bpifrance

LAB

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

GUIDE PRATIQUE DE SENSIBILISATION AU RGPD

POUR LES PETITES ET MOYENNES ENTREPRISES

LES GRANDES ÉTAPES POUR PROTÉGER
LES DONNÉES PERSONNELLES
DE VOTRE ENTREPRISE

PASSEZ
À L'ACTION

Le guide pratique
de sensibilisation
au RGPD des petites
et moyennes entreprises
a uniquement pour
objectif de sensibiliser
les PME à mettre
en œuvre leurs propres
dispositifs de protection
des données,
dont elles sont seules
et entièrement
responsables.

AVANT-PROPOS

Les données sont omniprésentes et désormais au cœur de la chaîne de création de valeur des entreprises. Bien gérées et sécurisées, elles permettent de gagner en efficacité et en compétitivité, de personnaliser et de conforter la relation avec les clients, de conquérir de nouveaux marchés, d'améliorer les produits et services et de faciliter la collaboration et la mobilité. Pour s'adapter aux enjeux du numérique et garantir une meilleure maîtrise des données personnelles, une nouvelle régulation européenne, le Règlement Général sur la Protection des Données (RGPD), entre en application le 25 mai 2018. Il renforce les droits des personnes et responsabilise davantage les organismes publics et privés qui traitent leurs données.

Si les données personnelles ne sont pas au cœur de votre activité, les moyens à déployer pour vous mettre en conformité au RGPD ne seront pas très importants !

En effet, le critère à prendre en compte est **le volume ou la sensibilité des données traitées** et non pas la taille ou le nombre d'employés d'une entreprise.

Ce règlement dans votre entreprise n'est donc pas obligatoirement un projet technique ou juridique, il s'agit avant tout de bon sens et d'organisation.

Au-delà du respect de la règlementation, le RGPD offre aussi des opportunités de nouveaux business et peut, en ce sens, constituer un projet d'entreprise et être créateur de valeur.

La CNIL, régulateur des données personnelles, et **Bpifrance,** qui accompagne le développement des entreprises, ont décidé d'unir leurs forces pour élaborer ce « *Guide pratique de sensibilisation au RGPD* » à destination des PME.

Il vous propose des clés de compréhension pratiques pour engager au sein de votre entreprise, petite ou moyenne, une démarche de conformité au RGPD, et faire progresser votre entreprise dans sa maturité numérique.

Ce guide ne répondra pour autant pas nécessairement aux besoins spécifiques de chaque entreprise, seul un aperçu des principales réflexions à mener et actions à mettre en œuvre est abordé.

Le site de la CNIL dispose de nombreux contenus pour ceux qui souhaiteront accéder à une documentation plus technique et plus complète.

Toutes les entreprises, dont les TPE et PME, ont à traiter des données permettant d'identifier des personnes physiques.

À cet égard, le 25 mai 2018 constitue une étape cruciale : la protection de ces informations est en effet renforcée avec l'entrée en application du « Règlement Général sur la Protection des Données » (RGPD).

Au-delà des obligations légales à comprendre et à respecter, préparer son entreprise à ce nouveau cadre européen représente une opportunité de sécurisation et de protection de ses données. La responsabilité accrue des entreprises dans la gestion de leurs données, alliée aux principes de transparence et de loyauté, constitue le fondement de la confiance entre acteurs économiques et citoyens. C'est aussi un vecteur d'accélération de la maturité digitale de l'entreprise.

Développer son activité en conformité avec le RGPD, c'est aussi (re)découvrir la richesse que constituent les données personnelles pour une entreprise. Leur valorisation, dans une démarche éthique, permet à celle-ci de créer des services innovants, qui plus est de façon harmonisée pour l'ensemble du marché européen.

Pour vous aider dans votre démarche de mise en œuvre, ce guide vous rappelle, de façon simple, les avantages que vous pouvez en obtenir, les principales notions à connaître ainsi que les actions essentielles à engager.

Isabelle Falque-Pierrotin,
Présidente de la CNIL

Nicolas Dufourcq,
Directeur général Bpifrance

AU SOMMAIRE

POUR QUOI...

01.

... CE NOUVEAU RÈGLEMENT ?

