Leto

CRÉER UN PROGRAMME DE CONFORMITÉ RGPD EFFICACE ET ENGAGEANT

EN 10 ÉTAPES

LE GUIDE LEGAL

SOMMAIRE

LES POINTS CLÉS

1. Introduction
2. Feuille de route
3. Acteurs de votre conformité
4. Cartographier les données
5. Registre des traitements
6. Cookies et bannière
7. Sous-traitants
8. Demandes d’exercice de droits
9. Politique de confidentialité
10. Évaluer et documenter vos risques
11. Sensibiliser et former vos équipes
12. Conclusion

À PROPOS DE LETO

NOTRE HISTOIRE

La protection à la vie privée est gage de transparence et de respect dans la relation avec les autres. Mais la mise en pratique n'est pas toujours simple. Cela peut faire peur.

C'est la raison pour laquelle nous avons créé Leto.
Une solution qui vient concilier simplicité, clarté et efficacité dans le respect des données personnelles d'une entreprise.

POUR NOUS, LA PROTECTION DE LA VIE PRIVÉE EST UN DROIT FONDAMENTAL.

Benjamin Lan Sun Luk et Édouard Schlumberger, fondateurs de Leto

1. INTRODUCTION

La problématique du RGPD est de plus en plus présente dans nos entreprises

INTRODUCTION

La mise en œuvre du Règlement Général sur la Protection des Données (RGPD), longtemps reléguée à une problématique de conformité légale, émerge progressivement comme une discipline de croissance.

Une meilleure compréhension des enjeux de structuration des patrimoines d'actifs de données des entreprises soutient désormais les exigences des clients, des partenaires, des salariés et des autorités de contrôle en matière de protection des données à caractère personnel.

Cette transition d'une conformité dite "de case à cocher" à une véritable gouvernance des données à caractère personnel est l'opportunité de poser un autre regard sur les étapes d'élaboration et de mise en œuvre des programmes de protection des données personnelles dans votre organisation.

Dans ce guide pratique, nous avons réuni les conseils et les retours d'expériences des praticiens du RGPD pour lesquels Leto travaille chaque jour à développer des solutions de conformité et de gestion des risques plus adaptées aux contraintes et spécificités opérationnelles des entreprises qu'ils accompagnent.

2. FEUILLE DE ROUTE

Une feuille de route claire permet de tracer un chemin précis vers la conformité

VALIDEZ VOTRE FEUILLE DE ROUTE RGPD ET ASSUREZ-VOUS DU SOUTIEN DE VOTRE ORGANISATION

Il existe autant de programmes de conformité au RGPD que d’entreprises. Grandes ou petites structures, avec ou sans DPO, traitements à risque, données pseudonymisées…

Les programmes qui offrent une protection efficace des données tout en combinant maîtrise des coûts, innovation et rapidité d’exécution ont tous au moins **deux caractéristiques en commun :**

- sens & priorisation : la raison d’être du programme et son insertion dans la stratégie globale de l'entreprise sont claires. Les objectifs annuels du programme sont partagés et tous les participants, du comité de direction jusqu’aux équipes opérationnelles, savent identifier les chantiers prioritaires.
- itération & outillage : les participants au programme saisissent les opportunités d’automatisation des processus de travail grâce aux services et technologies émergentes. Ils harmonisent et mettent à jour la documentation de conformité chaque fois que cela est possible.

La protection des données et la conformité RGPD sont une quête constante qui s’insère dans un objectif de performance plus large qui impacte l’ensemble d’une organisation : favoriser l’innovation et la circulation des données dans le respect des droits fondamentaux.

Les praticiens du RGPD opèrent dans un environnement mouvant dont ils ne maîtrisent pas (encore) tous les paramètres :

- mesurez et communiquez sur vos progrès ;
- adoptez une approche itérative: créez, testez, améliorez ;
- restez à l’écoute de vos collaborateurs et des évolutions réglementaires.

S’il est désormais admis qu’une conformité à 100% n’existe pas, vos collaborateurs, partenaires et auditeurs seront en revanche sensibles à la façon dont vous communiquez sur votre feuille de route et effectuez le suivi de vos actions.

