

Parc d'Activités Schweitzer
26 rue du Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

# FICHE CONSEIL

**Nous tenons à préciser que ce document a été rédigé par Alexandre JOLY et issu de son excellent blog sur la sécurité informatique et la sensibilisation des TPE/PME. https://www.kanjian.fr. Nous le remercions vivement de son accord de diffusion.**

## 7 CONSEILS RGPD POUR VOTRE SITE INTERNET

# 7 POINTS D'ECLAIRCISSEMENT SUR LE RGPD APPLIQUE AUX SITES INTERNET

Vous vous demandez sûrement ce que va changer le Règlement Général de Protection de Données (RGPD) **pour vous dans la gestion d'un site Internet ou d'un blog**. Je vous propose donc de voir certains **points précis comme les statistiques**, les marqueurs marketing, la conservation des données etc. Tous ces points sont des questions posées directement à la CNIL lors **d'un échange téléphonique de 50 minutes**. Petit rappel le RGPD ne concerne que la collecte de données personnelles de personne physique.

## 0 - LA QUESTION A VOUS POSER POUR TOUT TRAITEMENT

Pour toutes les données que vous souhaitez collecter et/ou que vous conservez la question principale à vous poser c'est : "Est-ce pertinent de conserver cette information et pourquoi la collectez-vous ?", si la réponse et non supprimez là ou ne la collectez pas. On reviendra plus loin dans l'article sur cette question à se poser et vous verrez que ça aide à clarifier certain point très particuliers.

## 1 - CONSENTEMENT A DEMANDER

**Comme c'est** déjà le cas pour les cookies**, vous devez demander le** consentement de manière explicite **à l'internaute pour la collecte/traitement de données personnelles telles que l'adresse IP, prénom, nom, etc. C'est valable pour tous les services : Google Analytics/Adsense/Adwords, Facebook, Twitter, AddThis, etc.**

**Vous avez le droit de demander le consentement** soit de manière globale**, pour tous les services avec une page explicative de tous les services,** soit de le faire un service à la fois**. Vous pouvez aussi grouper cookies et collecte de données, mais attention vous risquez de nuire à la lisibilité de l'information et une information floue est souvent cause de rejet par l'internaute. Attention toutefois à demander un consentement en bloc vous** risquez de voir un refus de l'internaute **juste pour un traqueur de moindre importance pour votre site, par exemple, le pixel Facebook, mais il est vrai que c'est tout de même plus simple pour l'internaute de devoir valider une seule fois.**

Consentement explicite : **vous n'avez pas le droit de mettre des messages du genre : "Si, vous continuez à naviguer sur notre site, vous acceptez etc." où la plupart du temps si vous ne cliquez pas sur "OK" et que vous consultez une autre page du site les cookies se mettent en place automatiquement. Vous devez donc avoir un bouton** "Autoriser" **et** "Refuser"**, les termes devant être compréhensibles par un enfant, vous n'aurez pas le droit de faire** des tournures très compliquées pour embrouiller l'internaute et le faire cliquer sur OUI.

**Il y a toutefois** des exceptions aux demandes d'acceptation **de cookie, tout cookie servant au bon fonctionnement de l'application ne doit pas être** nécessairement stipulés dans les mentions légales **et ne fait pas l'objet de consentement préalable à l'internaute. Cela aussi ne change pas par rapport à la précédente réglementation déjà en vigueur.**

## 2 - LOGS DE SERVEUR : UN CAS PARTICULIER

**On est tous d'accord que dans** les logs serveur **d'**Apache, Nginx ou IIS **il y a des données personnelles telles que l'adresse IP de la personne et dans d'autres logs l'adresse e-mail de l'internaute (mail.info par exemple). Ma question à la CNIL a été de savoir si je devais** demander là aussi un consentement préalable à la collecte de ces données**, ce qui entre nous serait une tâche complexe à mettre en œuvre.**

