Mission RGPD

BAROMÈTRE
DE LA CONFORMITÉ RGPD DES PME ET ETI

EN PARTENARIAT AVEC :

visiativ SIMON ASSOCIÉS

Édition **2024**

Sommaire

Avant-propos

Baromètre de la conformité RGPD des PME et ETI

Découvrez la **première édition du baromètre** de la conformité RGPD (Réglement Général sur la Protection des Données personnelles) des PME et ETI.

Mission RGPD, la plateforme qui s'occupe de la conformité RGPD des PME et ETI, a rassemblé ici les statistiques de 330 diagnostics réalisés sur l'année 2023.

Contexte réglementaire

En 2018, est entré en application le Règlement Général sur la Protection des Données personnelles (RGPD), marquant une étape cruciale dans la protection de la vie privée et des données personnelles à l'ère du numérique. La conformité RGPD est obligatoire pour toutes entreprises ou organisations européennes traitant des données personnelles, c'est à dire 100% des PME - ETI en France et en Europe. Le RGPD est né de la nécessité de répondre aux défis posés par l'évolution rapide des technologies et de la société, ainsi que de renforcer la confiance des individus dans le traitement de leurs données. Son objectif principal est de renforcer les droits des personnes en leur donnant davantage de contrôle sur leurs données personnelles, tout en imposant des obligations claires aux organisations qui les collectent et les traitent. Le RGPD a été adopté pour instaurer un cadre juridique harmonisé au niveau européen, afin de simplifier les règles et de garantir une protection cohérente des données personnelles dans l'ensemble de l'Union européenne (UE) et à l'échelle mondiale pour les citoyens européens. L'arrivée de ce réglement pour les PME et ETI fut un véritable enjeu tant stratégique, commercial que juridique et opérationnel impliquant des ressources humaines, financières et compétences nécessaires pour se conformer puis piloter cette conformité dans le temps.

Enjeux stratégiques

La conformité au RGPD sert ainsi les enjeux stratégiques des PME et ETI :

- **La cybersécurité**, en adoptant les mesures techniques et organisationnelles obligatoires afin de sécuriser les données.
- **La performance commerciale**, en justifiant du respect des normes au sein des produits et services proposés.
- **La responsabilité morale, sociétale et juridique (RSE)**, en prenant en compte les préoccupations des personnes concernées en matière de protection de leurs données personnelles et respect de la vie privée.

Les risques RGPD pour les PME et ETI

Risque d'amendes

Imaginez-vous recevoir une note de 20 millions d'euros ou **4% de votre chiffre d'affaires mondial** en amendes RGPD ! Oui, cela peut arriver si vous ne suivez pas les règles. En plus de cette amende XXL, vous pourriez recevoir des ordres stricts de se conformer, avec une amende journalière allant jusqu'à 100 000 euros.

Ça fait beaucoup d'argent à sortir de la poche, non ? Et croyez-nous, mieux vaut investir dans la croissance de votre entreprise que dans des amendes. En France, il s'agit d'un montant d'amendes cumulés de **89 millions € en 2023 et 594 millions € depuis 2019**, concernant toutes sortes d'entreprises, des petites aux grandes.

Risque commercial

Une mauvaise pub qui colle à la peau ! Si vous vous faites pincer, la sanction financière ou la mise en demeure pourrait devenir une affaire publique. Imaginez le choc de vos clients en découvrant cela ! En plus, ils pourraient se **plaindre à la CNIL et laisser des avis négatifs** sur Internet.

Ce n'est **pas le top pour votre réputation**, avouez ! De nos jours, de plus en plus de partenaires commerciaux demandent la conformité **RGPD avant de signer des contrats**. Ne pas être en règle, c'est risquer de perdre de gros contrats. Et on sait que cela peut faire fuir les clients existants et freiner l'arrivée des nouveaux.
Une réputation ternie, ce n'est pas facile à rattraper !

Risque RH

Vos salariés risquent de bouder ! Ne pas respecter le RGPD peut aussi **amener vos employés à déposer des plaintes** (surtout les anciens collaborateurs qui ne seraient pas partis en très bon terme...). Ils se sentiraient trahis si leurs données personnelles ne sont pas correctement protégées et si leurs droits ne sont pas respectés.

Risque cybersécurité

Les données personnelles, que vous possédez au sein de votre entreprise, sont de l'or pour les hackers ! Ne l'oubliez jamais, votre entreprise est une cible de choix. Ignorer le RGPD, c'est comme leur laisser la porte ouverte de votre entreprise. **Fuites de données, incidents, et autres mauvaises surprises sont au rendez-vous.**

Et parfois l'incident doit être signalé à la CNIL et communiqué publiquement, ce qui n'arrange pas votre réputation ni la confiance de vos clients. Cela peut coûter cher de gérer les incidents de cybersécurité et les pertes de données. Sans parler des dommages financiers et juridiques que cela peut entraîner. **Protégez-vous ! Juridiquement aussi !**

Risque pénal

Oui, vous avez bien lu ! Pas très tentant, n'est-ce pas ?

Bon, ce n'est encore jamais arrivé ...
Mais attention, les manquements aux règles de protection de données font pratiquement tous l'objet de sanctions pénales pouvant aller jusqu'à 5 ans de prison et 300 000 euros d'amende pour les dirigeants et 1 500 000 euros d'amende pour la personne morale. La responsabilité de l'entreprise et du dirigeant peuvent être engagées. Le code pénal a introduit des dispositions et des infractions spécifiques aux règles issues du RGPD.

Nous avons décidé de mener étude pragmatique au plus proche de la réalité **des PME-ETI** afin de révéler le véritable niveau de conformité de ces entreprises, souvent méconnu des études existantes.

Ce baromètre apporte **une vision plus opérationnelle du tissu économique français concernant la maîtrise des risques RGPD**, en partageant le niveau de conformité des PME-ETI et en illustrant les mesures concrètes mises en place depuis 2018.

Bertrand Bucelle
CEO, Co-fondateur Mission RGPD

Méthodologie

Cette section décrit les méthodes de **330 diagnostics menés** auprès de **+ 850 entreprises et organisations**. Nos diagnostics adoptent une approche pragmatique basée sur la méthodologie suivante afin de garantir que les informations présentées soient précises et fiables.

Découvrez comment cette édition 2024 du Baromètre RGPD des PME et ETI a été réalisée.

Méthode de collecte de données

La méthode de collecte de données pour notre baromètre RGPD repose sur l'analyse des résultats de plus de 330 diagnostics menés auprès de plus de 850 entreprises et organisations. Ces diagnostics ont été réalisés en ligne via notre solution Mission Diag RGPD, une fonctionnalité gratuite de notre plateforme SaaS, Mission RGPD.

L'idée est simple : cette fonctionnalité gratuite permet aux entreprises et organisations de faire une première évaluation de leur conformité au RGPD en toute autonomie, et ce, en moins de 15 minutes.