L'acronyme RGPD signifie : « Règlement Général sur la Protection des Données » [1].

Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…).

Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française « *Informatique et Libertés* » de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

Il harmonise les règles en Europe en **offrant un cadre juridique unique** aux professionnels. Il permet de développer leurs activités numériques au sein de l'Union européenne en se fondant sur la confiance des utilisateurs.

Pour mettre fin à une distorsion de concurrence désavantageant parfois les entreprises européennes, les mêmes obligations sont imposées aux entreprises établies hors de l'Union européenne, dès lors qu'elles proposent des produits ou services aux résidents européens.

Il n'existe pas d'exceptions à ces obligations pour les PME françaises. Toutefois, selon leur activité, elles seront plus ou moins concernées par cette législation.

En effet, l'approche du RGPD est fondée sur la notion de gestion de risques, offrant ainsi des marges de manœuvre pour définir des solutions sur mesure.

En tant qu'entrepreneur, ces nouvelles obligations vous inciteront notamment à plus de transparence dans vos relations avec vos interlocuteurs : clients, salariés, prospects, fournisseurs, etc.

Faire comprendre la manière dont vous utilisez leurs données personnelles et leur donner la possibilité de les maîtriser, renforcera la confiance et favorisera donc votre activité, y compris à l'export.

[1] En anglais « *General Data Protection Regulation* » ou GDPR.

QUI EST CONCERNÉ PAR LE RGPD ?

Tout organisme quels que soient sa taille, son pays d'implantation et son activité, peut être concerné.

En effet, le RGPD s'applique à toute organisation, **publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :**

- qu'elle **est établie sur le territoire de l'Union européenne ;**
- que son activité cible directement **des résidents européens.**

Par exemple, une société établie en France, qui exporte l'ensemble de ses produits en dehors de l'Union européenne doit respecter le RGPD. De même, une société établie en dehors de l'Union européenne, proposant un site de e-commerce en français livrant des produits en France doit respecter le RGPD.

Le RGPD **concerne aussi les sous-traitants** qui traitent des données personnelles pour le compte d'autres organismes.

Ainsi, si vous traitez ou collectez des données pour le compte d'une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées (voir chapître 5 « *La sous-traitance* », page 44).

À RETENIR

Le RGDP met sur le même pied d'égalité les entreprises établies au sein de l'Union européenne et celles basées hors d'Europe et met fin à une distorsion de concurrence.

02.

QUELS SONT...

...
LES 6
AVANTAGES
POUR
VOTRE PME ?

Plus qu'une obligation légale, se conformer à la nouvelle réglementation sur la protection des données est une occasion de se questionner sur son approche de la data et de sa transformation numérique.

Le RGPD constitue une opportunité économique pour votre entreprise.

1. Renforcer la confiance

Toute personne qui vous confie ses données personnelles établit avec vous une relation de confiance et souhaite le respect de ses droits et de sa vie privée.

Le RGPD réaffirme les droits pour les personnes concernées de maîtriser leurs données en leur conférant des droits : droits d'accès, de rectification, d'effacement, d'opposition, etc. Respecter ces droits contribue à **valoriser votre image d'entreprise sérieuse et responsable.**

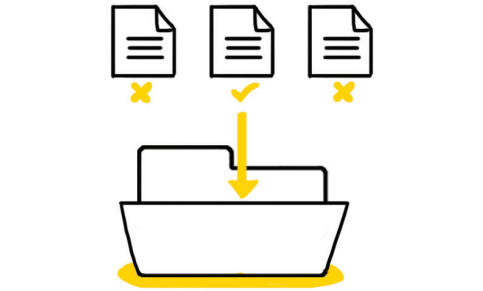
Une opportunité de sceller une relation de confiance avec vos interlocuteurs et d'**améliorer votre image de marque !**

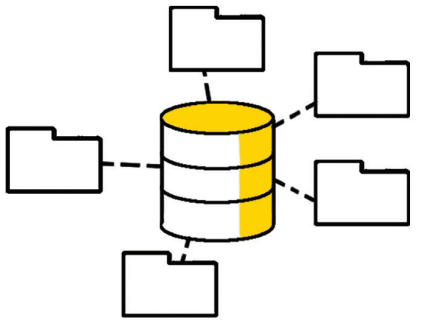
2. Améliorer votre efficacité commerciale

Pour vendre vos produits ou vos services, vous avez besoin de prospecter, de connaître vos clients et de gérer la facturation. Pour cela, vous constituez des fichiers concernant vos clients et prospects.