3 règles d’or pour une feuille de route RGPD actionnable :

1. simplifiez la mise à jour en intégrant votre outil de feuille de route aux outils de gestion de projet et de gestion de risques ;
2. organisez une revue régulière (une fois par trimestre ou par semestre) pour ajuster les objectifs et l’évaluation des risques en fonction des priorités de l’entreprise ;
3. communiquez régulièrement vos priorités à vos collaborateurs et à votre direction et impliquez-les dans le processus de validation des objectifs.

3. ACTEURS DE VOTRE CONFORMITÉ

Qui sont ces différents acteurs associés au RGPD et à la conformité des données ?

QUI SONT LES ACTEURS DE VOTRE CONFORMITÉ RGPD ?

“Lead RGPD”, “Data Privacy Owner”, “Data protection Steward”, “Privacy Champion”, “Relais RGPD”, “DPO”... autant d’acronymes et sobriquets couramment attribués aux personnes mises à contribution dans la mise en œuvre des règles et principes du RGPD.

⚡ **Multidisciplinarité**

Il faut tout un village pour faire progresser la protection des données personnelles. Un Data Protection Officer expérimenté est le profil idéal pour conduire et monitorer un programme RGPD. En effet, sa formation spécifique et pluridisciplinaire lui donne une compréhension poussée des évolutions réglementaires applicables à des systèmes d’information et des activités de traitement de données.

LA DESIGNATION DU DATA PROTECTION OFFICER (DPO)

Que sa désignation soit obligatoire ou non, le DPO est un acteur clef de la conformité RGPD et le partenaire privilégié de la protection des données personnelles au sein d'une organisation. Il conseille et accompagne vos équipes, pilote le programme de conformité, contrôle l'effectivité des règles applicables dans le temps. Il est aussi le point de contact privilégié des autorités de contrôle et des individus dont les données sont traitées (les "personnes concernées").

Dans son guide pratique, la CNIL rappelle pour être désigné DPO, un collaborateur doit remplir deux critères principaux:

Compétence. Disposer d'un "certain niveau de connaissances". Ces connaissances incluent notamment une expertise juridique et technique, la compréhension du secteur d'activités, des opérations de traitement, des systèmes d'information et des besoins de l'organisme en matière de protection et de sécurité des données. Le DPO doit donc être formé selon son profil et ses besoins.

Indépendance. Un DPO ne peut pas être "juge et partie". Il ne doit avoir aucun pouvoir décisionnel sur la détermination des finalités et moyens de traitements. Il doit disposer des ressources nécessaires pour exercer sa mission.

Bien qu'idéalement positionnés pour mener à bien la conformité au RGPD, les DPOs ne sont ni omniprésents ni omniscients.

Qu’elle soit DPO ou non, la personne responsable du programme RGPD doit pouvoir compter sur la participation active de collaborateurs experts pour mener sa mission à bien. Plus votre organisation grandit, plus vos traitements de données se complexifient, plus votre réseau RGPD devra refléter la diversité et la complémentarité des profils et des compétences qui irriguent la collecte et l’utilisation des données dans votre organisation.

Par exemple, si le responsable RGPD est membre de l’équipe chargée de la conformité réglementaire de l’entreprise, il aura probablement besoin de consulter des juristes spécialisés, des experts en sécurité des systèmes d’information et en analyse de données.

Entre 2019 et 2021, 47% des DPO n’étaient pas issus de domaines juridiques ou techniques, ce qui souligne la grande diversité des profils candidats à la fonction.

Chaque DPO apporte donc un bagage de compétences distinct. Par conséquent, concevez sa fiche de poste en adéquation avec vos priorités stratégiques, votre organigramme et votre culture d’entreprise.

⚡ Transversalité

Le responsable du programme RGPD et les collaborateurs impliqués travaillent le plus souvent au sein de départements différents.

Pour s’assurer qu’ils puissent collaborer efficacement, il est généralement recommandé de solliciter des personnes qui :

- ont l’habitude de travailler en conjonction avec d’autres équipes ;
- sont sensibilisées aux enjeux de la protection des données ou sont volontaires pour contribuer au programme ;
- disposent d’accès aux outils de travail et de communication communs ou dédiés.

Leto propose une interface simplifiée et adaptée à vos environnements métiers pour faciliter la collaboration transversale sur tous vos projets RGPD.

Les compétences interpersonnelles ou “soft skills” des candidats au programme sont également à prendre en considération. Les communicants rigoureux, les personnes résilientes et empathiques font généralement de très bons contributeurs RGPD puisqu’ils facilitent la compréhension commune de problématiques complexes à travers toute l’organisation.