**Du coup la réponse a été : "Pourquoi l'a collectez-vous et dans quel but ?" (Mon fameux paragraphe 0), pour ma part** ce n'est jamais dans des cas statistiques**, c'est généralement pour faire de la recherche incident notamment en cas d'attaques ou de tentatives d'attaques informatiques.** C'est important si vous utilisez un SIEM**.**

**La durée de** conservation maximale des logs **? 1 an après les données doivent être détruites (code des télécommunications), car on le voit souvent le délai de détection des APT est généralement de 3 à 6 mois, il paraît donc inutile de les conserver plus d'une année.**

Doit-on demander le consentement à l'internaute ? **Étant donné la finalité du traitement et la durée,** vous n'êtes pas obligé de demander le consentement**, mais comme vous y oblige déjà la loi informatique et libertés, vous devez en faire mention dans vos mentions légales. Ces données échappent à la CNIL sauf, si vous l'utilisez à des fin statistiques, il** faudra donc en demander le consentement**.**

## 3 - PREUVE DU CONSENTEMENT

**Le RGPD demande aussi que tout responsable de traitement puisse** apporter la preuve du consentement de la personne **qui aurait accepté un traitement, ce n'est pas nouveau c'est déjà le cas dans le droit commun. Sur ce point, je n'ai eu pour réponse uniquement : "La formalisation de la preuve de consentement pour être recevable n'a pas encore été transposée en droit Français", ce n'est en effet pas nécessaire de l'être, car c'est un règlement.**

**Grosso modo vous devez conserver la preuve du mieux que** vous pouvez**, car il y a peu de chances que nous ayons plus d'informations à ce sujet. Pour le moment, aucun texte de loi de figure à l'agenda du Parlement. Vous noterez aussi que la loi CNIL a déjà été modifiée pour se conformer au RGPD.**

**Il faudra notamment apporter un éclaircissement** sur la preuve de consentement par les parents pour un mineur**, car via un simple clic "Moi parent autorise..." ça me paraît léger.**

## 4 - DUREE DU CONSENTEMENT

**Une fois le consentement donné il n'y a** pas de limite de validité**, il est valable tant que l'utilisateur** ne change pas d'avis**. Cela concerne la collecte et le traitement des données, mais le consentement pour les cookies lui à toujours** une durée maximale de 13 mois**...**

**Attention toutefois, si vous ajoutez un nouveau service à votre site Internet, par exemple AddThis, vous** devrez demander le consentement pour ce service**. Si vous faites des consentements par bloc, le risque est de voir un utilisateur qui avait consenti à les refuser suite à cet ajout.**

**Cela va vous obliger à bien réfléchir la mise en place de nouveaux services pour vos internautes.**

## 5 - LES FORMULAIRES

**C'est aussi un cas un peu particulier, car** l'internaute les remplis de son plein gré et de ça propre volonté**. Cependant, vous devez tout de même pour chaque formulaire indiqué la durée de conservation des données et leurs finalités.** N'oubliez pas de mentionner si vous conservez l'adresse IP**, car on ne lui** demande pas de manière explicite **à la saisie dudit formulaire.**

**Pour un formulaire de demande de contact, comme me l'a dit la CNIL, si vous avez répondu à la demande, vous pouvez le supprimer directement** la conservation n'étant plus pertinente **le plus souvent. Bien entendu si vous souhaitez le conserver en tant que prospects dans vos bases vous en avez le droit tout en respectant la loi CNIL et le RGPD. C'est d'ailleurs** souvent le cas sur les sites WordPress **avec Flamingo et Contact Form 7 qui sauvegarde automatiquement les messages.** Il faut juste indiquer dans vos mentions légales combien de temps seront conservées les données**, honnêtement 6 mois seront largement suffisants, avec toujours un maximum d'une année.**

**Si l'échange doit avoir une valeur de preuve pas besoin de traitement particulier par contre comme me l'a fait remarquer Pierre Desmarais c'est surtout une question de : "degré de force probante".**

