PROPOSITION D'ACCOMPAGNEMENT A LA MISE EN CONFORMITÉ RGPD

par

PIXALIA

Proposition rédigée le 22/03/2023 - Valable 3 mois

CLIENT	**CONSEIL**
Votre entreprise	PIXALIA - RGPD 77 Stéphane PARIS : 06 85 33 46 44 E-mail : stephane.paris@pixalia-services.fr

NOTRE VISION

Stéphane PARIS
Consultant
cybermalveillance
et RGPD

“ Pour une société, le respect de la vie privée permet d'augmenter et de conserver le paramètre confiance des utilisateurs ou des clients, un élément majeur dans la relation client et usager.”

Notre Objectif : Accompagner nos clients dans la mise en conformité RGPD afin de les rendre autonomes et responsables.

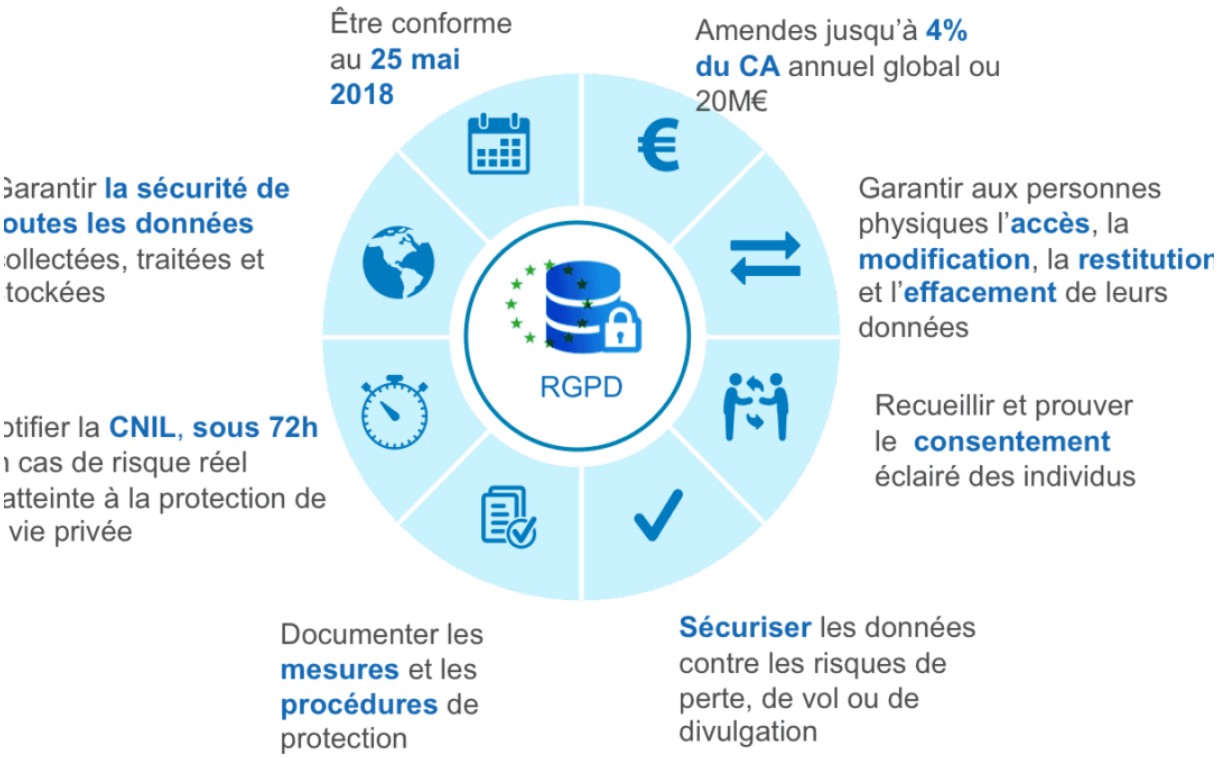
CONTEXTE DE LA PRESTATION

C’est fait, depuis le 25 mai 2018, le nouveau règlement sur la protection des données (RGPD) est pleinement entré en vigueur.