⚡ Responsabilité

Qu’elle soit internalisée ou non, la personne responsable du programme devra s’assurer que ses appuis et contributeurs au sein de l’organisation sont détenteurs de niveaux de responsabilités appropriés afin de garantir tant l'exécution que la légitimité des décisions prises. En pratique, un exercice de type R-A-C-I permettra d’allouer les ressources et les responsabilités en fonction, soit de la position dans l’organigramme de l’entreprise, soit du niveau d’expertise requis pour un projet donné.

Par exemple, il pourra être demandé à un membre du comité de direction de relire et signer systématiquement les documents et politiques qui atteignent un certain seuil de personnes concernées tandis qu’un spécialiste des infrastructures logicielles sera sollicité en mode projet pour déterminer les mesures de sécurité appropriées pour le déploiement d’une nouvelle application.

Important : la notion de responsabilité dans le cadre du pilotage de la conformité est à dissocier de celle, purement juridique, de “responsable de traitement”. Un DPO et son réseau de contributeurs sont responsables d’identifier les flux de données à caractère personnel (DCP) dans l’entreprise, de proposer et de mettre en œuvre les mesures appropriées pour protéger ces données de toute utilisation non autorisée.

4. CARTOGRAPHIER LES DONNÉES

Une de vos toutes premières tâches consistera à répertorier les données personnelles

COMMENT CARTOGRAPHIER LES DONNÉES À CARACTÈRE PERSONNEL ("DCP") ?

L’enjeu opérationnel de la protection des données est la connaissance et la maîtrise des risques pour les individus. Identifier les risques générés par l’utilisation des données personnelles des “personnes concernées” implique d’avoir au préalable inventorié ou cartographié les données traitées.

Un inventaire de DCP est plus qu'une liste à puces. Il s'agit d'un examen systématique d’une catégorie de données et de son comportement dans un environnement donné.

La grille d’analyse comprend la finalité du traitement, les destinataires, les durées de conservation ainsi que d'autres détails permettant de répondre aux exigences de conformité.

Cet inventaire est la base de tout effort de constitution et de mise à jour des registres de traitement dont la tenue est imposée par le RGPD.

Voici les bénéfices que vous pourrez retirer en travaillant avec le bon outil :

- analyse de données harmonisée : vous êtes capable de réconcilier des données de centaines de sources et de formats différents dans une interface simplifiée. Le processus d'analyse est rationalisé, garantissant que toutes les catégories de données sont étiquetées de façon cohérente et pertinente dans une source unique ;
- transparence accrue : chaque étape du processus d’analyse et de catégorisation est explicable et vérifiable. Le DPO et son réseau RGPD peuvent facilement utiliser l'outil pour vérifier les informations, ce qui en retour vous aide à repérer les erreurs, les dysfonctionnements et les risques potentiels ;
- facilité de mise à jour : vous effectuez des mises à jour régulières de vos cartographies et vous pouvez facilement suivre les modifications apportées à votre registre de traitement. Vous pouvez alors mesurer objectivement votre progression ;
- visualisation corrélée : la cartographie permet de mettre en relation deux ou plusieurs caractéristiques de traitements pour soutenir l’analyse des risques inhérents à certains flux de données, par exemple entre applications, entre pays, entre entités ou encore entre types des personnes concernées ;
- sécurité garantie : l’outil ne duplique pas et ne stocke pas les données inventoriées.

Leto offre un outil de data mapping automatisé qui s’intègre par API sécurisée aux 100 applications les plus utilisées par les entreprises.

Exemple : connectez Leto à votre API Slack, l’outil reconnaît et étiquette l’ensemble des données personnelles traitées par l’application par catégorie de données et par finalité.

Vos flux de données personnelles sont contextualisés et organisés pour vous permettre de compléter rapidement et précisément votre registre de traitement.

5. REGISTRE DES TRAITEMENTS

Il est impératif de tenir un registre des traitements des données personnelles

COMMENT CRÉER LE REGISTRE DES TRAITEMENTS DE DONNÉES PERSONNELLES ?

Les organisations de plus de 250 salariés ou qui traitent des volumes de données importants doivent “tenir un registre des activités de traitement effectuées sous leur responsabilité” permettant d’identifier :

- les catégories de données traitées ;
- à quoi servent ces données, qui y accède et à qui elles sont communiquées ;
- combien de temps les données personnelles sont conservées ;
- comment elles sont sécurisées.