Si le RGPD réaffirme le principe d'exactitude et de mise à jour des données enregistrées dans un fichier, maintenir vos fichiers à jour est surtout dans l'intérêt même du développement de votre chiffre d'affaires.

En ayant une gestion rigoureuse de vos données, vous **gagnez donc en efficacité et en productivité !**





3. Mieux gérer votre entreprise

Avec le temps et le développement de votre entreprise, votre volume de données augmente et nécessite de mobiliser de plus en plus de moyens humains et techniques (espace de stockage, logiciels adaptés, etc.) pour les gérer, les mettre à jour, et en assurer la sécurité.

Le principe de « minimisation » des données (« *Je ne collecte que les données dont j'ai vraiment besoin* ») et l'obligation de tenir à jour la liste de vos fichiers vous permettent de faire le point sur les données que vous collectez et d'identifier vos besoins réels.

Le RGPD exige par ailleurs que les données soient pertinentes par rapport à l'objectif pour lequel vous collectez les données.

Appliquer ces principes vous permet donc d'**optimiser vos investissements.**

L'arrivée du RGPD est ainsi une occasion forte de **se poser les bonnes questions sur son activité et ses process** (comme cela a été par exemple le cas lors du passage du papier à la dématérialisation).

4. Améliorer la sécurité des données de votre entreprise

L'actualité témoigne d'un nombre de plus en plus important de failles de sécurité et d'attaques informatiques. Ces dernières peuvent avoir des conséquences désastreuses sur l'activité des entreprises. Le niveau de sécurité de l'entreprise dans sa globalité se pose en préalable à la sécurité des données.

Au même titre que vous protégez le nom de votre PME ou son logo, vitaux pour le fonctionnement de votre entreprise, **les données personnelles doivent faire l'objet de mesures de sécurité particulières,** informatiques et physiques.

Protéger son patrimoine informationnel et protéger les personnes concernées des atteintes à leurs données, c'est donner à son entreprise des moyens de **se développer sereinement.**

5. Rassurer vos clients et donneurs d'ordre et ainsi développer votre activité

Dans tous les secteurs d'activité, les donneurs d'ordre seront très attentifs à la mise en œuvre du RGPD par leurs prestataires.

Il s'agit donc d'un sujet crucial pour les sous-traitants qui traitent des données personnelles pour le compte d'entreprises, à la fois pour maintenir leurs relations commerciales existantes mais également pour éventuellement en conquérir de nouvelles.

Si vous respectez le RGPD, vous aurez un **avantage concurrentiel !**

6. Créer de nouveaux services

Le RGPD introduit aussi de nouveaux concepts pouvant se traduire en nouveaux services (exemple : la portabilité des données).

Le développement et l'organisation de ces nouveaux outils et services représentent de véritables défis et de nouvelles opportunités économiques (exemple : sur les plateformes en ligne pour la musique, les vidéos, l'utilisateur pourrait à terme faire exporter ses choix, ses listes de préférences, etc.). L'utilisateur final pourrait fortement gagner en termes d'expérience, ces éléments entreront alors dans sa décision d'achat !

POUR ALLER PLUS LOIN :
« ***Guide Bpifrance Digitalisation des PME*** »

À RETENIR

La mise en conformité au RGPD peut parfois être complexe, même si cela sera rarement le cas pour une PME.

Soyez vigilants : certains acteurs peu scrupuleux profitent du RGPD pour proposer des prestations excessivement coûteuses ou générer des appels surtaxés. Renseignez-vous sur leurs compétences et références avant d'entrer en relations d'affaires.

Et au préalable, commencez par la lecture de ce guide ! Il vous sensibilisera et vous donnera les premiers éléments de langage pour échanger avec vos éventuels prestataires.

