous capable d'assurer la sécurité de ce transfert ?	a) ☐ Oui b) ☐ Non
17 - Avez-vous mis en place des mesures techniques et organisationnelles me permettant de maintenir la conformité de mon entité dans le temps et démontrer mon « accountability »	a) ☐ Oui b) ☐ Non
18 - Savez-vous ce qu'est un DPO (Délégué à la Protection des Données) ?	a) ☐ Oui b) ☐ Non
19 - Avez-vous pu déterminer si vous étiez concerné par l'obligation de désignation d'un DPO ?	a) ☐ Oui b) ☐ Non
20 - Si oui, avez-vous procédé à sa désignation ?	a) ☐ Oui b) ☐ Non

21 - Avez-vous mis en place un calendrier de sensibilisation / formation de votre personnel en matière de RGPD pour inculquer / maintenir les bonnes pratiques ?	a) ☐ Oui b) ☐ Non
22 - Un des membres de votre personnel vous informe que son poste a été piraté, et que certaines adresses email de vos clients ont été publiées sur internet. Que faites-vous ?	a) ☐ Je débranche immédiatement le poste et j'appelle le DSI pour l'informer de la situation, je documente la violation dans mon registre, et en fonction de mon évaluation du risque, je notifie à la CNIL ; b) ☐ Je jette le poste par la fenêtre, et l'employé avec (ni vu ni connu) c) ☐ Je débranche immédiatement le poste et j'appelle le DSI pour l'informer de la situation, je notifie à la CNIL, et je notifie à toutes les personnes concernées l'existence de cette violation et ses potentielles conséquences.

Vos résultats ?

Moins de 5 réponses a)	Entre 5 et 15 réponses a)	Entre 16 et 22 réponses a)
RGP... Quoi ? Le RGPD a encore beaucoup de secrets pour vous. Lui accorder de l'attention peut pourtant vous apporter bien plus que vous ne le pensez ! En effet, au-delà de la contrainte légale qu'il peut représenter, il vous apportera une optimisation de votre organisation et de l'utilisation de vos données. Sans parler de la sécurisation indispensable de votre système d'information. N'attendez plus et accordez à votre entité la valeur qu'elle mérite en contactant l'Agence RGPD, afin de bénéficier d'un accompagnement efficace et d'un outil intuitif pour assurer sereinement votre conformité RGPD.	Oui c'est bon je suis conforme... enfin je crois... On passe à autre chose ? Et bien pas tout à fait. Vous avez amorcé quelques actions, et c'est déjà une très bonne initiative, bravo ! Mais pourquoi s'arrêter en si bon chemin ? Contactez l'Agence RGPD pour maîtriser pleinement votre conformité RGPD et faire de cette vague notion quelque chose de concret et de réellement bénéfique pour votre entité, et ce dans la durée. Il vous reste encore du travail mais vous avez déjà manifesté votre volonté de mettre les bonnes actions en place, et nous pouvons vous aider à optimiser cette initiative pour renforcer votre conformité RGPD.	Je suis un pro du RGPD, j'ai tout mis en place, C'est bon, je suis tranquille ? Félicitations, vous avez pris beaucoup d'initiatives pour tenter d'appliquer correctement le RGPD. Mais comment être sûr que vos actions sont suffisantes, ou correctement mises en places, ou encore bien appliquées par vos équipes ? L'Agence RGPD vous permet d'avoir une vision objective de votre organisation, et conforme aux exigences de la CNIL. De même, une conformité à un instant T ne suffit pas. Il est important de savoir la maintenir, et l'Agence RGPD est à vos côtés pour assurer ce maintien de votre conformité RGPD.

N'y a-t-il que le RGPD ?

Si le **RGPD** est l'un des plus grands règlements, d'autres textes (présents ou futurs) sont aussi à prendre en compte en fonction souvent de la taille de la structure.

Il est important de s'y intéresser, car ils peuvent **impacter votre structure (ou vous-même)** directement ou indirectement.

Cela va être le cas de la **Loi CADA, du DGA, de la directive NIS II, de la Loi Sapin, de la directive Police-Justice, de l'IA Act, du Cyber Resilience Act**, etc...

Pour plus d'informations sur ces textes, vous pouvez consulter :

- Le site de la CNIL
- Le site de l'ANSSI
- Le site de la CADA
- Le site de l'Agence Française Anticorruption
- ...