En cas de non-respect de ces obligations, le responsable de traitement et le sous-traitant s’exposent à une amende allant jusqu’à 10 millions d’euros ou 2% du chiffre d’affaires annuel mondial calculé sur l’exercice précédent.

Plusieurs PME ont déjà été sanctionnées pour non-respect de l’article 30 du RGPD qui détaille les obligations de tenue de ce registre.

Au-delà de l'obligation légale de conformité, le registre de traitement est un outil stratégique pour la gouvernance des données de l'organisation qui présente de multiples avantages.

Anticiper la création et la mise à jour de ce document clef bien en amont de vos projets vous épargnera beaucoup de problèmes et de ralentissement opérationnels.

Il sera notamment utile au DPO qui pilote le programme de conformité et à ses relais pour :

- proposer et prioriser des pistes d'amélioration puisque qu'une absence d'information ou une information erronée lui permettra de mettre à jour sa cartographie des risques ;
- mesurer la progression du programme de conformité en calculant notamment la complétude et en constatant les fréquences de mise à jour ;
- justifier sa conformité auprès de clients et partenaires ;
- faciliter les échanges avec les autorités de contrôles auxquelles vous devrez transmettre le registre.

Construisez un registre de traitements qui ressemble à votre organisation et s’adapte aux ressources disponibles.

Le registre doit donner une vue d’ensemble qui contextualise les activités de traitement et détaille les informations recueillies lors de l’inventaire des données.

Trop fourni, il sera difficile à mettre à jour. Trop vague, il n’ajoutera pas de valeur à vos activités et ne satisfera pas les exigences des autorités de contrôle.

Pour vous faire gagner du temps, Leto met à disposition de nombreux templates d’activités de traitement qui vous permettent de sélectionner en quelques clics les données et les finalités concernées.

La fonctionnalité de préremplissage mobilise votre inventaire de données sur plus de 100 applications pour augmenter la pertinence de votre registre et progressivement automatiser sa mise à jour.

6. COOKIES ET BANNIÈRE

Pensez bien à respecter les règles concernant les cookies et les bannières

COOKIES : COMMENT METTRE EN PLACE UNE BANNIÈRE CONFORME ET COLLECTER LES CONSENTEMENTS ?

Les règles applicables aux cookies résultent de la combinaison du RGPD et de la directive européenne “e-privacy” (2009).

Les difficultés d’articulation et d’interprétation de ces textes en ont fait la bête noire de beaucoup d’entreprises, mais aussi des internautes. Selon cette association, ils seraient 90% à accepter l’ensemble des cookies déposés sur leurs appareils alors même que seulement 3% en ont réellement l’intention.

Tout l’enjeu est de donner aux utilisateurs une meilleure maîtrise du suivi de leurs activités en ligne. Pour simplifier, les organisations qui souhaitent utiliser des cookies dits “non strictement nécessaires” pour mesurer leur trafic, cibler leurs audiences et analyser leurs interactions avec leurs produits et services doivent s’assurer que ces cookies sont collectés avec le consentement libre et éclairé des internautes.

Checklist de conformité cookie :

- auditer les cookies : scanner vos sites web et vos applications ;
- inventoriez vos cookies : quels cookies, pour quelles finalités, pour combien de temps ;
- rédiger une politique de cookies facilement accessible qui reflète votre inventaire et vos pratiques ;
- concevoir une bannière qui donne un accès direct à votre politique de cookies, permet à l'utilisateur d'accepter ou de refuser les cookies "non strictement nécessaires" ;
- définir un système de stockage actualisé et sécurisé des consentements donnés ;
- donner aux utilisateurs la possibilité de retirer leur consentement à tout moment.

Il existe un marché florissant de solutions dédiées qui proposent, clefs en main, une gestion 360° des cookies et des consentements (Consent Management Platform).

Certaines prennent en compte d'autres réglementations extraeuropéennes en matière de cookies si vos offres ou services s'adressent par exemple à des résidents californiens protégés par le CCPA.

