CP DESIGN
CONCEPTION GRAPHIQUE & WEB

Tél. 06 14 88 88 85
e-mail : christophe@cporlier-design.com
www.cporlier-design.com

Le RGPD pour les webmasters

Le nouveau Règlement Général sur la Protection des Données européen (RGPD) prendra effet le 25 mai 2018 dans tous les pays de l'UE en même temps.

Cette nouvelle législation impose de nouvelles règles strictes de protection de la vie privée à toutes les entreprises qui traitent des données personnelles.

Même si ce règlement semble viser en premier lieu les GAFA qui ont largement abusé de leurs positions dominantes, il concerne potentiellement toutes les entreprises européennes ou qui traitent avec les européens.

Types de données concernées

Toutes les données permettant identifier directement ou de rendre identifiables par croisement d'informations des personnes physiques (ex. récupération d'adresses IP et recoupement avec d'autres données).

Elles sont de 3 types :

- Données d'identification : e-mail, nom, prénom, …
- Données sensibles : ethniques, religieuses, de santé, sexuelles, syndicales, …
- Données comportementales : contenus consultés, achats, recherches, téléchargements, …

Type de personnes protégées

Tous les utilisateurs d'interfaces informatiques, d'applications ou de site Web (clients, prospects, fournisseurs, salariés, demandeurs d'emploi, …).

Les simples nom et prénom d'une personne qui travaille dans une entreprise sont considérés comme données personnelles (ex. dans adresses e-mail professionnelles de type prénom.nom@société.com).

Cela signifie que sont concernés également tous les utilisateurs B to B et pas uniquement les visiteurs de sites B to C.

Nouveauté incontournable du règlement

Pour obtenir et conserver les données personnelles, il faut maintenant **demander et enregistrer la permission** de la personne.

Cette permission devra être active, explicite et informée.

Active

La personne devra faire une action claire pour donner son autorisation (ex. case à cocher obligatoire, sinon blocage de l'enregistrement).

Explicite et informée

La demande devra contenir une définition exacte des données recueillies et de l'utilisation qui en sera faite (ex. Vos données seront utilisées pour vous envoyer de l'information ou faire une relance commerciale).

Si la personne accepte, c'est uniquement pour l'utilisation décrite et aucune autre.

L'information doit également être faite sur les droits de la personne par rapport aux données qu'elle consent à laisser.

Renforcement de droits

L'utilisateur de l'interface doit pouvoir

- modifier,
- supprimer,
- obtenir ses données dans un format ouvert (csv, xml, …) pour leur portabilité,
- demander à être effacé (droit à l'oubli),
- refuser le profilage.

Conservation des données

La durée de conservation doit être définie au départ est limitée dans le temps (en conformité avec les directives du RGPD).

Une nouvelle demande d'autorisation est nécessaire si l'on souhaite prolonger l'exploitation des données.

Obligations administratives

L'entreprise responsable du traitement doit avoir un processus pour la gestion des bases de données qu'elle exploite.

Le règlement impose maintenant une fiche par base de données et un registre récapitulatif des données traitées.

Responsabilités

Les entreprises qui exploitent les données sont en premier lieu responsables mais, à partir du 25 mai 2018, la responsabilité des sous-traitants est susceptible d'être engagée en cas de manquement.

Tout prestataire de services (agences web, webmasters, consultants informatiques, webmarketeurs, …) doit désormais respecter plusieurs obligations s'il traite des données pour le compte de son client (sécurité, confidentialité, alerte, …) mais lui doit également assistance et conseil pour sa mise en conformité avec le RGPD.

Mon site est-il concerné ?

Pour ce qui concerne la gestion de sites web, voici les cas principaux qui traitent des données personnelles pour lesquels il va falloir se mettre en conformité avec le RGPD.

En fait, très peu de site ne sont pas concernés par le RGPD, surtout s'il y a un CMS (Content Manager Service) derrière qui s'appuie immanquablement sur une base de données.