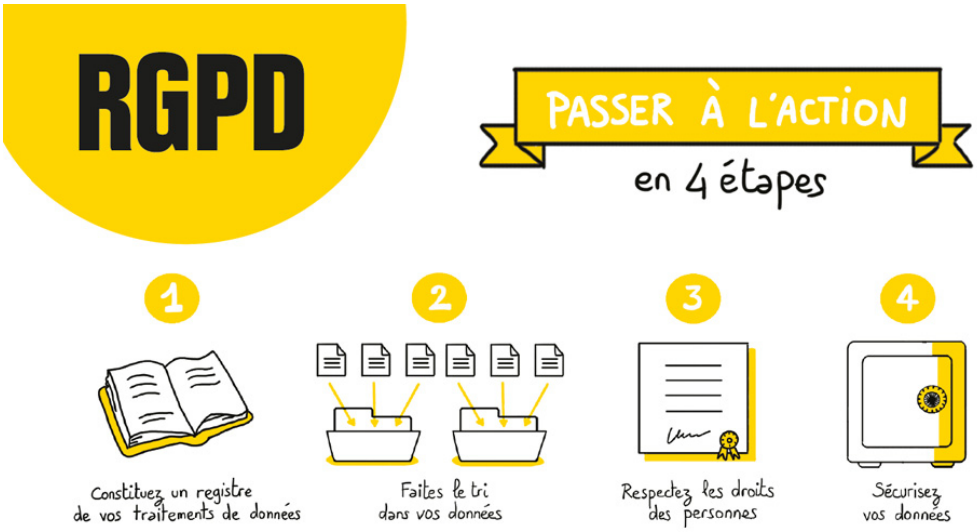
Il vient changer en profondeur la manière dont les organisations vont gérer les données des personnes avec qui elles interagissent (client, prospects, employés, partenaires…).

Si vous avez réussi à vous conformer à la nouvelle réglementation avant le 25 mai, vous vous mettez à l’abri des sanctions relativement sévères prévues. Sinon, pas de panique. Il n’est pas encore trop tard ! Mais il faut agir rapidement.

La conformité avec le RGPD constitue déjà la preuve du sérieux de l’entreprise.



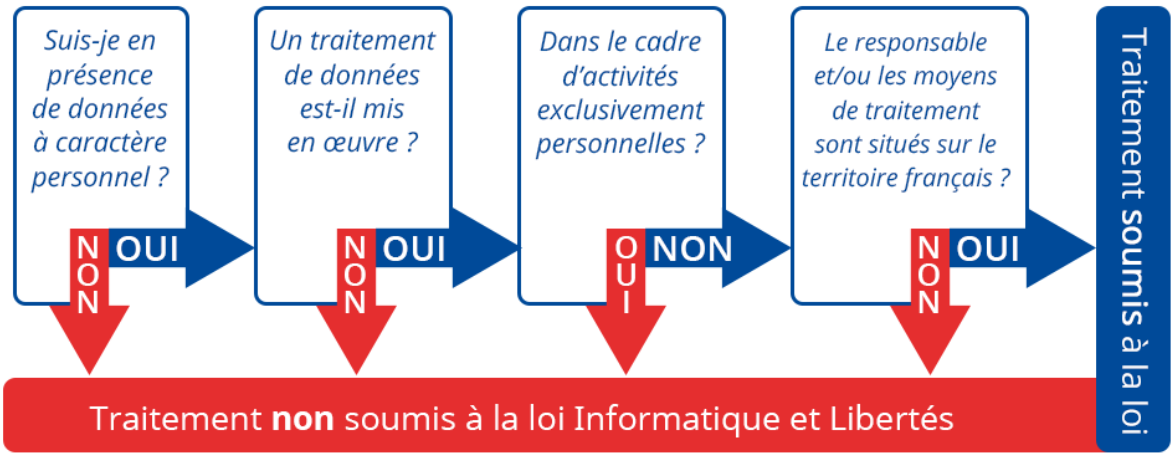
Notre méthodologie



1 - Nous constituons un registre de vos traitements de données

Ce document vous permet de recenser tous vos fichiers et bases de données et d'avoir une vision d'ensemble.