**Ne gardez pas les formulaires plus d'un an,** le consentement lui est sans limite de validité**. Au final, reprenez la question au point 0 et vous saurez si ces informations issues d'un formulaire doivent être conservées.**

**Vous n'êtes pas obligé d'afficher les informations au niveau du formulaire, mais un lien vers les mentions légales sur la section traitant du formulaire et** une preuve de transparence **en facilitant l'accès aux explications. Vous n'êtes pas obligé de faire une section par formulaire, sauf si l'un ou l'autre donne lieu à** une autre finalité du traitement et/ou de sa durée**.**

**Typiquement pour les newsletters la durée de conservation sera jusqu'à la** demande de suppression de l'internaute **ou si vous jugez qu'il n'est plus pertinent de lui envoyer des e-mailings, car il ne les ouvre jamais.**

## 6 - MISE EN PLACE TECHNIQUE

**Le plus gros chantier,** vous devez l'avoir déjà fait en théorie**, en effet la plus grosse difficulté pour la mise en place sur votre site Internet du** consentement de l'internaute est à 90% près celui qui doit être en place pour l'acceptation des cookies.

**Sur un site réalisé avec WordPress, je vous le concède, ça devient vite compliqué, il vous faudra faire** le deuil de la majorité de vos plugins favoris **tant qu'ils n'ont pas eu de mise à jour pour être conforme. Et d'ailleurs** ne rêvez pas car il devrait déjà l'être pour les cookies**, notamment AddThis, Yoast pour ne parler que de ces deux-là.**

**Il faut aussi voir que la simple utilisation de** fonctionnalités natives de WordPress deviennent compliquées**, notamment l'insertion d'une Twitter Card, il devient dorénavant impossible d'utiliser l'ajout natif de WordPress, vous devrez utiliser une autre solution... Ce sera de même pour l'insertion de vidéo Youtube, de player calameo et de carte Google Maps... En effet, ces insertions natives insèrent directement le code des services en question et il y aura collecte des données et de cookie sans consentement préalable.**

**Pour vous simplifier la vie vous pouvez notamment utiliser des gestionnaires de tag tel que Tarteaucitron (open-source) qui vous** permettra de gérer plus de 50 services**. C'est d'ailleurs ce dernier** qu'utilise la CNIL **pour gérer consentement et cookie sur son site Internet.**

## 7 - LES SITES DE VOS CLIENTS ?

**Vous êtes une agence de communication et vous avez réalisé de très nombreux sites et vous commencez à vous dire : "La charge de travail pour mettre nos clients en**

**conformité va être énorme". Vous avez raison, mais** vous avez l'obligation de l'en informer**, car c'est lui qui est gestionnaire de son site donc responsable du traitement des données.**

**Pour rappel** seul le gestionnaire du site Internet est responsable **de sa déclaration à la CNIL ou non. Avec le RGPD** vous serez aussi responsable en tant que sous-traitant**, bonne nouvelle** les déclarations à la CNIL elles disparaissent **en mai 2018 avec l'application du RGPD.**

## REMERCIEMENTS :

**Je tiens à remercier la CNIL pour le temps accordé, sachez d'ailleurs qu'ils sont à votre disposition pour toutes questions liées à leurs domaines et c'est vraiment appréciable.**

**Un très grand merci à Pierre Desmarais (@DesmaraisPierre) pour sa relecture et ses commentaires sur l'article, sans lui je l'avoue, il n'aurait pas été aussi précis et aurait laissé passer une ânerie ou deux.**

**Cet article n'engage bien sûr pas ces personnes, mais je tenais à les remercier.**

Article rédigé par Alexandre JOLY et issu de son excellent blog sur la sécurité informatique et la sensibilisation des TPE/PME. https://www.kanjian.fr. Nous le remercions vivement de son accord de diffusion.

Yann BELZ