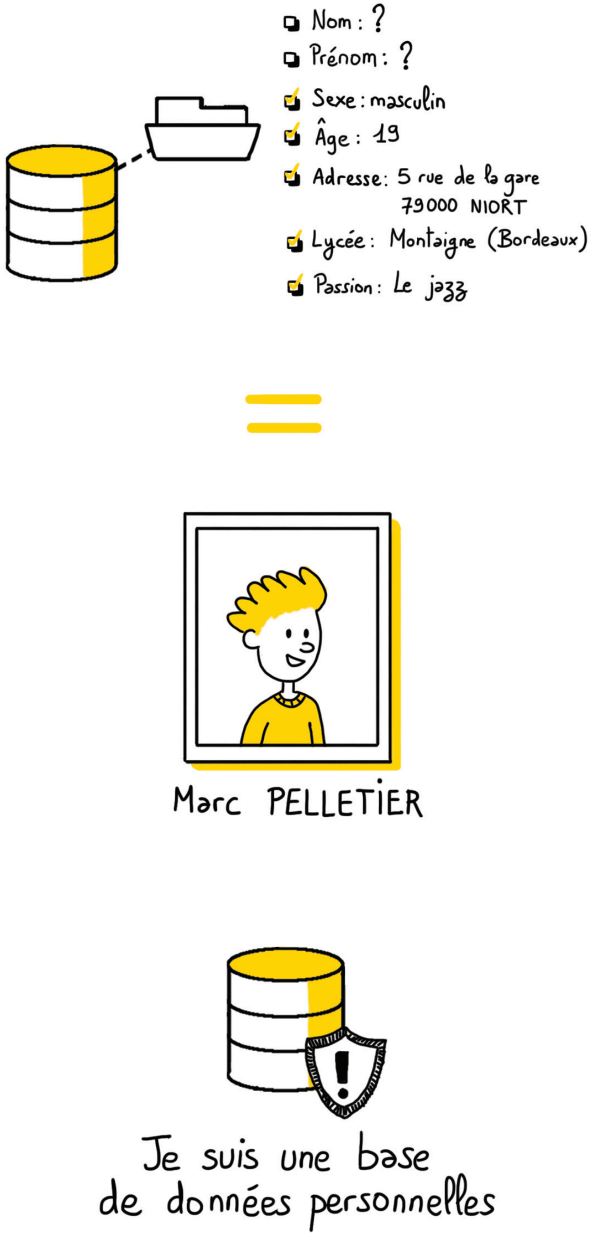
RGPD
LES 6 AVANTAGES

1. **Renforcer** la confiance
2. **Améliorer** votre efficacité commerciale
3. **Mieux gérer** votre entreprise
4. **Améliorer** la sécurité des données de votre entreprise
5. **Rassurer** vos clients et donneurs d'ordre et ainsi développer votre activité
6. **Créer** de nouveaux services

DONNÉES PERSONNELLES, TRAITEMENT DE DONNÉES :

03.

... DE QUOI PARLE-T-ON ?



QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne peut être identifiée :

- **directement** (exemple : nom, prénom) ;
- **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- **à partir d'une seule donnée** (exemple : numéro de sécurité sociale, ADN) ;
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association).

EXEMPLE

Une base marketing contenant de nombreuses informations précises sur la localisation, l'âge, les goûts et les comportements d'achats de consommateurs, y compris si leur nom n'est pas stocké, est considérée comme un traitement de données personnelles, dès lors qu'il est possible de remonter à une personne physique déterminée en se basant sur ces informations.

QU'EST-CE QU'UN TRAITEMENT DE DONNÉES PERSONNELLES ?

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

EXEMPLES DE TRAITEMENT

Tenue d'un fichier de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, etc.

Par contre, un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles.

Un traitement de données personnelles **n'est pas nécessairement informatisé :** les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Un traitement de données doit avoir un objectif, une finalité, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour. À chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de votre activité professionnelle.

Je m'assure que les données collectées servent bien l'objectif prévu

EXEMPLE

Vous collectez sur vos clients de nombreuses informations, lorsque vous effectuez une livraison, éditez une facture ou, proposez une carte de fidélité. Toutes ces opérations sur ces données constituent votre traitement de données personnelles ayant pour objectif la gestion de votre clientèle.

04.

COMMENT...

... PASSER À L'ACTION ?

