Initialisation & sensibilisation au RGPD

Présentation du 14/06/2018

Initialisation & sensibilisation au RGPD

Présentation du 14/06/2018

PLAN DE L'INTERVENTION

1. Le RGPD en quelques mots
2. Les changements pour votre organisation
3. Qu'est ce qu'une donnée personnelle ?
4. Qu'est que le traitement d'une donnée personnelle ?
5. Votre organisation est-elle concernée ?
6. Par où commmencer ?
7. Votre organisation doit-elle désigner un DPO ?
8. RGPD au quotidien
9. Les durées de conservation
10. Les sanctions prévues par la loi
11. Conclusions
12. Cas pratiques : site web, réseaux sociaux, collaborateurs,...

ERIC EMERY - DIRIGEANT DE NATURAL-NET

Agence web et webmarketing à Bordeaux depuis 2007

- http://www.natural-net.fr/
- http://www.site-internet-qualite.fr/
- http://www.guide-creer-son-site-web.fr/

Assistant maître de conférences Université Bordeaux III

Interventions à la demande du Club des Entrepreneurs du Médoc sur :

- action de **sensibilisation globale au RGPD**
- **impact sur les sites web** pour les organisations et entreprises.

1. LE RGPD EN QUELQUES MOTS

Le Règlement Général sur la Protection des Données – RGPD – est entré en application le 25 mai 2018

C'est la 3ème phase de mise en libre circulation européenne (après les personnes et les marchandises).

Ce texte européen (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016) a des conséquences importantes sur le **recueil et le traitement des données** réalisés par les organismes/sociétés.

Voir le texte de loi européen :

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

ou https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680&from=FR

1. LE RGPD EN QUELQUES MOTS

Le RGPD s'applique quand :

Une **organisation européenne** traite des données personnelles

OU

Un **citoyen européen** est directement visé par un traitement des données.

Toutes les organisations sont à priori concernées (PME, PMI, mais aussi associations et organismes publics) dès lors qu'elles traitent des données personnelles.

Mais les travaux à mener en fonction des organisations et des types de données sont variables.

Les **sous traitants de ces organisations sont également impliqués** (c'est une nouveauté de la loi).

1. LE RGPD EN QUELQUES MOTS

Le texte a pour objectif de faire respecter de **nouvelles règles sur la protection des données**.

Ces droits et devoirs seront communs à tous les pays de l'Union. Le **RGPD protégera toutes les personnes présentes sur le territoire de l'Union Européenne** quelque soit leur nationalité et les feront bénéficier d'un meilleur contrôle de leurs données personnelles.

Les **entreprises** quant à elles bénéficieront d'un **processus réglementaire simplifié** : il leur faudra **"juste"** être en conformité avec le texte sans avoir à faire de déclarations comme c'est le cas parfois avec la législation actuelle.

1. LE RGPD EN QUELQUES MOTS

Cette réglementation engendre des contraintes pour toutes les organisations mais c'est aussi une source d'opportunités !

1. Renforcer la **confiance** vis à vis des cibles
2. Améliorer votre **efficacité commerciale** avec des fichiers qualitatifs
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** (principe de portabilité des données)

Processus favorable à la digitalisation des PME

Sources : https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

EXEMPLES PRATIQUES DE VIGILANCE

Amélioration du droit à l'oubli

La réglementation sur les données personnelles prévoit **d'améliorer l'usage du droit à l'oubli.** La législation élargira ce droit à l'oubli à celui du droit d'être prévenu si les données ont été piratées et au droit à **l'effacement et au transfert des données** vers un autre prestataire.

Supprimer votre compte

EXEMPLES PRATIQUES DE VIGILANCE

Limitation de la collecte des données

Pour récolter des informations sur des citoyens, toute entreprise qui a une activité de collecte, de traitement et d'utilisation des données **devra justifier d'un fondement légal. La récolte du consentement des personnes à la collecte et au traitement de leurs données devra répondre à de strictes conditions posées par le texte, un simple croix pré-cochée devenant interdite.**

L'entreprise devra selon le RGPD **limiter la collecte des données personnelles au strict minimum nécessaire** (notion de *privacy by design*). La durée de conservation des données devra être indiquée et ne pourra persister inutilement dans le temps : il faudra se référer aux référentiels existants (règlements, lois, recommandations de la CNIL...)

EXEMPLES PRATIQUES DE VIGILANCE

Les entreprises sont garantes de la sécurité et confidentialité des données. Les données à caractère personnel collectées et traitées devront être conservée de manière sécurisée.