Site avec formulaire de contact

Une simple adresse e-mail contenant nom et prénom est une donnée personnelle.

Site utilisant scripts et plugins tiers

pour la bonne marche du site ou des utilisations moins transparentes : mesures d'audience, réseaux sociaux, régies pub, lecteurs vidéo, APIs, … Tous ces services gratuits qui installent des cookies et permettent à leurs éditeurs de récupérer des données comportementales précieuses sur les utilisateurs.

Exemple : Google Analytics récupère les adresses IP de vos visiteurs et peut, par recoupement, donner des infos précises sur leurs centres d'intérêts s'ils utilisent d'autres services de Google. Dans ce cas, l'adresse IP permet d'accéder à des données personnelles, elle doit être déclarée et doit faire l'objet d'un consentement.

Pour en savoir plus sur ces services, reportez-vous à l'annexe en fin de document.

Christophe PORLIER - Consultant – e-mail : christophe@cporlier-design.com – Tél. 06 14 88 88 85

Dès qu'il y a ouverture de compte
pour accéder à des forums, des téléchargements, des services, des devis en ligne, …

Site de e-commerce
Cas typique d'utilisation de données personnelles où l'on recueille nom, e-mail, tél, adresse de livraison, éventuellement informations de carte bancaire et où, bien souvent, le comportement du visiteur/acheteur est traqué à des fins de relance commerciale.

Site d'offre d'emploi
ou sites d'entreprises qui offrent des postes avec possibilité de postuler en ligne où l'on recueille nom, e-mail, date de naissance, études, jobs, …

Le RGPD va être très sensible aux traitements des services RH qui devront justifier l'utilisation de toutes les données et leur sécurité.

Site de jeux ou de sondages
Souvent mis en place pour collecter de l'information marketing.

Anciennes bases de données
Pour des newsletters, par exemple. Même si un double opt-in a été appliqué (accord sur formulaire confirmé par un lien e-mail personnalisé), il manquera sûrement les informations sur la durée et l'utilisation des données.

Les mesures imposées par le RGPD sont rétroactives. Un consentement tacite n'est pas possible.

Comment se mettre en conformité ?

Site avec formulaire de contact
La consigne du RGPD est très stricte sur la **minimisation des données**. Il faut toujours se poser la question « cette donnée est-elle nécessaire ? » et demander uniquement les données utiles au traitement déclaré et aucune autre.

Pour les mineurs, des précisions sont à venir, mais une autorisation parentale sera au minimum nécessaire.

Le formulaire doit comporter une **case à cocher pour le consentement** devant une mention de style « En envoyant ce formulaire, j'accepte que les informations saisie soient exploitées dans le cadre de […] » et une **mention sur les droits** de l'utilisateur avec un lien vers la page précisant la politique de confidentialité.

Il faut **conserver la preuve du consentement**, même pour un simple formulaire réceptionné sur e-mail sans traitement automatique (le mail devra contenir le détail du consentement).

Le consentement doit **informer sur la durée de conservation**. Pour prolonger, il faut demander à nouveau l'autorisation (ex. pour les cookies, le consentement doit être renouvelé tous les 13 mois).

La CNIL a fixé une durée **conservation maximale de 3 ans** pour les données des **personnes non-actives** dans une base de données.

Il faut **garder une preuve de la suppression** des données dans un fichier à part, hors serveur et crypté, idéalement.

Pour la **sécurité de transfert des données**, le **HTTPS** est maintenant imposé par l'Europe. Tous les hébergeurs proposent des certificats pour adopter ce protocole.

Un **processus** doit permettre aux utilisateurs de **modifier, supprimer, recevoir une copie** de leurs données. Légalement, cela doit être fait sous un délai d'un mois, manuellement ou automatiquement avec preuve.

Une **fiche** de base de données et un **registre** doivent être **tenus à jour**.

E-mails marketing, newsletters

Les **mêmes principes que pour les formulaires** sont à appliquer au moment de l'inscription du visiteur avec double opt-in de consentement.