En choisissant, un outil de gestion des cookies, pensez à privilégier :

- une plateforme qui inclut la gestion des enregistrements de consentement des visiteurs ;
- un système qui peut gérer d'autres questions de consentement, telles que le consentement relatif au lieu de stockage des données RGPD ;
- un service géré qui offre une API pour fournir toutes les popups de consentement ;
- un tableau de bord qui vous permet de visualiser toutes les activités liées au consentement ;
- un service qui peut facilement s'intégrer à d'autres plateformes Web, comme les plateformes ; d'hébergement ou les systèmes de gestion de contenu
- un essai gratuit avec une période d'évaluation sans aucun frais pour vous permettre de tester la solution ;
- un bon rapport qualité-prix et un système de paiement simple, sans période d’engagement ni frais d'installation initiaux.

> **“ J’ai d’autres priorités et mon entreprise n’a pas besoin de toutes ces données**

Faites comme Leto et passez au cookie-less !

7. SOUS-TRAITANTS

Vos sous-traitants sont aussi impactés par les règles du RGPD

COMMENT GÉRER VOS SOUS-TRAITANTS DE DONNÉES PERSONNELLES ?

Entre quelles mains placez-vous les données personnelles que vous traitez et la réputation de votre organisation?

C’est la réflexion à laquelle vous invitent les praticiens et tout particulièrement le chapitre IV du RGPD.

Les prestataires tiers auxquels les entreprises confient la collecte et l’utilisation de DCP constituent la source principale de risque pour la sécurité des données personnelles et la conformité des traitements.

La majorité des violations de données personnelles impliquent des prestataires tiers.

Créez un module d’évaluation et de contrôle des sous-traitants de données personnelles dans votre programme qui couvre les points de contrôle principaux :

- recensement - Vous avez une liste à jour de vos partenaires, prestataires et fournisseurs. Vous avez une vue d’ensemble des activités de traitement de données personnelles qui s’y rapportent ;
- instruments juridiques et contractuels - Des annexes de protection des données personnelles sont signées entre les entités concernées, la répartition des rôles et responsabilités entre les parties et vis-à-vis des éventuels sous-traitants ultérieurs est claire. Des clauses contractuelles types adoptées par la Commission Européenne sont incorporées à vos contrats pour encadrer les transferts à des entités non soumises au RGPD. Enfin, les instructions du responsable de traitement au sous-traitant sont formalisées ;
- évaluation & contrôle - Vous avez des processus de consultation internes qui permettent d’identifier et d’évaluer a priori et a posteriori chaque nouveau sous-traitant de données en fonction des risques que présentent les activités envisagées. Vous avez prévu contractuellement les modalités d’audit et de contrôle des sous-traitants qui doivent pouvoir justifier de la conformité et de la sécurité des traitements effectués ;

- sécurité des traitements - La confidentialité, l’intégrité et la disponibilité des données personnelles traitées par vos partenaires tiers sont régulièrement testées par des auditeurs indépendants. Un nombre croissant de sous-traitants qui traitent des données à très grande échelle et/ou des données dites sensibles (ex. : services Cloud, hébergement de données de santé) sont détenteurs de certifications de sécurité organisationnelle et technique. Demandez-leur ces certificats pour documenter votre conformité à l’article 32 du RGPD (“Sécurité du traitement”).

Leto a recensé pour vous plus de 6000 applications SaaS et vous suggère des clauses contractuelles en fonction des sources de données identifiées.

Grâce à Leto, vous automatisez votre clausier et votre librairie contractuelle pour vous concentrer sur les tâches à valeur ajoutée: négociation contractuelle, programme de contrôle des partenaires et collaboration avec les équipes impliquées.

Fini les copier-coller dans vos templates de contrats !

8. DEMANDES D'EXERCICE DE DROITS

Apprenez à gérer les différentes demandes d'exercices de droits

COMMENT RÉPONDRE AUX DEMANDES D'EXERCICE DE DROITS ?

Accès, effacement, rectification, opposition, information, portabilité…

Favoriser l'exercice des droits des personnes concernées, c'est le premier axe stratégique de la CNIL pour une mise en œuvre effective du RGPD.

Par ailleurs, la CNIL a connu un sursaut de 35% des plaintes concernant l'exercice de droits qui concernent désormais 49 % du total des demandes effectuées auprès de l'autorité de contrôle.

Qu'il s'agisse de clients, de salariés, ou de partenaires, la maîtrise du sujet est donc essentielle pour les entreprises afin de préserver la confiance des interlocuteurs et d'éviter les sanctions.

Il s'agit également de gagner du temps car certaines demandes complexes peuvent être lourdes à gérer et mobiliser beaucoup d'interlocuteurs internes et externes.