Il est important de noter que toutes **les entreprises et organisations évaluées** pour ce baromètre **n'étaient pas clientes de nos services à ce moment-là**. Cela signifie que Mission RGPD ne les accompagnait pas à l'époque du diagnostic en ligne, et par conséquent, **nos services de mise et maintien en conformité n'ont pas influencé les résultats obtenus à ce stade.** En prenant en compte cette distinction, nous sommes en mesure de fournir des statistiques et des résultats qui reflètent fidèlement le niveau de conformité des PME et ETI, en toute objectivité sans biais lié à notre implication antérieure. Cette transparence renforce la crédibilité de nos données et garantit une analyse objective de la situation de conformité au RGPD des entreprises concernées.

Domaines d'analyses du Diag RGPD en ligne
• Analyse des profils d'entreprises évaluées
• Diagnostic de conformité des sites web
• Diagnostic de conformité aux droits des personnes : interne et externe
• Diagnostic de conformité aux obligations de sécurité des données
• Diagnostic de conformité des relations avec les sous-traitants
• Diagnostic de conformité des documents réglementaires
• Évaluation des freins à la mise en conformité au sein des PME et ETI

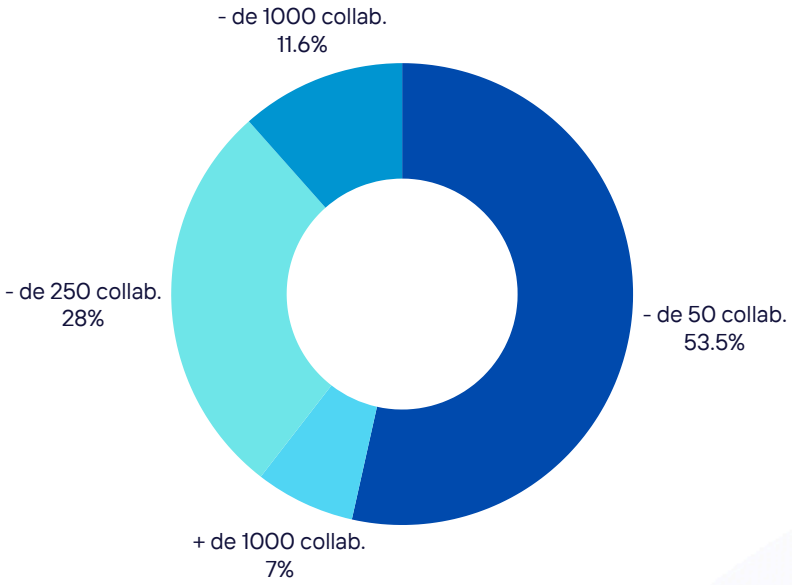
1 Profil d'entreprises évaluées

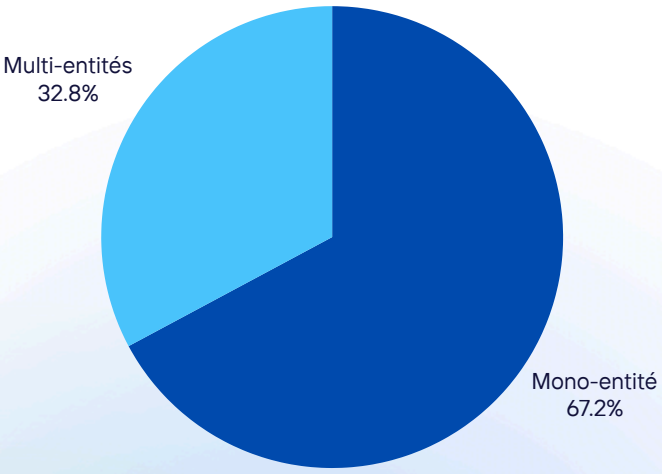
Taille d'entreprise

Découvrez la taille des entreprises et organisations analysées pour ce baromètre de la conformité RGPD.

53,5%
PME de moins de 50 collab.