Un lien de désabonnement bien visible, un rappel des droits de l'utilisateur et les coordonnées de l'entreprise responsable doivent être intégrés au message envoyé qui ne doit porter que sur le contenu déclaré à l'inscription.

Site utilisant scripts et plugins de tracking ou de profilage

Tout ce qui utilise des cookies, sessions, logs, etc pour traquer les clics, les visites, les téléchargements, les accès à contenu, les partages, les achats, etc et peut concerner des personnes identifiables - et pas uniquement identifiées immédiatement - doit maintenant faire l'objet d'une **explication sur la finalité de la collecte** d'informations et **définir clairement la durée** de conservation des données pour **permettre le consentement éclairé** de l'utilisateur.

Même si les données sont collectées par les éditeurs des plug-ins et que vous ne les utilisez pas vous même directement, **si vous les intégrez à votre site, vous êtes responsable** de leur propagation.

Il est donc conseillé de vérifier et d'**utiliser uniquement des services conformes** au RGPD.

En attendant la mise en conformité de ces services, une solution transitoire consiste à intégrer à votre site un **gestionnaire de tag** permettant à l'utilisateur de gérer lui-même les cookies et d'en réduire les actions (ex. la solution tarteaucitron qui est recommandée par la CNIL).

Site de e-commerce

Ces sites utilisent beaucoup de techniques de **tracking d'e-mails et de profilage d'achat** où l'acheteur potentiel est identifié. Cela doit maintenant être **fait avec le consentement de l'utilisateur** qui doit aussi pouvoir demander à faire un achat sans être profilé ou à être effacé des listes.

Les données qui ne présentent plus d'intérêt doivent être supprimées sans délai (paniers oubliés, achats non finalisés, articles consultés, …).

Les **mêmes contraintes que pour le formulaires** sont applicables dans ce cas : minimisation, mentions des droits, durée de conservation, preuve de consentement et de suppression, sécurité de transfert, possibilités d'accès et tenue de fiche et registre.

Le consentement en bonne et due forme devra être redemandé aux clients existants.

La CNIL précise que les informations des **cartes bancaires ne peuvent pas être conservées** au delà du temps de la réalisation de l'opération de paiement. La mémorisation d'une carte pour faciliter de futurs achats devient donc impossible

Site proposant des emplois

Tous ce qui est lié aux relations humaines est fortement impacté par les règles du RGPD. Les données utilisées sont considérées comme données très personnelles, voire sensibles.

Lorsqu'un candidat répond à une offre d'emploi, il doit savoir **quel usage précis sera fait des données** qu'il laisse.

Les **mêmes contraintes que pour le formulaires** sont applicables dans ce cas : minimisation, consentement, mentions des droits, durée de conservation, preuve de consentement et de suppression, sécurité de transfert, possibilités d'accès et tenue de fiche et registre.

Site de jeux ou de sondages

Il va falloir être très clair sur la finalité de la collecte des données et bien **expliquer pourquoi le jeu ou le sondage sont organisés.**

Dans la mesure où cela est précisément fait pour récolter de manière peu transparente des données, il est probable que ce type de pratiques perdra en efficacité si elles respectent le RGPD.

Pour autant, les **mêmes contraintes que pour le formulaires** sont applicables dans ce cas : minimisation, consentement, mentions des droits, durée de conservation, preuve de consentement et de suppression, sécurité de transfert, possibilités d'accès et tenue de fiche et registre.

Pour compléter sa mise en conformité

Les mentions légales

Obligatoires depuis longtemps, elles devront être **mises à jour en mentionnant les nouvelles exigences du RGPD** et en expliquant votre politique de confidentialité : respect du RGPD, notions de permissions et des droits des utilisateurs.

Ne pas les modifier pourrait alerter les autorités sur le fait que vous n'êtes pas en conformité.

La protection des données

Il y a maintenant obligation légale à **sécuriser leur transit et leur stockage** et à **restreindre leur accès.**

En cas de violation des données, il faudra alerter la CNIL et les utilisateurs par une procédure contraignante.