Mettre en œuvre la gestion des demandes d’exercice de droits, c’est avant tout construire des processus opérationnels adaptés qui en retour renforcent la connaissance interne de vos flux de données et des risques associés.

De plus en plus d’entreprises confient d’ailleurs le traitement des requêtes à des spécialistes d’un nouveau pan de la protection des données personnelles: les “Privacy Ops”.

4 piliers opérationnels pour une gestion efficace et conforme des exercices de droits :

- authentification : votre processus prévoit les situations dans lesquelles vous procédez à des vérifications complémentaires si vous n’êtes pas raisonnablement certains que le demandeur est bien la personne concernée. Cela implique de minimiser le nombre de canaux de réception par lesquels les requêtes arrivent en prenant garde toutefois à ce que les points d’entrée demeurent facilement accessibles pour les individus. Le système d’authentification, surtout s’il implique la collecte de données additionnelles, et en particulier de pièces d'identité, devra être sécurisé ;
- limitations : les droits accordés par le RGPD ne sont pas absolus. Ils doivent être mis en balance avec les intérêts d’autres personnes concernées par les données qui font l’objet des demandes ainsi que des contraintes légales applicables à l’organisation telles que l’obligation de conserver des documents fiscaux. Certaines demandes, jugées excessives, pourront être rejetées ou faire l’objet de clarifications. Le périmètre des demandes acceptables doit être clair pour les collaborateurs qui les traitent au risque d’allonger inutilement des délais de réponse, ou pire, de se tromper dans l’analyse juridique de la demande ;
- délai : la première cause de plainte des personnes concernées à la CNIL est le dépassement du délai de réponse standard à une demande d’exercice de droits: 1 mois. Afin de réduire les temps de latence, pensez à calculer le coût et le temps de traitement nécessaire à vos requêtes les plus courantes, surtout lorsque le traitement d’une demande nécessite l’intervention de plusieurs équipes ;

- transparence : les réponses aux demandes, et tout particulièrement les décisions de rejet, doivent être justifiées et expliquées aux personnes concernées dans un langage clair et accessible. Les personnes doivent être informées de leurs droits de recours. Enfin, gardez à l'esprit qu'il s'agit d'une communication sensible qui doit être considérée dans le cadre plus large de la stratégie de l'entreprise. Par exemple, une personne qui effectue une demande d'effacement d'un compte est peut-être un client insatisfait. Une réponse automatisée ne veut pas nécessairement dire qu'elle est impersonnelle.

Leto vous aide à harmoniser la réception et l'analyse de vos demandes d'exercices de droit grâce à un module dédié qui centralise les demandes à partir d'un portail personnalisé qui s'intègre facilement à vos pages dédiées.

En quelques clics, vos actions sont attribuées aux équipes responsables et vous suivez l'avancement du processus de traitement en temps réel.

Lorsque la demande est traitée, Leto envoie automatiquement les notifications que vous avez paramétrées dans l'outil. Fini les emails orphelins et les fils de conversations interminables !

9. POLITIQUE DE CONFIDENTIALITÉ

Vous devez rédiger une politique de confidentialité qui respecte le droit à la vie privée

COMMENT RÉDIGER UNE POLITIQUE DE CONFIDENTIALITÉ CLAIRE, ACCESSIBLE ET INTERACTIVE?

Vos politiques de confidentialité sont le reflet non seulement de vos activités de traitement de données personnelles mais aussi de la façon dont vous considérez et respectez le droit à la vie privée des personnes concernées, qu'ils s'agissent de vos clients, de vos salariés ou de vos partenaires.

Il s'agit d'un support de communication qui revêt une importance croissante, surtout pour des entreprises dont l'activité repose sur le traitement des données à caractère personnel.

La transparence de ces informations est donc non seulement une obligation légale mais aussi, de plus en plus, une exigence.