Supposons que la base de données qui contient les informations de vos prospects et clients soit stockée sur l'espace administrateur de votre site.

Si cet espace est protégé par un code trop faible (alphabétique, sans chiffre, sans caractère spécial, etc.) et que votre site est piraté, vous risquez d'être tenu responsable de la fuite.

2. LES CHANGEMENTS POUR VOTRE ORGANISATION

De manière globale, le RGPD a forcément des conséquences sur votre organisation et nous vous invitons à consacrer du temps sur ce sujet qui doit être abordé de manière globale.

Consultez les importantes informations disponibles sur le site de la CNIL :

- **RGPD : Par quoi commencer** :
- https://www.cnil.fr/fr/rgpd-par-ou-commencer

- **RGPD : Vos obligations** :
- https://www.cnil.fr/fr/comprendre-vos-obligations
- **RGPD : Les outils de conformité** :
- https://www.cnil.fr/fr/les-outils-de-la-conformite

2. LES CHANGEMENTS POUR VOTRE ORGANISATION

Initier la démarche de mise en conformité sans attendre tout en prenant en compte la relative indulgence de la CNIL dans les mois à venir

Jean Lessi (secrétaire général de la Cnil) : « **Le 25 mai 2018 n'est pas une date couperet** »

Si le 25 mai 2018 ne doit pas être perçu comme une date couperet, mais comme une étape, il convient de se préparer dès maintenant. Le RGDP est un texte dense qui introduit de nouveaux principes, de nouvelles obligations. Collectivement, nous devons tous – régulateur et entreprises – participer dès à présent à sa bonne appropriation.

Source : https://www.zdnet.fr/actualites/jean-lessi-cnil-le-25-mai-2018-n-est-pas-une-date-couperet-39856876.htm

3. QU'EST CE QU'UNE DONNÉE PERSONNELLE ?

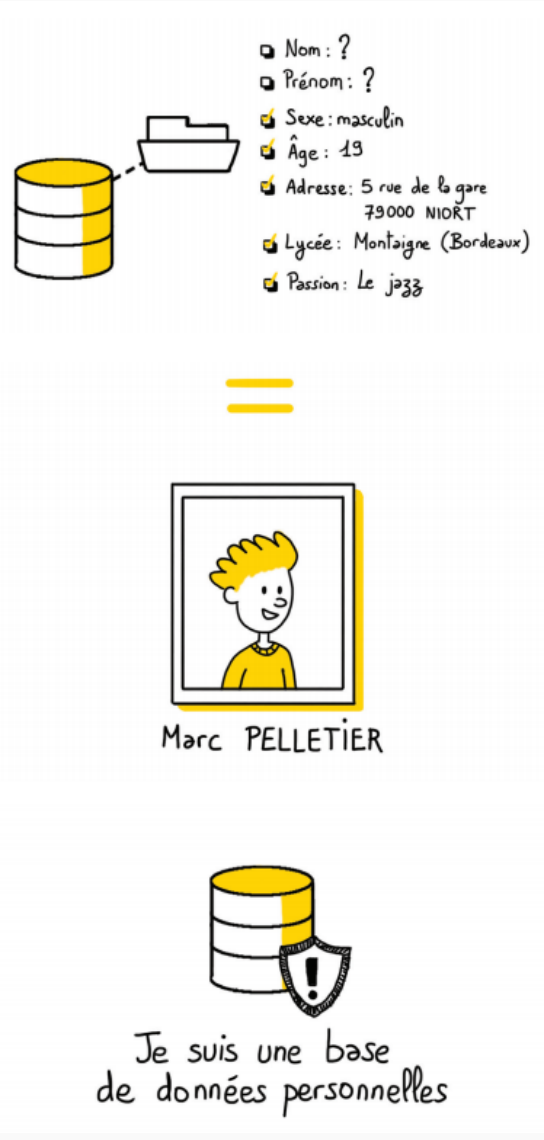
Une « **donnée personnelle** » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne peut être identifiée :

- directement (exemple : nom, prénom) ;
- indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, 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).



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

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.

5. VOTRE ORGANISATION EST-ELLE CONCERNÉE ?

La plupart des organisations sont concernées par le RGPD

Mais en fonction de :

- la **taille** de l'organisation
- le **volume** de données traitées
- la **sensibilité** des données traitées

Les impacts varient notablement pour votre organisation.