32,8%
Multi-entités



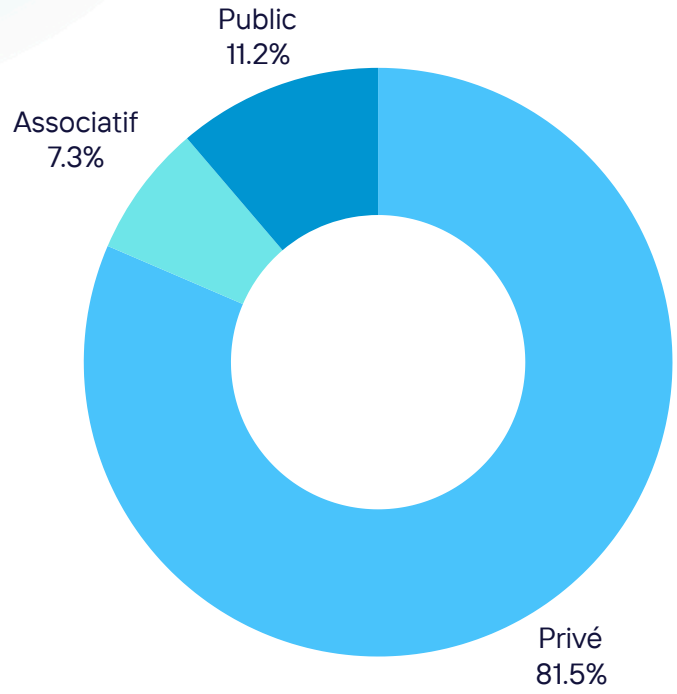


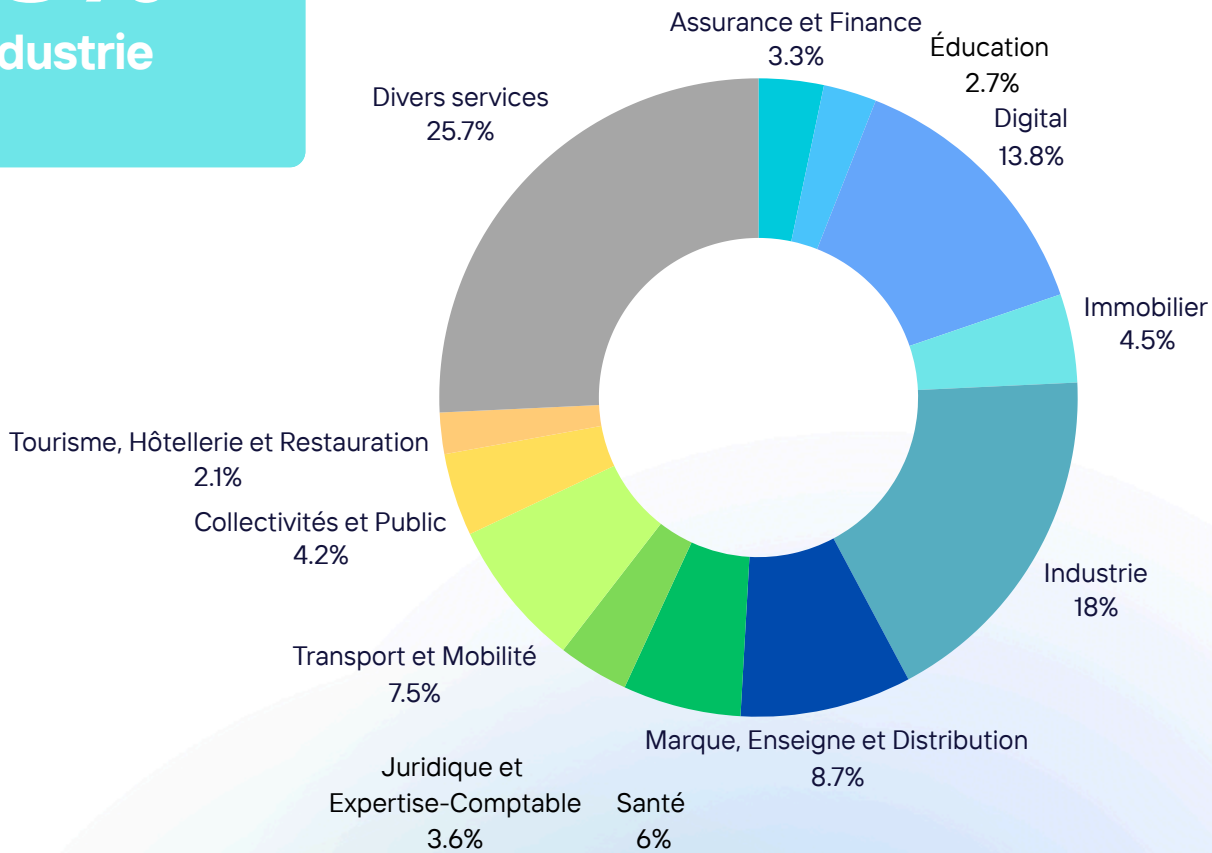
Secteurs d'activité

Découvrez les secteurs d'activité des entreprises et organisations analysées pour ce baromètre de la conformité RGPD.

81,5%
du secteur privé

18%
Industrie



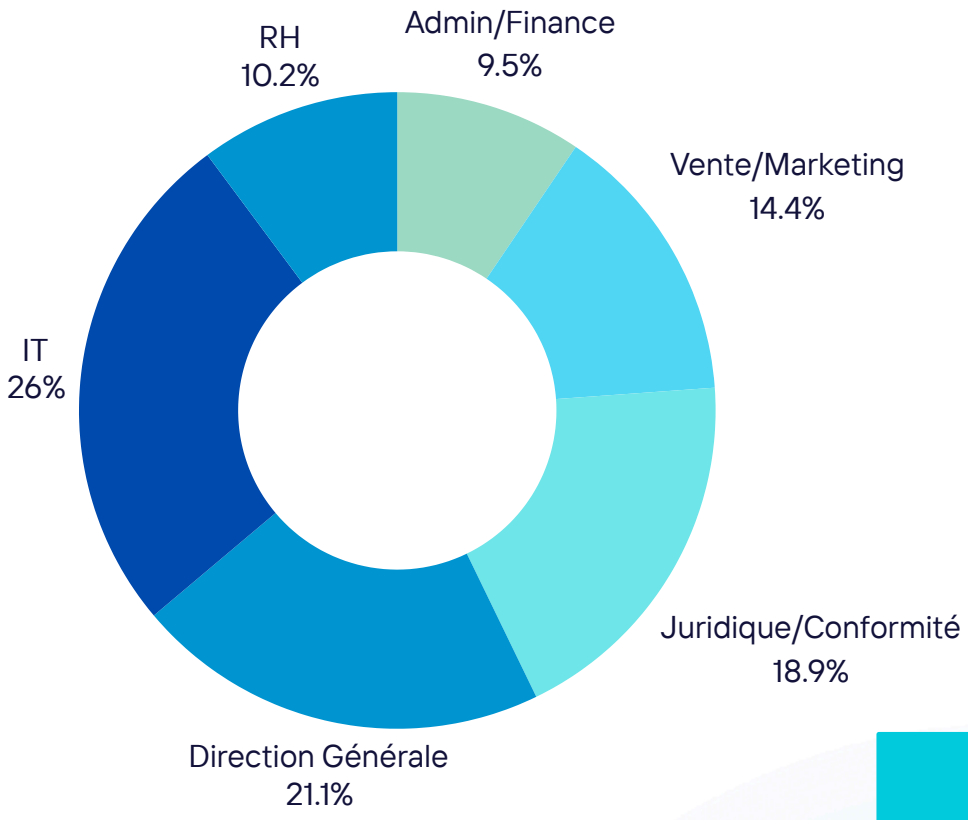


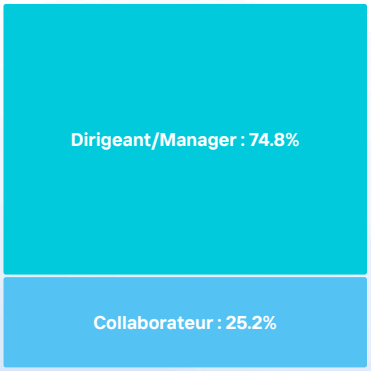
Fonction des interlocuteurs

Découvrez les profils des interlocuteurs qui ont répondu aux questionnaires de diagnostic RGPD.

26%
Profil IT

21,1%
Profil DG



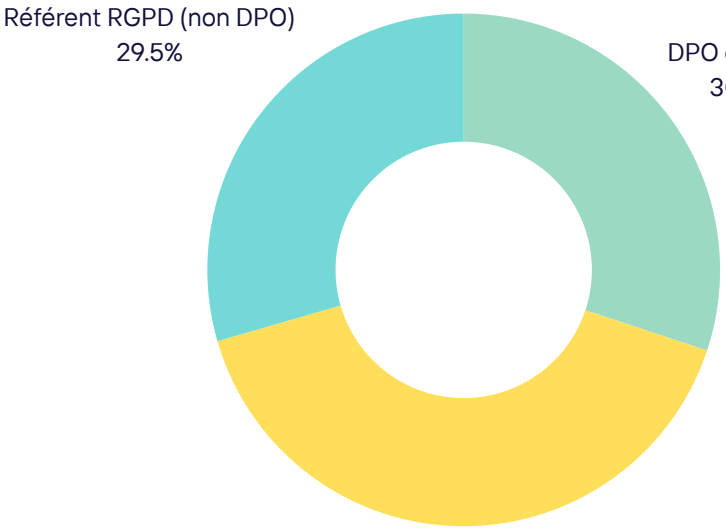


DPO ou Référent RGPD ?

Découvrez la répartition des entreprises et organisations qui ont décidé de désigner un DPO (Data Protection Officer ou Délégué à la Protection des Données).