Quelques bonnes pratiques vous aideront à développer et mettre à jour ce document :

- précision. Votre déclaration de confidentialité doit refléter avec précision la collecte et l'utilisation des données de vos services et produits ;
- clarté. Votre déclaration de confidentialité doit être claire, directe et facile à comprendre pour des non-experts. Des obligations renforcées s’appliquent pour les biens et services offerts à des mineurs. Limitez au maximum le jargon technique et la terminologie juridique. L’enjeu principal est d'expliciter les bases légales et les finalités sélectionnées pour vos différentes activités de traitement. Le consentement des utilisateurs à certaines activités remplit les conditions posées par le RGPD ;
- mise à jour: si vous décidez de modifier la manière dont vous utilisez les informations personnelles, vous devez en informer les utilisateurs. Des règles robustes et partagées concernant le versionnage du document vous feront gagner du temps des mises à jour ;
- effectivité. La politique de protection de la vie privée d'une entreprise est aussi solide que le personnel qui la met en œuvre. Il est donc primordial que vos collaborateurs soient prévenus et informés des pratiques énoncées afin qu’ils puissent la mettre en œuvre ou proposer des correctifs.

Grâce à des widgets dits “no-code”, Leto permet à vos utilisateurs de visualiser votre politique de confidentialité de façon interactive et simplifiée.

En quelques clics, vous leur offrez une compréhension nouvelle et accessible de l’utilisation que vous faites de leurs données personnelles.

Des templates sont également disponibles pour vous aider à démarrer.

Laissez-vous guider !

10. ÉVALUER ET DOCUMENTER VOS RISQUES

Il est maintenant incontournable d'adopter pour une entreprise une gouvernance des risques fortes

COMMENT ÉVALUER ET DOCUMENTER VOS RISQUES ?

Le RGPD a modifié la posture de conformité des responsables de traitement en adoptant une logique dites d' "accountability" qui mise sur l'autoresponsabilité et des contrôles a posteriori.

Pour toute entreprise qui souhaite se mettre durablement en conformité et protéger efficacement son patrimoine de données, l'adoption d'un système de gouvernance des risques ("GRC") devient incontournable.

En soi, l'existence d'un suivi des risques démontre votre montée en maturité et envoie un signal positif à vos clients, à vos partenaires et aux auditeurs.

Cela pose deux grandes questions aux professionnels du risque et de la protection des données :

1. Quels seuils ou critères pour conduire des analyses des risques ?

Le RGPD et les lignes directrices associées décrivent les scénarios dans lesquelles les responsables doivent effectuer une analyse d'impact relative à la protection des données (AIPD) :

- soit le traitement envisagé figure dans la liste des types d'opérations de traitement pour lesquelles la CNIL a estimé obligatoire de réaliser une analyse d'impact relative à la protection des données ;
- soit le traitement remplit au moins deux des neuf critères issus des lignes directrices du G29.

2. Comment suivre les risques et contrôler les mesures correctives dans le temps ?

Si l'un des seuils énumérés est franchi, vous devrez conduire une AIPD avec les équipes impliquées dans l'activité considérée.

Or, ce type d'analyse de risque est encore nouveau pour beaucoup d'entreprises qui manquent de ressources pour appliquer et interpréter les clefs méthodologiques proposées par les autorités de contrôles.

Quelle que soit la méthode utilisée, les contributeurs devront documenter les évaluations de risques et leurs mesures préventives ou correctives suivantes :

- mesures garantissant la proportionnalité et la nécessité du traitement : expliciter et justifier les choix effectués pour respecter les grands principes de loyauté, de minimisation des données et de licéité des traitements (Articles 5 et 6 du RGPD) ;
- mesures protectrices des droits des personnes concernées : expliciter et vérifier l'effectivité des mesures concernant la transparence, le consentement, l'exercice des droits, les transferts et la sous-traitance ;
- mesures de sécurité visant à prévenir les atteintes à la vie privée : la qualification des risques repose ici sur une étude de (1) leur vraisemblance et (2) de leur gravité. L'analyse des sources de risque prend en compte tant les éléments organisationnels (ex. : mise en œuvre d'une politique d'accès) que les éléments techniques (ex. : application d'un protocole de chiffrement de bout en bout).

À chaque étape, les contributeurs vérifieront qu'il n'est pas opportun ou possible d'adopter des méthodes de traitement alternatives, moins risquées.

Par exemple :

- tester des outils d'analyses de données qui maximisent le ciblage de campagnes publicitaires tout en respectant la vie privée ;
- l'utilisation d'un prestataire d'hébergement certifié ISO qui adhère à des codes de conduite homologué ;
- réduire la durée de conservation des données ;
- limiter les accès aux bases de données des clients.

Le cas échéant, ces mesures non applicables en l'état sont consignées en attendant adoption et implémentation ultérieure. Cela favorise l'amélioration continue des traitements à risque.