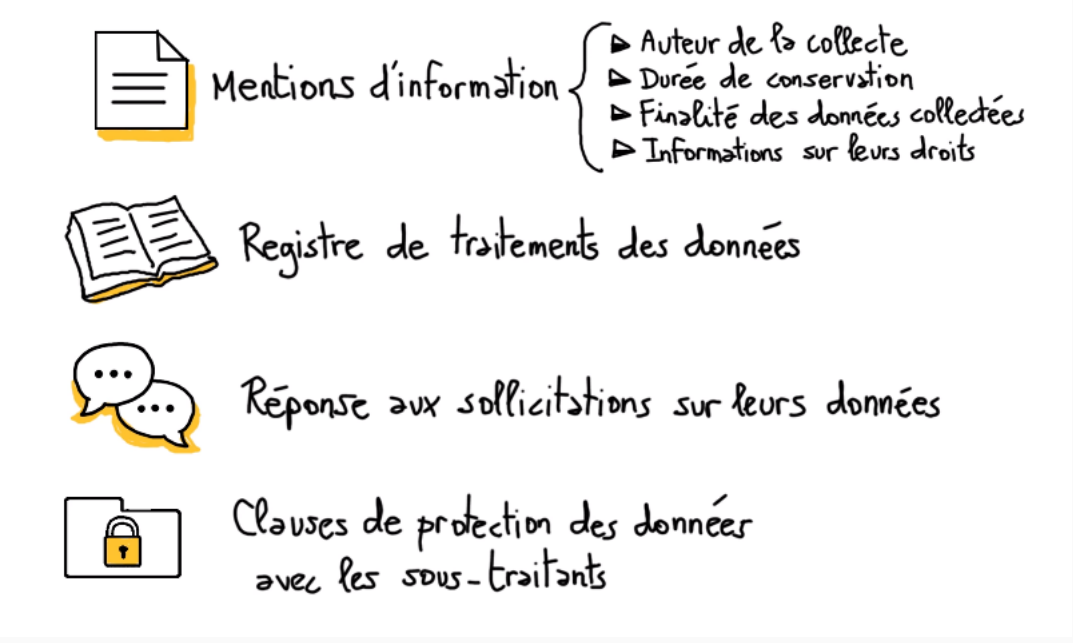
Données sensibles (article 9 RGPD**)**

" Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. ."

5. MON ORGANISATION EST-ELLE CONCERNÉE ?

Le cas des associations

Les associations sont également concernées et doivent s'impliquer dans la mise en conformité au RGPD, ses devoirs sont minimisés mais elles doivent prendre en compte et respecter :



Sources : https://www.cnil.fr/fr/rgpd-passer-a-laction

5. MON ORGANISATION EST-ELLE CONCERNÉE ?

Le cas des auto entrepreneurs

Toutes les entreprises sont concernées par le Règlement européen sur la protection des données (RGPD). Les **autoentrepreneurs également** :

- Si ils collectent, stockent, utilisent des données à caractère personnel. Dans ce cas, les entreprises sont "responsables de traitements".
- Si ils traitent des données à caractère personnel pour le compte d'autres entreprises. Dans ce cas, les entreprises sont "sous-traitantes".

Sources : https://www.federation-auto-entrepreneur.fr/actualites/auto-entrepreneur-et-rgpd-que-faire

6. PAR OÙ COMMENCER ?

Les **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.

Sources : https://www.cnil.fr/fr/rgpd-par-ou-commencer

6. PAR OÙ COMMENCER ?

6.1. Constituer un registre

Ce document **recense tous vos fichiers** et apporte une vision d'ensemble. Identifiez les **activités principales** de votre entreprise qui nécessitent la collecte et le traitement de données (recrutement, gestion de la paye, statistiques de ventes, gestion des clients prospects,...). Créez une **fiche pour chaque activité** recensée :

- **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, 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).

Modèles de registre : https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

6.2. Faites 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, 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) ;

  - 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, améliorez vos pratiques, purgez vos anciennes données non conformes !

6.3. Respectez les droits des personnes : Information

C'est l'**obligation d'information et de transparence** à l'égard des personnes dont vous traitez les données (clients, collaborateurs,...). A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des **mentions d'information** :

- Pourquoi vous collectez les données (« la **finalité** ») ;
- 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** a accès aux données (services internes, prestataires, 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** (retrait & rectification) ;

6.4. Respectez les droits des personnes : droit de retrait & de rectification

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.

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

6.5. Sécurisez vos données

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.

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.