Voici
les 4 actions principales
à mener pour entamer votre mise en conformité aux règles de protection des données.

Ces actions doivent perdurer dans le temps pour être efficaces.

1. RECENSEZ VOS FICHIERS

Le registre listant vos traitements de données vous permettra d'avoir une vision d'ensemble.

Identifiez les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données (exemples : recrutement, gestion de la paye, formation, gestion des badges et des accès, statistiques de ventes, gestion des clients prospects, etc.).

Appuyez-vous sur le modèle de registre proposé par la CNIL sur son site internet.

Dans votre registre, créez 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.

Vous n'avez pas en revanche à mentionner au registre les traitements purement occasionnels (exemple : fichier constitué pour une opération événementielle ponctuelle comme l'inauguration d'une boutique).

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

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

2. FAITES LE TRI DANS VOS DONNÉES

Pour chaque fiche de registre créée, vérifiez :

- 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) ;
- que vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter (voir chapître 6 « *Traitements de données à risque : êtes-vous concerné ?* », page 50) ;
- que seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- que vous ne conservez pas vos données au-delà de ce qui est nécessaire.

À cette occasion, améliorez vos pratiques !

Minimisez la collecte de données, en éliminant de vos formulaires de collecte et vos bases de données toutes les informations inutiles. Redéfinissez qui doit pouvoir accéder à quelles données dans votre entreprise. Pensez à poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

BONNE PRATIQUE

Échanger avec d'autres entrepreneurs d'entreprises comparables ou consulter votre fédération professionnelle vous aidera à mieux appréhender la mise en œuvre du RGPD.

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

3. RESPECTEZ LES DROITS DES PERSONNES

Informez les personnes

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

Vérifiez que l'information comporte notamment 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'Union européenne** (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

Des exemples de mentions sont disponibles sur le site internet de la CNIL.

Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez 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, vous avez répondu à votre obligation de transparence.

Permettez 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, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, donnez à vos clients la possibilité d'exercer leurs droits à partir de leur compte.

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

BONNE PRATIQUE : SOYEZ RÉACTIFS !

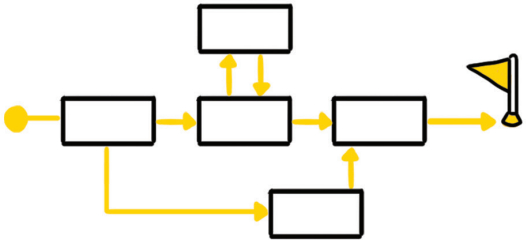
Bien traiter les demandes des consommateurs quant à leurs données personnelles, c'est :

- *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.

POUR EN SAVOIR PLUS :
« *Dossier respecter les droits des personnes* »
sur le site internet de la CNIL

Je donne les moyens aux personnes d'exercer leurs droits sur leurs données



Je mets en place un processus interne pour le traitement des demandes

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 d'assurer la sécurité des données personnelles que vous détenez.

4. SÉCURISEZ VOS DONNÉES

Garantissez 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 d'incident.

Différentes actions doivent être mises 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.

BONNE PRATIQUE

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.

EXEMPLE

Vous êtes restaurateur et vous livrez à domicile. Vos clients vous communiquent leur adresse précise et le code d'entrée de leur immeuble. Si ces informations sont piratées ou perdues, elles peuvent être utilisées pour s'introduire frauduleusement au domicile de votre client. Conséquence désastreuse pour vos clients, mais aussi pour vous !

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 ?*

POUR EN SAVOIR PLUS :

« *Guide des bonnes pratiques de l'informatique* » réalisé par l'ANSSI et la CPME sur le site internet www.cybermalveillance.gouv.fr

« *Guide sécurité des données personnelles* » sur le site internet de la CNIL

POUR VOUS AIDER :

En cas de difficultés (un sinistre, une attaque informatique, etc.), le site gouvernemental www.cybermalveillance.gouv.fr vous propose de l'aide en ligne ainsi qu'une liste de prestataires approuvés.

BONNE PRATIQUE

Une démarche d'anticipation sur le niveau global de sécurité peut être complétée par une approche assurantielle.