40,4%

des PME et ETI n'ont pas nommé de personne en charge de la conformité RGPD



dont 56% sont seul sur ce projet et 44% travaillent avec des relais au sein des services de l'entreprise

À RETENIR

Pour rappel, la désignation d'un DPO auprès de la CNIL est obligatoire uniquement pour :

- Les autorités et organismes publics (par exemple, les ministères, collectivités territoriales, établissements publics).
- Les organismes dont les activités de base conduisent à réaliser un suivi régulier et systématique des personnes à grande échelle. Par exemple : les compagnies d'assurance ou les banques pour leurs fichiers clients, les opérateurs téléphoniques ou les fournisseurs d'accès internet.
- Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » (données biométriques, génétiques, relatives à la santé, la vie sexuelle, l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale) ou relatives à des condamnations pénales et infractions.

Source : CNIL – Règlement européen : le Délégué à la protection des données, c'est obligatoire ?

Néanmoins, la conformité RGPD est obligatoire pour 100% des entreprises et organisations en France et en Europe, ainsi il est fortement recommandé de nommer à minima un référent RGPD.

2 Score RGPD : Niveau de conformité des PME et ETI

Évaluation du niveau de conformité RGPD

Les résultats du Diag RGPD sont restitués sous forme de niveau de conformité déterminé selon le nombre de manquements aux obligations prévues par le réglement et selon la gravité des manquements détectés. Les niveaux de conformité sont gradués sur une échelle de taux de conformité (%) de 0 à 100, correspondant à un Score RGPD (A, B, C, D et E) associé à un code couleur.

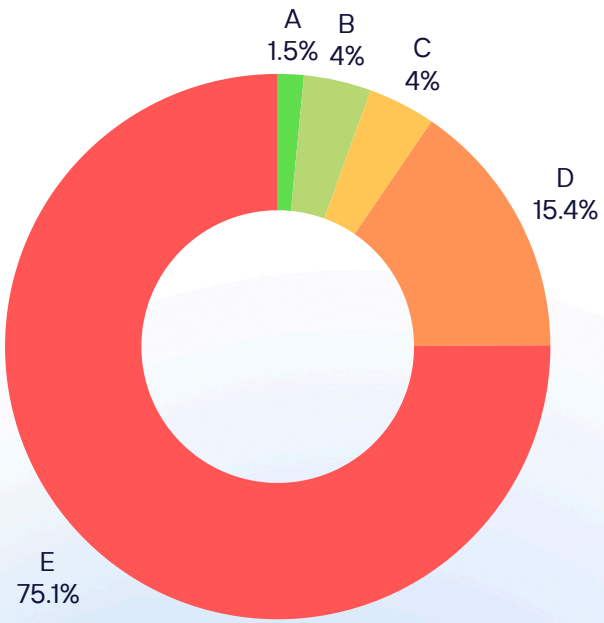
Découvrez la correspondance entre les taux de conformité associés aux Scores RGPD ci-contre.

Découvrez la répartition des Scores RGPD en % pour les entreprises et organisations évaluées lors de ces diagnostics.

- **A** — 99%-100% : Conformité optimale
- **B** — 85%-98% : Risque RGPD maitrisé
- **C** — 75%-84% : Risque RGPD détecté
- **D** — 50%-74% : Risque RGPD élevé détecté
- **E** — < 50% : Risque RGPD très élevé détecté

5,5%

des PME et ETI maitrisent les risques RGPD



Observations d'expert

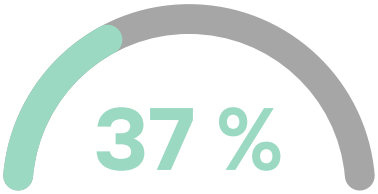
Le baromètre révèle que **5,5% des PME - ETI maîtrisent les risques RGPD**. Ces résultats mettent en lumière une forte difficulté face à une réglementation qui impacte tous les domaines de l'entreprise : des ressources humaines jusqu'aux activités commerciales.

Actuellement, **94.5% des entreprises évaluées sont exposées à de nombreux risques**, tant dans leurs activités en France que dans leurs opérations à l'échelle européenne. Il est crucial pour ces entreprises de réaliser un diagnostic complet de la conformité de leurs activités afin de corriger puis maintenir des activités conformes au RGPD.

Ce baromètre est un outil précieux qui nous permet de mieux **identifier les failles existantes**, d'en **comprendre les raisons** et d'**élaborer des solutions pour y remédier** afin d'accompagner les PME et ETI dans la maitrise des risques RGPD.

Aymeric Guyard
CRO, Co-fondateur Mission RGPD

3 Conformité des sites web



Source : Rapport annuel 2023 - CNIL

des contrôles CNIL, en 2023, se sont fait en ligne

La conformité au RGPD des sites web est particulièrement sensible pour les PME et les ETI, car elle impacte directement leur activité et présente une exposition forte aux risques :

- **Source de collecte de données** : Les sites web sont souvent des canaux de collecte de données majeurs, que ce soit via des cookies, des formulaires de contact ou des transactions en ligne. Le RGPD impose des règles strictes sur la manière dont ces données sont collectées, traitées et stockées.
- **Image de l'entreprise** : Le site web est souvent la première impression que les clients potentiels ont d'une entreprise. Respecter les normes et réglementations, y compris le RGPD, renvoie une image positive de l'entreprise, démontrant son engagement envers la protection de la vie privée et la sécurité des données.
- **Influence sur les décisions d'achat** : Dans un monde de plus en plus numérique, les clients B2C et B2B se tournent vers les informations en ligne pour prendre leurs décisions d'achat. Un site web respectueux de la vie privée et conforme au RGPD peut renforcer la confiance des clients et influencer positivement leur décision d'achat, ou dans le cas contraire, freiner le cycle d'achat.
- **Exposition aux risques** : Les sites web sont exposés à un risque élevé de non-conformité en matière de RGPD en raison de la quantité de données personnelles collectées et traitées. Les plaintes des visiteurs ou des consommateurs, ainsi que les contrôles des autorités compétentes comme la CNIL, peuvent entraîner des sanctions financières et une atteinte à la réputation de l'entreprise.
- **Contrôles de conformité en ligne** : La CNIL et d'autres autorités effectuent de plus en plus de contrôles en ligne pour vérifier la conformité des sites web aux règles du RGPD. Ces contrôles peuvent porter sur les informations fournies aux utilisateurs, les données collectées, les cookies utilisés et les mesures de sécurité mises en place.

Résultats et Statistiques

Découvrez l'analyse des diagnostics de sites web réalisés dans le cadre de l'évaluation de la conformité RGPD des PME et ETI menée par Mission RGPD.

89,7%
des sites web collectent des données personnelles

98,4%
d'entre eux ne sont pas conformes au RGPD

Sources de collecte de données personnelles des sites web

Explorez les différentes sources de collecte de données personnelles des sites web analysés lors des diagnostics de conformité RGPD menés auprès des PME et ETI, par Mission RGPD.