Sources : https://www.cnil.fr/fr/rgpd-par-ou-commencer

6.6. Sécurisez vos données : déclarez un incident

Si votre entreprise 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.

Sources : https://www.cnil.fr/fr/rgpd-par-ou-commencer

7. VOTRE ORGANISATION DOIT-ELLE NOMMER UN DPO ?

Le Délégué à la Protection des données ou Data protection officer (DPO) : ses missions

Sources : https://www.cnil.fr/fr/rgpd-passer-a-laction

7. VOTRE ORGANISATION DOIT-ELLE NOMMER UN DPO ?

Le **Délégué à la Protection des données** n'est pas obligatoire pour toutes les structures, mais toutes les structures peuvent nommer un DPO et le déclarer auprès de la CNIL (https://www.cnil.fr/fr/designation-dpo).

Sources : https://www.cnil.fr/fr/rgpd-passer-a-laction

8. RGPD AU QUOTIDIEN

Une fois les étapes initiales de mise en conformité au RGPD traitées (identification des fichiers, purge des fichiers), vous devez **garantir la conformité au quotidien** par la mise en place de routines et mécanismes permettant :

- De **respecter les délais de conservation** des données prévues,
- De **préserver la sécurité** des données (changements de mot de passe,...),
- De **prendre en compte pour l'ensemble des activités** et **contrats** avec les partenaires, clients, prospects, sous-traitants, salariés, stagiaires,... l'ensemble des aspects et dispositifs liés au RGPD.

Le RGPD ne change pas tout !

Le RGPD ne remplace pas l'ensemble des législations en vigueur, les délais de conservation de données spécifiques (factures, bulletins de paye,...) sont maintenues & les **relations clients-fournisseurs** restent encadrées par le contrat, les CGV,... comme avant le RGPD.

9. LES DURÉES DE CONSERVATION DES DONNÉES

Ce que dit la loi :

"Les données personnelles doivent donc être conservées et accessibles par les services opérationnels uniquement le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte."

Dans les faits :

La durée de conservation doit être définie par le responsable du fichier, sauf si un texte impose une durée précise. Cette durée dépend de la nature des données et des objectifs poursuivis.

- Les données relatives à **gestion de la paie** ou au contrôle des horaires des salariés peuvent être conservées pendant **5 ans.**
- Les données figurant dans un **dossier médical** doivent être conservées **10 ans** à compter de la consolidation du dommage.
- La Cnil recommande que les **coordonnées d'un prospect** qui ne répond à aucune sollicitation pendant **3 ans** soient supprimées.

Source : https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

10. LES SANCTIONS PRÉVUES PAR LA LOI

Des sanctions financières élevées

Le RGPD prévoit des sanctions extrêmement dissuasives :

- Jusqu'à **10 millions d'euros** ou, dans le cas d'une entreprise, **2% du chiffre d'affaires annuel mondial** pour des manquements notamment au *Privacy By Design*, *Privacy By Default*,...
- Jusqu'à **20 millions d'euros** ou, dans le cas d'une entreprise, **4% du chiffres d'affaires annuel mondial** pour manquement notamment aux droits des personnes (droits d'accès, de rectification, d'opposition, de suppression, droit à l'oubli, etc.).

Et des sanctions administratives & pénales

Les sanctions pénales en cas de manquement aux règles en matière de protection des données sont déjà prévues en droit français et réprimées par les articles 226-16 à 226-24 du Code pénal.

Source : https://www.haas-avocats.com/ecommerce/rgpd-focus-sur-les-sanctions/

11. CONCLUSIONS

Le RGPD apporte une **protection plus importante des données personnelles** et est censée favoriser des **innovations importantes** pour tous (comme la portabilité des données).

Toutes les organisations sont concernées par le RGPD et se doivent au plus tôt d'entamer des démarches de mise en conformité, les organismes de contrôle comme la CNIL feront preuve d'indulgence pendant quelques mois, mais **à terme le non respect du RGPD peut entrainer des sanctions importantes**.

En cas de contrôle le fait d'avoir **initié des démarches** et de progresser dans le temps dans la mise en conformité de l'organisation aura toujours un **effet positif**.