Renseignez-vous auprès de ces professionnels sur le contenu possible des polices d'assurance (responsabilité civile, dommages couverts…) et surtout sur les services à l'assuré (notamment l'assistance en cas de sinistre, de gestion de crise…).

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.

RGPD

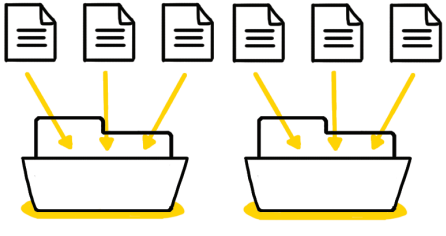
PASSEZ À L'ACTION

en 4 étapes

1

Constituez un registre de vos traitements de données

2

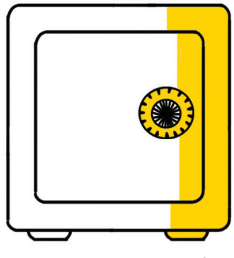


Faites le tri dans vos données

3

Respectez les droits des personnes

4



Sécurisez vos données

LA SOUS-TRAITANCE

05.

Le RGPD reconnaît le rôle des sous-traitants dans le traitement de données personnelles, et leur impose des obligations particulières.

QUI EST CONCERNÉ ?

Le sous-traitant est la personne physique ou morale qui traite des données personnelles pour le compte d'un autre organisme (le « responsable de traitement »), dans le cadre d'un service ou d'une prestation.

Vous êtes concerné, en qualité de **responsable de traitement,** si vous choisissez de confier la gestion de vos données personnelles à des prestataires qui seront vos sous-traitants (exemple : SSII, intégrateurs de logiciels, hébergeurs de données).

Vous êtes concerné, **en qualité de sous-traitant,** si votre entreprise traite des données personnelles sur instruction et pour le compte d'un autre organisme dans le cadre d'un service ou d'une prestation (exemple : vous effectuez des opérations de prospection commerciale pour le compte de vos clients).

QUE DOIVENT FAIRE LES SOUS-TRAITANTS ?

Les sous-traitants sont tenus de respecter des **obligations spécifiques** en matière de sécurité, de confidentialité et de documentation de leur activité.

Ils doivent prendre en compte l'objectif de protection des données personnelles et de la vie privée dès la conception de leur service (principe du « *privacy by design* ») ou de leur produit, et ils doivent mettre en place des mesures permettant de garantir une protection optimale des données.

EXEMPLE

Un éditeur de logiciel doit s'interroger dès la création de son outil sur les champs que ses clients pourront remplir dans le cadre de son objet. Dans un outil de gestion clients (CRM ou ERP), la présence de champs de texte libre pour insérer des commentaires suite à un contact client peut conduire, par exemple, à inscrire des propos excessifs ou non pertinents. Il est donc utile de prévoir des listes déroulantes de motifs de contacts à la place, qui seront objectifs et neutres.

EXEMPLE

Un hébergeur de données doit proposer à ses clients de purger automatiquement et sélectivement les données d'une base active à l'issue d'une certaine durée.

Les sous-traitants ont également une **obligation de conseil** auprès de leurs clients (exemple : insister auprès de ses clients pour les mises à jour de logiciel). Ils doivent les aider dans la mise en œuvre de certaines obligations du règlement (exemple : étude d'impact sur la vie privée, notification de violation de données, sécurité, etc.).

Les sous-traitants doivent enfin **tenir un registre des activités de traitement effectuées pour le compte de leurs clients** en complément de leurs propres traitements !

Pour déterminer les obligations respectives des responsables de traitements et de leurs sous-traitants, il est nécessaire de rédiger un contrat.

Ce contrat doit prévoir une clause spécifique sur la protection des données personnelles. Des exemples de clauses sont disponibles sur le site internet de la CNIL.

BONNE PRATIQUE

Médiation : vous pouvez prévoir et anticiper le recours à la médiation pour gérer un potentiel conflit.

POUR EN SAVOIR PLUS :
« *Guide RGPD pour les sous-traitants* »
sur le site internet de la CNIL

06.

TRAITEMENTS DE DONNÉES À RISQUE...

...

ÊTES-VOUS CONCERNÉ ?

Les données personnelles sont au cœur de votre modèle économique, vous mettez en place des services innovants, vous traitez des données sensibles ?