Leto développe un module d'évaluation et de gestion des risques qui présélectionne les typologies de risques en fonction des catégories d'activités.

Ce gain de temps et d'analyse vous permet de vous concentrer sur la qualification des niveaux de risque et d'impact spécifiques à votre organisation et à votre activité.

11. SENSIBILISER ET FORMER VOS ÉQUIPES

Vos équipes sont au coeur du dispositif RGPD : pensez à les former en priorité

COMMENT SENSIBILISER ET FORMER VOS ÉQUIPES?

> **Oui, je sais ce qu’est le RGPD, je clique "refuser" sur les bannières cookies.**

> **Non le RGPD ne s’applique pas à cette base de données hashée car les données sont anonymes.**

Les DPO et leurs relais ont beaucoup œuvré ces dernières années pour faire monter en compétences l’ensemble des collaborateurs sur les enjeux du RGPD et de la protection des données.

Pourtant, de nombreuses entreprises tâtonnent encore dans leur stratégie de sensibilisation et de formation, laissant ainsi leur organisation à la merci du premier facteur de risque pour la sécurité des données : les salariés.

Selon une étude récente, 71% des DPO en France exercent dans une structure qui était dans l’obligation de désigner un DPO, ce qui signifie que les petites et moyennes structures manquent d’un appui interne pour garantir l’obligation de sensibilisation inscrite dans le RGPD.

Une stratégie gagnante de sensibilisation et de formation à la protection des données personnelles embarque les bonnes pratiques suivantes :

- des interventions ciblées et circonstanciées : une réunion plénière est l'occasion de sensibiliser aux enjeux stratégiques et la manière dont la culture de l'entreprise embrasse les principes de protection des données. À l'inverse, une réunion de lancement d'un projet doit véritablement former les contributeurs aux contraintes d'implémentation du RGPD et aux méthodes spécifiques d'évaluation de risques ;
- supports visuels et variés : distiller l'information dans des supports les plus interactifs possibles via différents médiums : des vidéos, des quizz, des jeux, des discussions-débats, des ateliers ;
- des outils de mesure du niveau et de la fréquence des sensibilisations et formations pour justifier votre conformité et informer la stratégie de protection des données de l'entreprise.

Les praticiens s’accordent à dire que plus les sensibilisations sont fréquentes et les formats variés, plus les réflexes sont solides.

C’est pourquoi Leto a développé des modules “no-code” de sensibilisation ciblés qui s’intègrent facilement à vos applications de messagerie sans développement additionnel.

Vous pouvez ainsi interroger ou insister rapidement et efficacement sur des points d’attention spécifiques, en temps réel auprès des collaborateurs et des équipes.

N’attendez pas le trimestre prochain pour parler RGPD avec vos équipes !

12. CONCLUSION

Ne craignez surtout pas le RGPD, au contraire, adoptez-le rapidement

CONCLUSION

La conformité au RGPD est moins complexe qu’on ne pourrait le craindre à la lecture des 99 articles qui le composent.

En effet, ses principes directeurs ne sont pas nouveaux et s’imbriquent naturellement avec les enjeux de croissance : confiance, transparence et excellence opérationnelle.

Or, la plupart des actions de conformité s’inscrivent dans un temps court, comprenant des tâches souvent répétitives et chronophages : mettre à jour des registres, répondre à des demandes de clients, compléter des cartographies de risques, sensibiliser des équipes, ajouter des clauses à un contrat...

Le risque est donc de décourager les collaborateurs qui participent (la plupart du temps volontairement) au développement du programme de conformité.

Une mise en œuvre efficace et durable de la protection des données personnelles revient donc à saisir les opportunités d'automatisation.

On reconnaît ici l'émergence des "Privacy Ops".

Ces spécialistes, de plus en plus plébiscités par les scale-up et les entreprises modernes de technologies, misent sur le déploiement d'outils puissants et collaboratifs pour assurer une application itérative, uniforme et transversale des mesures de protection des données.

En combinant gain de temps et optimisation des coûts, le bon outil permet à vos collaborateurs de rester concentrés sur leur cœur de métier.

Ils peuvent ainsi limiter leurs contributions à des tâches à valeur ajoutée : analyser les risques, proposer des solutions innovantes et prendre des décisions éclairées.

CONTACT

POSEZ-NOUS TOUTES
VOS QUESTIONS

E-MAIL :
contact@leto.legal

SITE WEB :
leto.legal