12. CAS PRATIQUE : LE SITE WEB

Dans le cas d'un **site web "simple"** disposant de formulaires de contact, de newsletter les recommandations sont les suivantes :

1. Page spécifique “Protection des Données personnelles”

Cette page indique aux internautes de manière claire et précise

- Responsable du traitement
- Finalités du ou des traitement(s)
- Type de données collectées
- Durée de conservation des données
- Destinataires des données
- Hébergeurs et localisation des données hébergées
- Modalités de droit d’accès, de modification et de droit à l’oubli

Exemple : https://www.natural-net.fr/donnees-personnelles.html

2. Ajout de la demande de consentement éclairée dans les formulaires

Pour **chaque formulaire présent sur le site** (formulaire de contact, de création de comptes, de commentaires de blog,...) doit être proposée une demande de consentement préalable, conforme aux exigences du RGPD (libre, spécifique, éclairé, univoque, révocable...) indiquant :

- les **finalités** de traitements des données collectées.
- les **destinataires** des données collectées.
- la **durée de conservation** des données.

Exemple : https://www.natural-net.fr/site-internet-bordeaux-paris.html

3. Droit de suppression et droit de rectification

Le site Internet doit proposer des **moyens simples & accessibles** pour qu'un citoyen puisse exercer ses **droits de suppression et de rectification des données :**

- Si vous proposez aux internautes de disposer de comptes, vous devez proposer sur le site un **formulaire de suppression de compte** qui supprimera les données associées à ce compte client et lui confirmera cette action par mail.
- Vous devez pour tout formulaire collectant des données **hors comptes clients/membres proposer aux internautes une procédure de droit de rectification et de droit à l'oubli** (par mail, courrier,...)

Exemple : https://www.natural-net.fr/donnees-personnelles.html

4. Cas des cookies collectant des données personnelles

Un **cookie** est un petit fichier texte au format alphanumérique déposé sur le disque dur de l'internaute par le serveur du site visité ou par un serveur tiers (régie publicitaire, service de web analytique, etc.) qui **mémorise et collecte des informations** dont certaines peuvent être des données personnelles.

Le site web doit

- informer les internautes sur les cookies utilisés sur votre site collectant des données personnelles (services par services)
- permettre à l'internaute de continuer sa navigation malgré le refus de certain cookies

Exemple : https://www.natural-net.fr/

5. Conséquences pour votre entreprise

Comme la plupart des organisations vous devez :

- au plus tôt **assurer la conformité de votre site au RGPD** & parallèlement adapter vos processus internes et votre organisation pour respecter le RGPD sur le long terme,
- décider des **actions menées sur les fichiers de données personnelles collectées de manière non conformes au RGPD** :

  > en **sollicitant un nouvel opt-in des** personnes physiques présentes dans vos fichiers.

  > en **supprimant** ces fichiers et toutes archives de ces données.

Exemple : https://www.natural-net.fr/donnees-personnelles.html

12. CAS PRATIQUE : LES RESEAUX SOCIAUX

Sur les réseaux sociaux

Depuis Twitter, Facebook, et autres réseaux sociaux, il est recommandé :

- De **rendre accessible un article ou un lien qui mène vers une page d'information sur les droits**. Anticipez les effets d'une opération de communication en ligne (emailing par exemple).
- De **prévoir une réponse type** aux internautes mécontents, qui exerceraient, par exemple leur droit d'opposition. La réactivité et l'efficacité de votre réponse contribuent à votre réputation en ligne (ou e-reputation).

Exemple : https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche-1_que-faire-quand-votre-entreprise-communique-vend-en-ligne.pdf

12. CAS PRATIQUE : LES COLLABORATEURS

Les recommandations

- **Minimiser les données collectées** : ne demandez à vos employés que les informations utiles pour accomplir leurs missions,
- **Informez vos collaborateurs** à chaque fois que vous leur demander des informations,
- Assurez-vous d'en garantir la **confidentialité** et la **sécurité**. Ainsi, seules les **personnes habilitées** doivent en prendre connaissance.

Source : https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche_3_protegez-les-donnees-de-vos-collaborateurs.pdf

12. CAS PRATIQUE : LA RELATION CLIENT

Les recommandations

- **N'utilisez pas des données personnelles** librement accessibles sur internet sans prendre des **précautions**.
- Soyez **vigilant** sur les bases de données marketing en vente sur internet à des prix particulièrement attractifs.
- Utilisez des **fichiers « qualifiés »**, c'est-à-dire comportant des données fiables concernant des personnes qui seront a priori attirées par l'offre ou le service que vous proposez.
- Dans tous les cas, les **personnes doivent pouvoir refuser** de recevoir d'autres sollicitations de votre part.

Source : https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche_2_ameliorez-maitrisez-votre-relation-client_0.pdf

Des Questions ?

Contactez notre agence web :

05.56.17.75.19.

contact@natural-net.fr