89,8%
des sites web comportent un formulaire de contact

37,8%
des sites web comportent un formulaire d'inscription à une liste de diffusion/newsletter

96,3%
des sites web comportent des cookies (traceurs)

27%
des sites web vendent en ligne (B2B et/ou B2C)

31%
des sites web intègrent un compte client ou un compte utilisateur

Formulaire de collecte : Information des personnes sur l'usage et la protection de leurs données personnelles

Dans le cas de collecte de données personnelles par formulaire de contact, lors de vente en ligne, création d'un compte utilisateur ou d'inscription à une newsletter, **des mentions RGPD** doivent figurer au bas de **chaque formulaire** de collecte **avec un renvoi vers une politique de confidentialité.**

45%

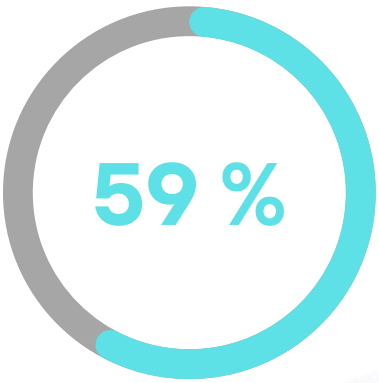
des sites web ne contiennent pas les mentions d'informations obligatoires sur les formulaires de collecte

41,29%

des politiques de confidentialité, ne sont pas conformes au RGPD

Cookies : consentement et information des personnes

Dans le cas de cookies (traceurs) sur un site web, l'internaute doit avoir la possibilité via un "bandeau cookies" d'accepter ou refuser avec simplicité, de paramétrer à tout moment le dépot de cookies (publicitaire, statistiques, réseaux sociaux) et d'être correctement informé de la présence de ces derniers.



des "bandeaux cookies" (lorsqu'ils sont présents) ne sont pas conformes au RGPD

À RETENIR

En 2023, 1 sanction RGPD sur 3 prononcée par la CNIL concerne soit un manquement à l'information des personnes et/ou un manquement à l'obligation de consentement en matière de cookies.

Observations d'expert

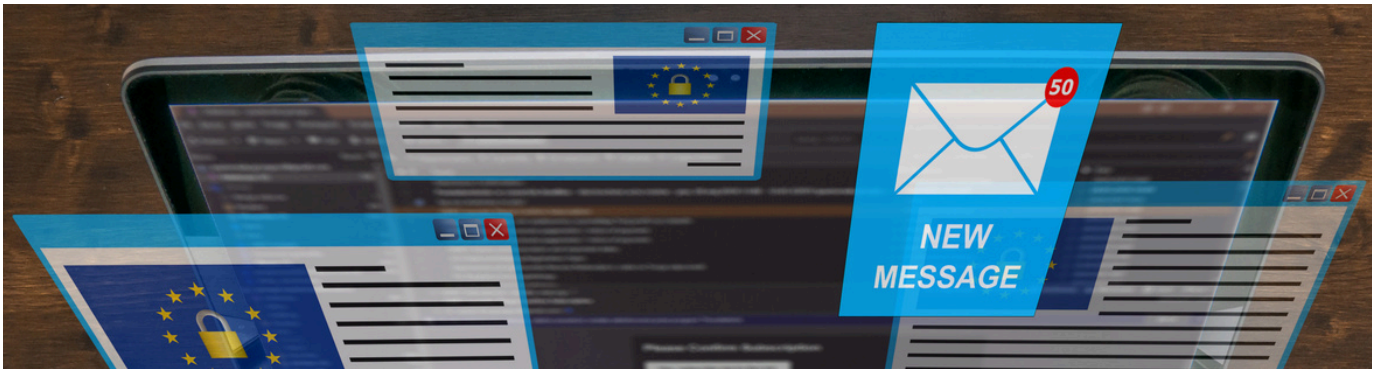
En 2024, les statistiques montrent que de nombreuses **TPE et PME peinent encore à atteindre une conformité optimale au RGPD**, **notamment sur leur site internet**.

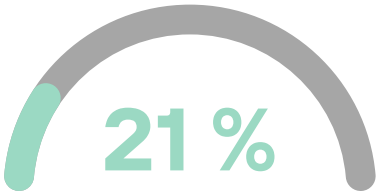
Il est essentiel pour ces entreprises de comprendre que se conformer au RGPD n'est pas seulement une obligation légale, mais aussi une opportunité de **renforcer la confiance des clients et d'améliorer, en ce sens, leur compétitivité**.

La plupart des TPE et PME confient la gestion de leur site internet à un prestataire, pensant que cela suffit pour garantir sa conformité. Cependant, notre diagnostic RGPD révèle que ces sites ne répondent souvent pas aux exigences légales. Il est donc essentiel de faire appel à un expert pour vérifier et assurer la conformité, afin de **protéger les données, d'éviter les sanctions financières, et de valoriser l'image de marque de l'entreprise.**

Marie Gossiôme
Expert DPO - Mission RGPD

4 Conformité aux droits des personnes





Source : CNIL

des sanctions CNIL, en 2023, présentent des manquements au respect des droits des personnes

Saviez-vous que chaque citoyen européen a des droits en ce qui concerne ses données personnelles ? Le Règlement Général sur la Protection des Données (RGPD) les garantit, et les PME et ETI doivent les respecter.

- **Le droit d'accès :** Imaginez pouvoir demander à une entreprise si elle détient des informations vous concernant, et qu'elle soit obligée de vous fournir toutes ces données. Eh bien, c'est possible !
- **Le droit de rectification :** Il arrive parfois que les informations détenues sur vous ne soient pas exactes. Mais pas de panique ! Vous avez le droit de demander à ce qu'elles soient corrigées. Ainsi, vos données seront toujours à jour.
- **Le droit d'opposition :** Vous préférez ne pas figurer dans une base de données ? C'est votre droit ! Vous pouvez vous opposer à être inclus dans un fichier, et même empêcher la diffusion ou la conservation de vos données personnelles.
- **Le droit à la portabilité :** Imaginez pouvoir récupérer vos données dans un format facilement utilisable. Avec le RGPD, vous avez ce pouvoir ! Vous pouvez transférer vos données d'un service à un autre ou les stocker où bon vous semble.
- **Le droit au déréférencement :** Vous souhaitez effacer une page web liée à vos informations personnelles des résultats des moteurs de recherche ? C'est possible !
- **Le droit à l'effacement :** Vous avez le droit de demander à une organisation d'effacer toutes les données personnelles qu'elle détient vous concernant. C'est une façon de garder le contrôle sur vos informations.
- **Le droit à la limitation :** Parfois, vous préférez limiter temporairement l'utilisation de vos données par une organisation. Pas de souci ! Vous pouvez demander à « geler » temporairement l'utilisation de certaines de vos données.

Résultats et Statistiques

Découvrez l'analyse des diagnostics concernant le respect des droits des personnes (salariés, clients, prospects, etc) réalisés dans le cadre de l'évaluation de la conformité RGPD des PME et ETI menée par Mission RGPD.

44,5%

des PME - ETI ont déjà reçu une demande de droit

72,1%

d'entre elles n'ont pas respecté toutes les démarches prévues par le RGPD

Types de demandes, réponses et suivis des demandes

Découvrez les types de demandes de droits les plus fréquentes ainsi que les démarches réalisées pour les réponses et suivis, grâce aux diagnostics de conformité RGPD menés auprès des PME et ETI, par Mission RGPD.