Directive Police-Justice

Directive (UE) 2016/680 du 27 avril 2016

Cette directive faisait partie, avec le RGPD, du “**paquet européen de protection des données à caractère personnel**”. Elle a été transposée avec la modification de la Loi Informatiques et Libertés.

Cette directive s'applique en **matière pénale**, ou pour des actions en amont d'une éventuelle infraction pénale, et concerne en particulier les activités menées par la police dans ses missions de prévention, constatation, détection, ou encore gestion des mesures d'application des peines.

Seuls les traitements effectués par les “autorités compétentes” entrent dans le champ d'application.

Elle est assez proche du RGPD concernant les obligations qu'elle apporte, mais prévoit également des spécificités.

Pour plus d'informations :

<https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t>.

Directive NIS 2

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (Texte présentant de l'intérêt pour l'E

Cette directive est entrée en vigueur en **octobre 2024**.

La **directive NIS 2** est une nouvelle réglementation européenne qui s'appuie sur les acquis de la **directive NIS 1** (adoptée en 2016) et qui vise à apporter une protection au niveau européen contre les acteurs malveillants, notamment concernant les moyens de production des entreprises et administrations de l'UE, ainsi que des régimes de sanctions.

Cette directive concerne de nombreux acteurs, allant des **TPE/PME** aux **administrations** : environ **600 types d'entités différentes**.

Pour plus d'informations, vous pouvez consulter la page dédiée sur le site de l'ANSSI :

<https://cyber.gouv.fr/la-directive-nis-2>.

Data Governance Act

Ce règlement est applicable depuis **septembre 2023**. Il vise à être l'une des premières pierres concernant le partage des données personnelles et non personnelles en mettant en place des structures d'intermédiation.

Concrètement, cela signifie mettre en place un espace européen unique des données dans lequel les données pourraient être utilisées.

Cela permet aux TPE/PME et petites entreprises d'avoir un meilleur accès aux données en évitant un effet de verrouillage, notamment concernant les partages de données par le secteur public.

Pour plus d'informations :

<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022R0868>.

Data Act

Ce règlement est entré en vigueur le **11 janvier 2024**.

Il a vocation à **faciliter l'accès aux données sur le marché de l'Union**. Ainsi, l'objectif est de :

- Baisser les prix des services après-vente liés aux dispositifs intelligents (en vous permettant de choisir n'importe quel service de réparation) ;
- Avoir de nouvelles possibilités d'utiliser des services reposant sur l'accès aux données ;
- Améliorer l'accès aux données recueillies ou générées par un appareil ;
- Pour le secteur public, accéder aux données du secteur privé et les utiliser pour faire face aux "urgences publiques" (inondations ou incendies de forêt par exemple).

Pour plus d'informations :

https://commission.europa.eu/news/data-act-enters-force-what-it-means-you-2024-01-11_fr.

La loi CADA

La loi CADA met en place le principe de l'**Open data** au sein des administrations.

Elle oblige les **administrations** avant tout, et permet aux administrés d'avoir accès aux documents administratifs (dans la limite des règles applicables).

Pour plus d'informations :

<https://www.cnil.fr/fr/ouverture-et-reutilisation-de-donnees-personnelles-sur-internet-la-cnil-publie-ses-recommandations>



Loi du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal

Loi SAPIN 2

Loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et la modernisation de la vie économique

La **loi Sapin II** a apporté de nombreuses nouveautés :

- Le déploiement de dispositifs anti-corruption;
- La protection des lanceurs d'alerte;
- Des règles sur les finances.

Elle concerne **toutes les entreprises**, mais s'applique surtout aux **grandes sociétés** et aux **administrations**.

Appliquer les dispositifs prévus par cette loi est un atout pour les entreprises, notamment concernant la mise en place des dispositifs anti-corruption.

L'Agence française anticorruption a publié des recommandations pour sa mise en œuvre :

<https://www.agence-francaise-anticorruption.gouv.fr/files/files/Recommandations%20AFA.pdf>

Mais ce n'est pas tout !

Digital Markets Act

IA Act

Règlement sur la cyberrésilience (CRA)

DSA

DMA

Loi numérique (SREN)

et bien d'autres...

A background image showing two people in business attire shaking hands. The image is partially obscured by a white semi-transparent banner that contains the text. The banner has purple triangular accents at the top-left and bottom-right corners.

**Pour toute question sur votre mise en conformité,
désormais,
vous savez qui contacter**

agence rgpd

Une expertise du réseau
Bras Droit des Dirigeants



contact@agencergpd.eu



<https://www.agencergpd.eu/>