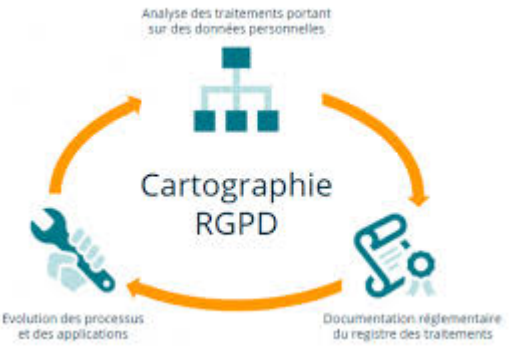
Nous identifions les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données.



Exemples : recrutement, gestion de la paie, formation, gestion des badges et des accès, statistiques de ventes, gestion des clients prospects, etc.

Dans votre registre, nous créons une fiche pour chaque activité recensée, en précisant :

- L'objectif poursuivi (la finalité - exemple : la fidélisation client) ;
- Les catégories de données utilisées (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;
- Qui a accès aux données (le destinataire - exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
- La durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).



Le registre est placé sous la responsabilité du dirigeant de l'entreprise.

Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'entreprise susceptibles de traiter des données personnelles.

En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données.

2 - Nous vous aidons à faire le tri dans vos données

La constitution du registre vous permet de vous interroger sur les données dont votre entreprise a réellement besoin.

Pour chaque fiche de registre créée, nous vérifions que :

- les données que vous traitez sont nécessaires à vos activités (par exemple, il n'est pas utile de savoir si vos salariés ont des enfants, si vous n'offrez aucun service ou rémunération attachée à cette caractéristique) ;
- vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter (voir la fiche « Traitements de données à risque : êtes-vous concerné ? ») ;
  seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- vous ne conservez pas vos données au-delà de ce qui est nécessaire.

A cette occasion, nous vous accompagnons à améliorer vos pratiques comme minimiser la collecte de données, en éliminant de vos formulaires de collecte et vos bases de données toutes les informations inutiles.

Nous vous aidons à redéfinir qui doit pouvoir accéder à quelles données dans votre entreprise. Dans la mesure du possible, nous poserons des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications

3 - Nous vous conseillons pour respecter les droits des personnes

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, etc.).

Informez les personnes

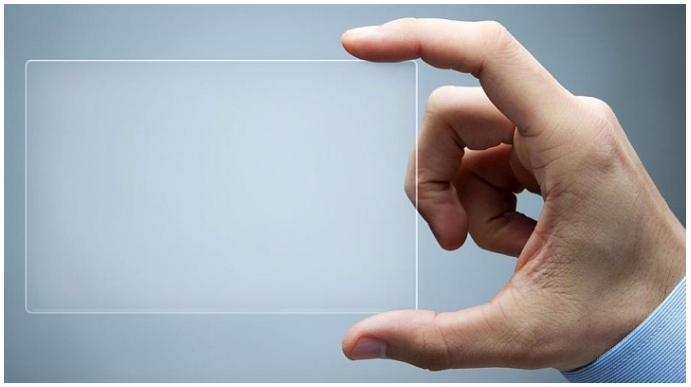
A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.

Nous vérifions que l'information comporte les éléments suivants :

- pourquoi vous collectez les données (« la finalité » ; par exemple pour gérer l'achat en ligne du consommateur) ;
- ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime ») ;
- Qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.) ;
- Combien de temps vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle ») ;
- Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;
- Si vous transférez des données hors de l'UE (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, nous pouvons par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à une politique de confidentialité / page vie privée sur votre site internet.

À l'issue de cette étape, nous aurons répondu ensemble à votre obligation de transparence.