67 %

ont déjà reçu une demande d'opposition à leurs communications par email

55 %

ont déjà reçu une demande de rectification : mise à jour de données

72,1%

ont accusé réception de la demande

63,9%

ont répondu à la demande dans le délai légal d'un mois maximum

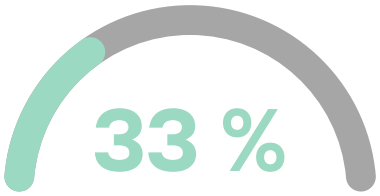
32,6%

tiennent un registre des demandes de droits

19%

n'ont fait aucunes des démarches ci-dessus

5 Conformité aux mesures de sécurité des données

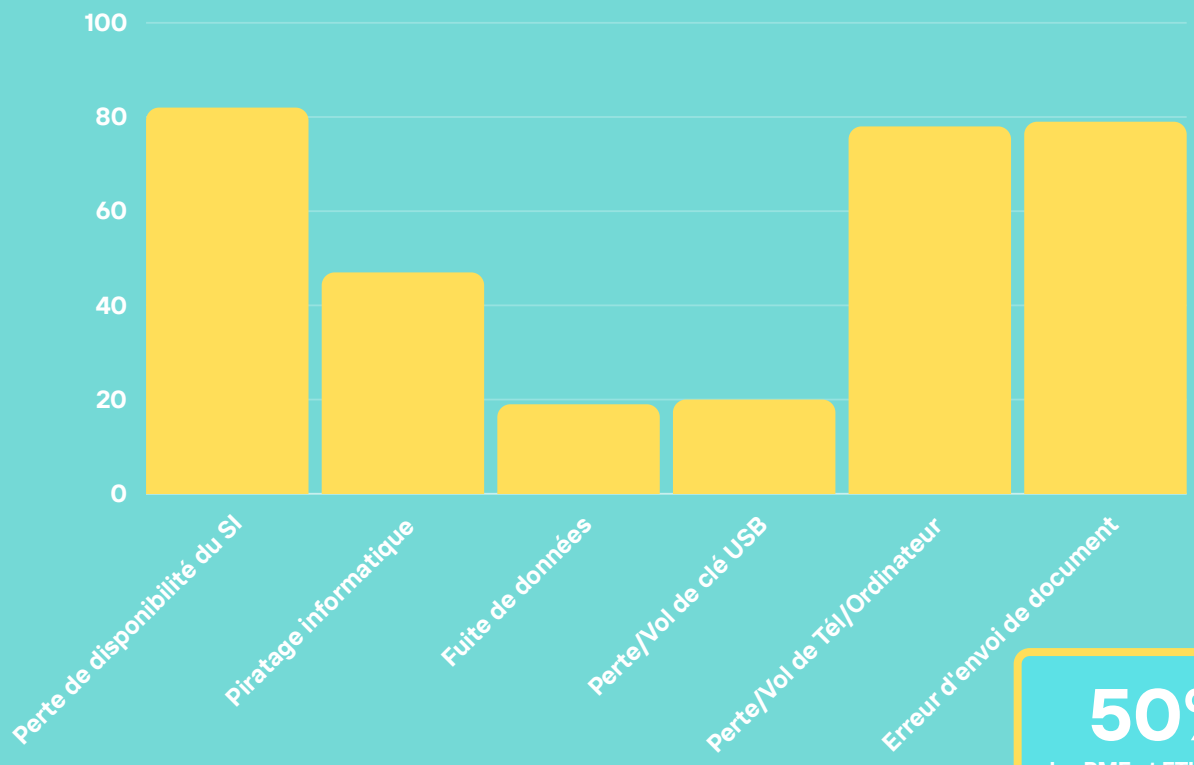


Source : CNIL

des sanctions CNIL, en 2023, présentent un défaut de sécurité des données

Types d'incident de sécurité des données connus et déclarés au sein des PME et ETI

La sécurité est un enjeu central de la protection des données. Les mesures techniques et organisationnelles permettent d'assurer la confidentialité, l'intégrité et plus généralement la disponibilité des données. Voici les incidents qui ont déjà eu lieu au sein des PME et ETI analysées. En ordonné le nombre d'entreprises - En abscisse les types d'incidents subis.



50%
des PME et ETI ont subi au moins un des incidents relevés ci-dessus

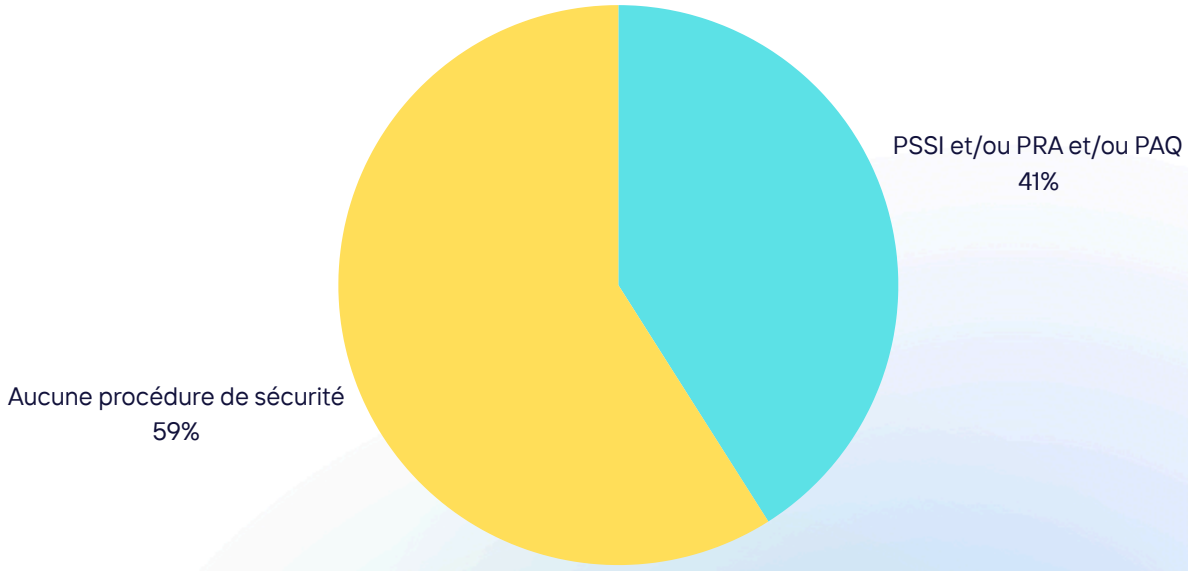
Procédure en cas d'incident de sécurité des données

Découvrez l'analyse des diagnostics concernant les procédures de gestion des incidents de sécurité des données, réalisés dans le cadre de l'évaluation de la conformité RGPD des PME et ETI menée par Mission RGPD.