Il est donc fortement conseillé de prendre les mesures suivantes pour éviter les problèmes :

- Passer son hébergement en HTTPS pour protéger le transfert de données (voir solutions proposées par votre hébergeur)
- Utiliser des solutions de cryptage si des données personnelles sont hébergées, surtout si ce sont des données sensibles (voir solutions proposées par votre hébergeur)
- Disposer d'une solution Firewall au niveau du serveur (voir solutions proposées par votre hébergeur)
- S'assurer que votre CMS utilise un plugin de sécurité

Certaines pratiques sont à bannir :

- Utiliser des solutions Cloud hors CEE
- Stocker les mots de passe en clair
- Utiliser un protocole de transfert non-sécurisé
- Choisir un algorithme de hachage faible
- Utiliser des Apps externes non-conformes

Pensez aussi à :

- Authentifier les utilisateurs / Gérer les habilitations
- Tracer les accès et gérer les incidents
- Sécuriser le hardware (fixes, portables, mobiles, objets)
- Sécuriser les serveurs et les réseaux
- Archiver de manière sécurisée
- Encadrer la maintenance et la destruction des données
- Gérer la sous-traitance
- Sécuriser les échanges avec d'autres entreprises

La conservation trop longue des données peut occasionner des risques. Pour information, la CNIL a définit quelques délais maximum qui seront complétés à l'avenir :

- Données sensibles : redemander le consentement des personnes tous 6 mois (+ Accord explicite de base)

- Personnes inactives : supprimer les données tous les 3 ans
- Cookies : tous les 13 mois (redemander le consentement)
- Vidéo surveillance : 1 mois
- Gestions des données des salariées : 5 ans
- Carte bancaire : suppression immédiate sauf demande explicite
- En cas d'attaque : 72h pour prévenir la CNIL

Liens utiles

Toutes les informations de ce document sont des conseils et des indications pour mener votre propre réflexion sur votre mise en conformité au RGPD (source Pierre Cat).

Pour compléter vos connaissances sur ce sujet, vous pouvez consulter les liens suivants et vous trouverez sur le site de la CNIL bien d'autres informations utiles :

https://www.cnil.fr/comprendre-le-reglement-europeen

https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement

https://www.cnil.fr/fr/declarer-un-fichier

https://www.cnil.fr/fr/declaration/ns-048-fichiers-clients-prospects-et-vente-en-ligne

https://www.cnil.fr/fr/garantir-la-securite-des-donnees

Il est de votre responsabilité de réaliser toutes les démarches nécessaires au respect de ce nouveau règlement.

Certaines règles nécessitent des modifications de fonctionnalités et de contenus sur vos interfaces web pour lesquelles nous pouvons intervenir ou vous aider.

Nous restons à votre disposition pour tout complément d'information.

Annexe

Liste indicative et non exhaustive de scripts et plugins pouvant récupérer et exploiter des données personnelles à l'insu des utilisateurs et pour lesquels il faudra s'assurer à l'avenir de la conformité au RGPD.

Formulaires : Contact Form +, Gravity Forms, Ninja Forms, QuFrom, …

Mesure d'audience : Alexa, Clicky, CrazyEgg, FeRank, Get+, Google Ananlytics, StatCounter, Visual revenue, Xiti, …

Régie publicitaire : Amazon, ClickManager, Criteo, FeRank Pub, Google Adsense, Google Adwords, Pubdirecte, Twenga, VShop, …

Commentaires : Disquq, Facebook Commentaire, …

Réseaux sociaux : Addthis, Addtoany Feed, Addtoany Share, Ekom, Facebook, Shareaholic, Sharethis, …

Support en ligne (chat) : Uservoice, Zopim, …

Lecteurs vidéo : Calameo, Daily Motion, Prezi, SlideShare, Viméo, Youtube, …

Christophe PORLIER - Consultant – e-mail : christophe@cporlier-design.com – Tél. 06 14 88 88 85