Permettre aux personnes d'exercer facilement leurs droits

Les personnes dont vous traitez les données (clients, collaborateurs, prestataires, etc.) ont des droits sur leurs données, qui sont d'ailleurs renforcés par le RGPD : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.

Vous devez leur donner les moyens d'exercer effectivement leurs droits. Si vous disposez d'un site web, nous prévoirons un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, il faudra donner à vos clients la possibilité d'exercer leurs droits à partir de leur compte.

Nous vous aiderons à mettre en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

Bien traiter les demandes des consommateurs quant à leurs données personnelles c'est:

- renforcer la confiance qui sécurise la relation-client ;
- vous mettre à l'abri de critiques sur les réseaux sociaux, ou de réclamations auprès de la CNIL.

À l'issue de cette étape, vous serez en capacité de répondre aux demandes des personnes concernées.

4 - Nous vous aidons à sécuriser vos données

Si le risque zéro n'existe pas en informatique, vous devez prendre les mesures nécessaires pour garantir au mieux la sécurité des données. Vous êtes en effet tenu à une obligation légale d'assurer la sécurité des données personnelles que vous détenez.

Notre expertise dans la sécurité informatique et la cyber-malveillance nous permet de vous faire les recommandations et l'accompagnement technique dans la mise en oeuvre des solutions de sécurité nécessaire à la protection des données personnelles que vous manipulez.

Vous garantissez ainsi l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas de d'incident.

Des réflexes doivent être mis en place : mises à jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement de vos données dans certaines situations. En cas de perte ou vol d'un outil informatique, il sera plus difficile pour un tiers d'y accéder.

ASTUCE

Demandez à votre responsable informatique ou votre prestataire combien de fois vos utilisateurs activent la fonctionnalité « oubli de mot passe » chaque année. Si ce taux est faible voire nul, c'est que

votre politique de gestion des mots de passe n'est pas assez exigeante !

Les failles de sécurité ont également des conséquences pour ceux qui vous ont confié des données personnelles : Ayez à l'esprit les conséquences pour les personnes de la perte, la divulgation, la modification non souhaitée de leurs données, et prenez les mesures nécessaires pour minimiser ces risques.

BONNE PRATIQUE

Pour évaluer le niveau de sécurité des données personnelles dans votre entreprise, voici quelques questions à se poser :

- *Les comptes utilisateurs internes et externes sont-ils protégés par des mots de passe d'une complexité suffisante ?*
- *Les accès aux locaux sont-ils sécurisés ?*
- *Des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?*
- *Avez-vous mis en place une procédure de sauvegarde et de récupération des données en cas d'incident ?*

Signalez à la CNIL les violations de données personnelles

Votre entreprise a subi une violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou vous avez constaté un accès non autorisé à des données) ?

Vous devez la signaler à la CNIL dans les 72 heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Cette notification s'effectue en ligne sur le site internet de la CNIL.

Si ces risques sont élevés pour ces personnes, vous devrez les en informer.

À l'issue de cette étape, vous serez en capacité d'assurer une protection des données personnelles en continu et de faire face aux incidents.

PROPOSITION

DEVIS

Nature de la prestation	Tarif HT
ETAPE 1 ET 2 : RECENSEMENT DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL **Mission de 1 à 3 jours comprenant :** ● Audit et de collecte d'informations dans vos locaux avec les responsables de traitements (3x½ journée chez le client) ● Traitement des information collectées comprenant la revue des moyens de collects, les contrats, les processus internes (½ à 1 j) ● Identification de tous vos sous-traitants sur leur conformité RGPD (½ j) ● Restitution (½ j) Livrables (*) : - Registre des traitements permettant de répondre aux obligations de l'article 30. - Rapport d'audit avec recommandation sur les données, les moyens de protections et les moyens de collecte et définition du plan d'action	2800€HT
EN OPTION SUITE A NOTRE AUDIT : **ETAPE 3 : DÉFINITION DES CHANTIERS RGPD A MENER** 1 réunion de travail sur la qualification des chantiers (3h-4h) Formalisation du plan d'action	Sur devis
ETAPE 4 : GESTION DE PROJET TECHNIQUE SUR LES CHANTIERS DÉFINIS Basé sur le plan d'action et en fonction des besoins d'accompagnement, nous proposons un accompagnement technique et organisationnel sur votre plan d'action.	Selon les besoins d'accompagnement