#	Procédures	Description	% de PME et ETI
1.	Évaluer les risques de l'incident et corriger	Il convient d'évaluer les risques encourus pour déterminer un plan de remédiation.	**29,0%**
2.	Documenter l'incident	Le principe d'accountability oblige à documenter les incidents de sécurité.	**26,6%**
3.	Vérifier si besoin de notifier la CNIL	En cas de violation de données à risque élevé pour les personnes concernées, vous devez prévenir la CNIL sous 72h.	**10,6%**

Politique de sécurité documentée

L'article 32 du RGPD relatif à la sécurité du traitement de données exige que les responsables de traitements et les sous-traitants mettent en oeuvre des mesures techniques et organisationnelles afin d'assurer un niveau de sécurité adapté aux traitements qu'ils réalisent. Ces mesures, doivent être documentées. Des procédures et règles de sécurité doivent être organisées et documentées (gestion des mots de passe, accès aux locaux, sauvegarde des données, etc.) dans divers documents tels qu'une politique de sécurité du système d'information (PSSI), un plan de reprise et de continuité d'activité (PRA, PCA), un plan d'assurance qualité (PAQ), etc.



6 Conformité des relations avec les sous-traitants

Source : CNIL

des sanctions CNIL présentent un manquement à la conformité des relations avec un sous-traitant en 2023

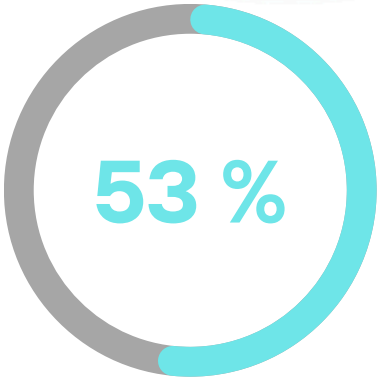
Lorsqu'il s'agit de respecter le RGPD, la conformité des relations avec les sous-traitants revêt une importance capitale. Mais qu'est-ce que cela signifie vraiment ?

Imaginez votre entreprise comme le maillon d'une grande chaîne. Vous confiez parfois certaines tâches à des partenaires externes, par exemple en faisant appel à une agence de communication pour votre site web ou utilisant un logiciel en ligne pour la gestion de la paie de vos salariés. Ces partenaires sont vos sous-traitants. Or, avec le RGPD, la responsabilité de protéger les données personnelles ne repose pas uniquement sur vos épaules, mais également sur celles de vos sous-traitants (et inversement !). C'est pourquoi, il est obligatoire de s'assurer de la conformité RGPD de vos sous-traitants et d'encadrer juridiquement ces relations.

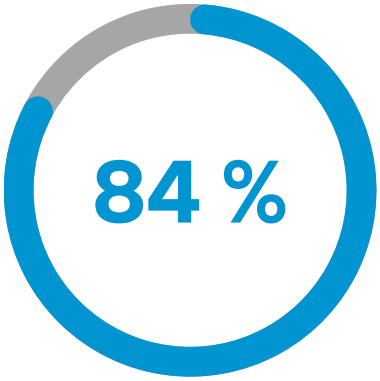
97 % **des PME et ETI ont identifié des sous-traitants qui traitent leurs données personnelles**

Exemples de sous-traitants

Découvrez l'analyse des diagnostics des relations sous-traitants réalisés dans le cadre de l'évaluation de la conformité RGPD des PME et ETI menée par Mission RGPD.



utilisent des logiciels SaaS (en ligne)



font appel à un prestataire pour la gestion du SI et/ou du site web

Encadrement des relations avec les sous-traitants

Découvrez ce que les PME et ETI ont mis en place pour encadrer les relations avec les sous-traitants.

19,2%
ont régularisé les contrats avec les ST (Annexe, Avenant, DPA)

59,6%
n'ont rien mis en place pour encadrer les relations ST

28,1%
se sont assurés de la conformité RGPD des ST

1,5%
encadrent correctement les relations ST et les évaluent régulièrement

7 Conformité des documents réglementaires

40 %

des sanctions CNIL présentent un manquement à l'information et/ou la documentation en matière de protection des données personnelles

Source : CNIL

Le RGPD exige que les entreprises documentent leurs processus, politiques et mesures de sécurité en matière de protection des données personnelles. Cette documentation joue un rôle crucial dans la justification et la démonstration de la conformité, tant dans le cas des relations commerciales, qu'auprès des parties prenantes ou encore lors de contrôles menés par les autorités compétentes françaises et européennes. Cette documentation est également essentielle pour informer les personnes concernant l'usage et la protection de leurs données personnelles. Voici les documents nécessaires et utiles pour démontrer la conformité RGPD des PME et ETI :

- Le registre des traitements de données personnelles
- La politique de confidentialité
- La politique cookies
- La charte informatique et des systèmes d'informations
- Le DPA (Data Processing Agreement) ou Accord de traitements de données pour les sous-traitants
- Le registre d'incidents et de violations de données personnelles
- Le registre des exercices des droits des personnes concernées
- Les politiques interne et externe de protection des données personnelles
- Les mentions d'informations interne et externe sur la collecte de données personnelles
- Le PIA / AIPD (Analyse d'impact sur la protection des données personnelles)*

* obligatoire selon certains critères

Résultats et Statistiques

Découvrez l'analyse des diagnostics concernant la documentation RGPD, réalisés dans le cadre de l'évaluation de la conformité RGPD des PME et ETI menée par Mission RGPD.

5,7%

des PME et ETI ont une documentation RGPD complète

36,9%

des PME et ETI n'ont aucun document RGPD

Registres, documents et informations

Découvrez les taux de mise en place des documents RGPD prévus et exigés par le réglement, grâce aux diagnostics de conformité RGPD menés auprès des PME et ETI, par Mission RGPD.

30 %

ont mis en place un registre des traitements de données personnelles

21 %

informent avec des mentions sur les formulaires de collecte

46 %

ont mis en place une politique de confidentialité pour informer les personnes

45 %

ont mis en place une charte informatique en interne

Registre des traitements de données personnelles

Découvrez les statistiques sur la mise en place du registre des traitements exigé par le réglement, grâce aux diagnostics de conformité RGPD menés auprès des PME et ETI, par Mission RGPD.

61%

des PME et ETI qui ont un registre des traitements de données rencontrent des difficultés pour gérer ce document

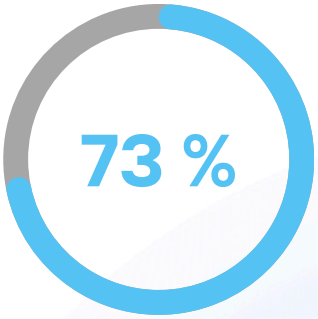
17 %

rencontrent des difficultés à créer et compléter le registre des traitements

44 %

rencontrent des difficultés pour assurer la mise à jour du registre des traitements dans le temps

Pilotage de la conformité et centralisation des documents RGPD



des PME et ETI n'ont pas centralisé les documents RGPD en cas de contrôle des autorités compétentes ou en cas de demande d'un tiers

Observations d'expert

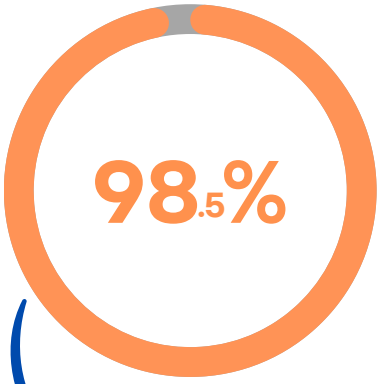
En 2024, de nombreuses **TPE et PME rencontrent encore des difficultés à établir et maintenir à jour les documents nécessaires** pour leur conformité RGPD. Souvent, elles manquent de ressources internes spécialisées et ne savent pas par où commencer.