Une analyse approfondie de la règlementation est nécessaire pour déterminer les mesures à mettre en œuvre.

LES POINTS DE VIGILANCE

Certaines données ou certains types de traitements nécessitent une vigilance particulière :

Lorsque vous traitez certains types de données à risque

Sont notamment concernées les données dites « sensibles » :

- révélant l'origine prétendument raciale ou ethnique ;
- portant sur les opinions politiques, philosophiques ou religieuses ;
- relatives à l'appartenance syndicale ;
- concernant la santé ou l'orientation sexuelle ;
- génétiques ou biométriques.

Les données d'infraction ou de condamnation pénale font également l'objet de règles particulières. Ces données ne peuvent être utilisées que sous certaines conditions strictement encadrées par la loi Informatique et libertés et par le RGPD.

Lorsque votre traitement a pour objet ou pour effet :

1. l'évaluation d'aspects personnels ou notation d'une personne (exemple : scoring financier) ;
2. une prise de décision automatisée ;
3. la surveillance systématique de personnes (exemple : télésurveillance) ;
4. le traitement de données sensibles (exemple : santé, biométrie, etc.) ;
5. le traitement de données concernant des personnes vulnérables (exemple : mineurs) ;
6. le traitement à grande échelle de données personnelles ;
7. le croisement d'ensembles de données ;
8. des usages innovants ou l'application de nouvelles technologies (exemple : objet connecté) ;
9. l'exclusion du bénéfice d'un droit, d'un service ou contrat (exemple : liste noire).

Si vos traitements de données répondent à au moins 2 de ces 9 critères, vous devez, *a priori*, conduire une analyse d'impact sur la protection des données (PIA : Privacy Impact Assesment), avant de commencer les opérations de traitement.

En complément de l'établissement du registre et de la description du traitement, cette analyse de l'impact sur la vie privée vous permettra d'identifier les risques associés à ces données personnelles. Il ne s'agit donc pas du même travail.

POUR EN SAVOIR PLUS :
Sur les cas dans lesquels un PIA est nécessaire et comment l'élaborer :
« *Dossier PIA* »
sur le site internet de la CNIL

Lorsque vous transférez des données en dehors de l'Union européenne

Vérifiez si le pays hors Union européenne vers lequel vous transférez les données dispose d'une législation de protection des données et si elle est reconnue adéquate par la Commission européenne.

Une carte du monde présentant les législations de protection des données est à votre disposition sur le site de la CNIL.

Sinon, vous devrez encadrer juridiquement vos transferts pour assurer la protection des données à l'étranger.

POUR EN SAVOIR PLUS :
« *Dossier transférer des données hors de l'UE* »
sur le site internet de la CNIL

Si votre situation correspond à l'un ou à plusieurs de ces points de vigilance, une analyse approfondie du RGPD et de la loi Informatique et Libertés est nécessaire pour déterminer les mesures à mettre en œuvre.

Il est alors utile de se faire accompagner !

QUI CONTACTER POUR SE FAIRE AIDER ?

Dans certains cas, vous pourrez être conduits à désigner un délégué à la protection des données.

Cette désignation est obligatoire pour certaines entreprises opérant des traitements à grande échelle présentant des risques particuliers. Dans les autres cas, la désignation d'un délégué est recommandée notamment si votre activité vous impose de mener une analyse approfondie du RGPD.

Le délégué peut être désigné en interne parmi vos collaborateurs ou en externe. Il peut aussi être mutualisé entre plusieurs organismes ou au sein d'associations ou fédérations professionnelles.

POUR EN SAVOIR PLUS :
Sur les cas de désignation obligatoires et les compétences du délégué à la protection des données :
« *Dossier le délégué à la protection des données* »
sur le site internet de la CNIL

Si vos traitements de données sont susceptibles d'engendrer des risques spécifiques ou des problématiques nouvelles au regard de la protection des données, n'hésitez pas à vous informer auprès de la CNIL (modalités de contact sur la page « CONTACT » du site internet de la CNIL).

Par ailleurs, vos sous-traitants ont une obligation d'alerte et de conseil en matière de protection des données. N'hésitez-pas à les solliciter.