*** L'ensemble de ses documents constituent les éléments démontrant votre action sur la mise en conformité RGPD de votre entreprise en cas de contrôle de CNIL.**

MODALITÉS DE PAIEMENT

Nous vous proposons un paiement comprenant un **acompte de 30% du montant TTC des prestations** à la commande. Le solde à la livraison des livrables ou des opérations.

Sauf délai de paiement supplémentaire convenu par accord entre les deux parties et figurant sur la facture, le paiement s'effectue au plus tard au 30ème jour suivant la date de facturation (C. Com. art L. 441-6, al.2 modifié de la loi du 15 mai 2001). Tout retard de paiement pourra donner lieu à des pénalités de retard exigibles sans rappel, au taux de 10% de la facture totale par mois de retard (Lutte contre les retards de paiement / article 53 de la Loi NRE), ainsi qu'à une indemnité forfaitaire de 40€ (C. Com. art. D441-5).

PLANNING

A réception de votre commande ou à une date convenue d'un commun accord, respectant notre plan de charge au moment de la commande, nous débuterons la réalisation de la mission.

La mission sera planifiée dans le temps en fonction de vos disponibilités afin d'effectuer la mission dans les meilleures conditions d'échanges avec les personnes impliquées dans l'entreprise.

CONDITIONS GÉNÉRALES DE VENTE

PRESTATION

La prestation comprend tout ce qui est explicitement listé dans le cadre de cette présente proposition. De façon corollaire, elle ne comprend pas ce qui n'est pas explicité dans cette même proposition. Les tarifs indiqués ne comprennent pas, sauf indication du contraire dans le devis :

- L'achat de solutions techniques et informatiques pour votre entreprise.
- Les frais de déplacement éventuels pour des déplacement en dehors des départements suivants (75,77,93,94)

ASSISTANCE

Le présent contrat prévoit une assistance en termes de conseil pendant une durée de 3 mois à compter de la date de fin de mission et ceux dans la limite de 2 heures d'assistance par mois.

CONFIDENTIALITÉ ET FICHIERS CLIENTS SOURCES

PIXALIA garantit la confidentialité des informations fournies par le client.

Le client s'engage à fournir, à la demande de PIXALIA tous les éléments nécessaires à la bonne réalisation de la mission. PIXALIA s'engage à les restituer ou à les détruire en fin de mission.

RESPONSABILITÉS

Il est rappelé que le Prestataire est tenu à une obligation de moyens. Il doit donc exécuter sa mission conformément aux règles en vigueur dans sa profession et en se conformant à toutes les données acquises dans son domaine de compétence.

Sa responsabilité pourra être engagée s'il est établi qu'il a manqué à son obligation de moyens. En revanche, elle ne pourra pas être engagée en cas de retard résultant d'une cause indépendante de sa volonté.

RETARD ET RUPTURE DU CONTRAT

Si le présent contrat ne pouvait être réalisé en tout ou en partie, du fait de causes indépendantes de la volonté de PIXALIA, sa responsabilité ne pourrait être engagée.

En cas d'incapacité de travail des personnes de PIXALIA ayant les compétences pour intervenir sur les différents éléments du projet, par suite de maladie ou d'accident, PIXALIA se réservent le droit de modifier le calendrier en cours et/ou de rompre le présent contrat, sans qu'il ne puisse être exigé par le client le versement d'indemnités. Il est admis que PIXALIA se doit d'avertir, dans la mesure du possible, le client dès le premier jour ouvrable d'incapacité et le cas échéant proposer une solution alternative.

Fait en 2 exemplaires ;

Paraphe sur toutes les pages
Signature (accompagnées de la mention lu et approuvé) :

CLIENT **PRESTATAIRE**