Pour les entreprises qui ont réussi à mettre en place un registre, beaucoup peinent à le mettre à jour régulièrement. C'est pourtant un document essentiel à présenter en cas de contrôle de la CNIL. Ce document permet également d'établir des politiques claires et transparentes afin d'informer les prospects et les clients sur l'usage et la protection de leurs données.

Au delà de l'obligation légale, les politiques, les registres de traitement des données et les clauses dans les contrats sont surtout **des alliés business permettant de démontrer les engagements pris** en matière de protection des données.

Marie Gossiôme
Expert DPO - Mission RGPD

8 Évaluation des freins à la conformité des PME et ETI



des PME et ETI ne sont pas en conformité optimale au RGPD

voir p.5

Voici les freins à la conformité selon les PME et ETI

52 % manquent de temps

50 % manquent de compétences juridiques

47 % ne savent pas par où commencer

36 % ont des difficultés à assurer une conformité à jour dans le temps

Observations d'expert

Les résultats du baromètre démontrent la réalité opérationnelle de la conformité au RGPD pour les PME et ETI.

Pour surmonter ces freins, nous recommandons plusieurs solutions :

- **Prioriser les actions :** Identifiez les domaines les plus critiques et commencez par là. Un audit initial peut révéler les non-conformités exposant à des risques élevés et les points d'amélioration prioritaires.

- **Externaliser si nécessaire :** Si les ressources internes et l'expertise juridique manquent, n'hésitez pas à faire appel à des experts externes. Un expert DPO peut apporter une expertise précieuse et vous guider efficacement.

- **Automatiser la mise et maintien en conformité :** Utilisez des solutions qui peuvent vous aider à la mise et maintien en conformité en automatisant certaines tâches, comme par exemple : la création et mise à jour du registre des traitements, la gestion des demandes de droits ou encore la sécurisation de votre site web.

Emma Saby
Expert Mission RGPD

“La protection des données est un enjeu crucial pour toutes les entreprises, quelque soit leur taille. 6 ans après la mise en place du RGPD, ce baromètre montre que nombreuses PME et ETI rencontrent encore des difficultés pour se mettre en conformité. Il est essentiel de bien se faire accompagner et de disposer d'une feuille de route claire pour maîtriser ce sujet. Nous sommes fiers d'accompagner **Mission RGPD** et ses clients au quotidien à travers **Visiativ Transformer**, une application dédiée au pilotage des transformations en entreprise. Visiativ est un écosystème de solutions pragmatiques, ensemble **nous contribuons à renforcer la confiance et la sécurité dans le traitement des données.**“

Laurent Fiard
Président Directeur Général
Visiativ

À propos de visiativ co-fondateur de Mission RGPD

Visiativ accompagne depuis plus de 35 ans les entreprises dans leur transformation et leur innovation pour gagner en rapidité et en compétitivité. Les solutions proposées par Visiativ permettent aux organisations d’améliorer significativement leur profitabilité et leur croissance, grâce à l’accélération de l’innovation, une plus grande mobilisation de leur capital humain et une ouverture de l’entreprise avec son écosystème. Visiativ apporte des solutions collaboratives et sociales qui s’adaptent aux différents métiers de l’entreprise et décloisonnent les flux entre directions métiers. Visiativ, conçoit et commercialise Visiativ Innovation Engine, au service de l’entreprise et de ses enjeux. En s’appuyant sur son savoir-faire et son expertise métier, les équipes conçoivent des applications verticalisées par secteur d’activité et par fonction, personnalisables et activables à la demande. Visiativ accompagne ainsi la digitalisation du bureau d’études, du service achat, des services généraux, des ressources humaines, du département vente et marketing, du service client, ou du service qualité, en développant des expériences métiers dédiées.

“A l’origine de la création de **Mission RGPD** il y a plusieurs années, nous avons toujours pensé que la donnée était essentielle dans la vie des entreprises. Une donnée identifiée, fiable, **transparente**, et sécurisée. L’IA ne sera pas sans la donnée. C’est dire qu’aujourd'hui Mission RGPD à plus qu’une mission. Un devoir. C’est le travail quotidien d’équipes engagées pour **la valorisation des données** et pour leur garantir une exploitation optimale dans **le respect des règlementations.** “

Jean-Charles Simon
Avocat Simon Associés

À propos de SIMON ASSOCIÉS co-fondateur de Mission RGPD

Fondé en 1992, SIMON ASSOCIÉS est un cabinet d’affaires pluridisciplinaire. Élu cabinet innovant de l’année 2024 par le Monde du Droit, il regroupe 180 avocats en France (Simon Associés + Réseau Simon Avocats) et s’appuie sur un réseau international avec des cabinets de renom dans plus de 64 pays. En France, SIMON ASSOCIÉS est présent à Paris, Lille, Lyon, Nantes, Nice, Montpellier, Toulouse, Versailles et via SIMON AVOCATS (réseau de cabinets indépendants) à Aix-en-Provence, Bordeaux, Bourg-en-Bresse, Clermont-Ferrand, Le Havre, Marseille, Metz, Montluçon, Nancy, Nice, Pontarlier, Rouen, Vichy.

Mission RGPD

La plateforme qui s'occupe de la conformité **RGPD des PME et ETI en toute simplicité**

www.mission-rgpd.com

Démarrez et estimez votre score RGPD

Assurez votre conformité RGPD en quelques clics

GRATUIT FAIRE MON DIAG RGPD EN LIGNE — A B C D E → A B C D E — DEMANDER UNE DÉMO

Excellent 4.6 sur 5 Trustpilot

À propos de

Mission RGPD est la 1ère plateforme tout-en-un qui s'occupe de la conformité RGPD des PME et ETI. Créée par l'alliance de Visiativ et Simon Associés, la solution clé en main accompagne + 1 000 entreprises et organisations dans plus de 22 pays. La plateforme 100% SaaS offre un véritable guide pour mettre le cap rapidement vers la conformité incluant l'accompagnement par des experts DPO d'un diagnostic complet, jusqu'au pilotage de la conformité sans oublier la sensibilisation des collaborateurs, la sécurité des données, la création et mise à jour automatisées des registres, des simulations de contrôles, la gestion des demandes de droits et bien plus encore. Assurez votre conformité RGPD à jour en quelques clics.