Collecter et traiter des données personnelles implique avant tout d'informer les personnes sur ce que vous faites de leurs données et de respecter leurs droits.

En tant que responsable d'un traitement de données, ou en tant que sous-traitant, vous devez prendre des mesures pour garantir une utilisation de ces données respectueuse de la vie privée des personnes concernées.

LES 6 BONS RÉFLEXES
DE LA PROTECTION DES DONNÉES PERSONNELLES

1. **Ne collectez que les données vraiment nécessaires**
   Posez-vous les bonnes questions : Quel est mon objectif ? Quelles données sont indispensables pour atteindre cet objectif ? Ai-je le droit de collecter ces données ? Est-ce pertinent ? Les personnes concernées sont-elles d'accord ?

2. **Soyez transparent**
   Une information claire et complète constitue le socle du contrat de confiance qui vous lie avec les personnes dont vous traitez les données.

3. **Pensez aux droits des personnes**
   Vous devez répondre dans les meilleurs délais, aux demandes de consultation, de rectification ou de suppression des données.

4. **Gardez la maîtrise de vos données**
   Le partage et la circulation des données personnelles doivent être encadrées et contractualisées, afin de leur assurer une protection à tout moment.

5. **Identifiez les risques**
   Vous traitez énormément de données, ou bien des données sensibles ou avez des activités ayant des conséquences particulières pour les personnes, des mesures spécifiques peuvent s'appliquer.

6. **Sécurisez vos données**
   Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

QUEL EST LE RÔLE DE LA CNIL ?

La Commission nationale de l'informatique et des libertés, (CNIL) est le régulateur français des données personnelles.

La CNIL accompagne les acteurs privés et publics dans la mise en œuvre de leur conformité en matière de protection des données personnelles.

Elle reçoit et traite les réclamations des particuliers et dispose des pouvoirs de contrôles sur place ou en ligne.

Elle peut imposer à un acteur de régulariser son traitement (mise en demeure) ou prononcer des sanctions (amende, etc.).

QUEL EST LE RÔLE DE BPIFRANCE ?

Bpifrance finance les entreprises, à chaque étape de leur développement, en crédit, en garantie et en fonds propres. **Bpifrance** les accompagne dans leurs projets d'innovation et à l'international.

Bpifrance assure aussi, désormais leur activité export à travers une large gamme de produits. Conseil, université, mise en réseau et programmes d'accélération font également partie de l'offre proposée aux entrepreneurs.

Grâce à **Bpifrance** et ses 48 implantations régionales, les entrepreneurs bénéficient d'un interlocuteur proche, unique et efficace pour faire face à leurs défis.

ZOOM SUR BPIFRANCE LE LAB

Bpifrance Le Lab est le laboratoire d'idées de Bpifrance lancé en mars 2014 pour « faire le pont » entre le monde de la recherche et celui de l'entreprise.

Bpifrance Le Lab est un agitateur d'idées pour Bpifrance et les dirigeants d'entreprises, de la startup à l'ETI.

Bpifrance Le Lab décrypte les déterminants de la croissance et éclaire les chefs d'entreprises dans un monde de ruptures à la fois économiques, sociétales et environnementales, avec 2 finalités :

- *participer à l'amélioration des pratiques de financement et d'accompagnement de Bpifrance ;*
- *stimuler la réflexion stratégique des dirigeants et favoriser la croissance de leur entreprise.*

Bpifrance Le Lab s'est doté de sa propre gouvernance, avec un conseil d'orientation composé de personnalités interdisciplinaires et présidé par Nicolas Dufourcq, Directeur général de Bpifrance.

Pour enrichir
vos connaissances,
consultez nos 3 fiches
pratiques :

- **Sachez que faire**
  quand votre entreprise
  communique et/ou vend en ligne
- **Améliorez et maîtrisez**
  votre relation client
- **Protégez les données**
  de vos collaborateurs

SERVIR L'AVENIR

Réf. : 1002-01

CNIL

3, Place de Fontenoy - TSA 80715
75334 Paris Cedex 07
Tél. : 01 53 73 22 22

Bpifrance

27-31, avenue du Général Leclerc
94710 Maisons-Alfort Cedex
Tél. : 01 41 79 80 00