CONFORMITÉ DES SITES WEB : OÙ EN EST-ON ?

Le 2 mars dernier, la CNIL a fait connaître les trois points qui feront l'objet d'un contrôle prioritaire durant cette année 2021. Elle sera particulièrement attentive à propos de vos sites web puisque deux de ces points concernent leur sécurisation ainsi que l'utilisation des cookies.

Focus sur le protocole HTTPS

La CNIL a la cybersécurité des sites web français dans sa ligne de mire dont l'insuffisance est souvent constatée par l'Autorité lors de ses contrôles. Son attention se portera particulièrement sur la présence de certificats SSL/TLS chiffrant d'une part, les échanges entre l'utilisateur (son navigateur) et le site web visité, et d'autre part d'authentifier le propriétaire du site.

En pratique : ce certificat fait apparaître un cadenas à gauche de l'adresse URL et celle-ci débute par « https » au lieu de « http », le « s » faisant référence au terme « secure », pour un site sécurisé.

Pour vérifier la conformité des certificats, il est possible de se rendre sur https://www.digicert.com/help/, ou même https://www.robtex.com/ qui donne des informations plus techniques.

En l'absence de ce protocole, toutes les informations transitent en clair entre le client et le serveur et peuvent être altérées ou interceptées. Cela signifie que n'importe qui peut espionner et récupérer les éléments échangés au cours de la navigation sur le site, tels que l'identifiant et le mot de passe saisis pour se connecter au site en question. Cette sécurité empêche donc les attaques du type Man in the middle (homme au milieu), tiers qui se place entre vous et le visiteur de votre site.

L'utilisation du protocole HTTPS est désormais la norme comme le démontre le tableau de bord publié par Google ; au 1er septembre 2020, 94% des pages chargées en France l'étaient via HTTPS. L'absence de ce cadenas ou du https, parfois signalée par un message provenant du navigateur qui indique que la connexion n'est pas sécurisée, invite les visiteurs à se méfier voire éviter toute navigation sur le site en question. Cela constitue un manque à gagner potentiellement important dû à la place qu'a pris Internet dans notre société. **A noter que l'absence du protocole HTTPS influe également en votre défaveur sur le référencement naturel de votre site internet.**

Ce manquement peut constituer un véritable défaut de sécurisation fautif pour certaines catégories de sites, tel que :

- Des sites qui proposent la vente en ligne,
- Les sites de services bancaires,
- Les sites qui prévoient une authentification,
- Ou tout autre site susceptible de collecter des informations via des formulaires.

Les enjeux : en rappel de la *Note d'information de mars 2021 de DPO Consulting*, l'article 32 du RGPD impose au responsable de traitement ainsi qu'au sous-traitant de « *mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».

L'organisme ayant un site en ligne, en tant que responsable de traitement, a donc l'obligation de préserver la sécurité des données personnelles de ses visiteurs. La mise en place du protocole HTTPS est bien visée en tant que mesure technique de sécurité à appliquer au regard du risque pour les données personnelles qui transitent.

Les cookies : nouvelle recette depuis le 31 mars 2021 !

Le cookie peut être un outil marketing important. C'est donc un handicap majeur dans la collecte, le traitement et le partage de données personnelles, d'autant plus qu'il est, la plupart du temps, totalement incompris des utilisateurs dont sont partagées les données.

Définition : Un cookie est un petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web (c'est à dire d'un site web). Ce fichier est automatiquement renvoyé lors de contacts ultérieurs avec le même domaine.

Une distinction existe encore entre les cookies internes et les cookies tiers :

- **Cookies internes :** sont définis par le domaine du site que l'utilisateur visite. L'objectif est d'offrir une expérience utilisateur optimale. Cela signifie que le site se souvient des informations de connexion, des paniers… etc. Seul le domaine hôte peut récupérer et lire le contenu du cookie une fois qu'il a été défini.
- **Cookies tiers :** sont au contraire définis par un domaine qui n'est pas celui que l'utilisateur visite à ce moment-là. Ces cookies sont généralement utilisés à des fins de ciblage publicitaire et ne sont pas contrôlés par le domaine visité. A terme ceux-ci seront d'ailleurs bannis des navigateurs web.

Certains disparaissent après la navigation, d'autres encore, sans être des cookies tiers, persistent. **Cela constitue un risque pour les utilisateurs qui se connectent à des outils publics du type cybercafé, ordinateurs d'école et qui ne naviguent pas en session privé.**

La mauvaise gestion des cookies, et notamment des cookies tiers, a poussé les autorités européennes à légiférer. La CNIL a ainsi donné une date butoir à tous les sites concernés de se mettre en conformité au RGPD au 31 mars 2021.

Suis-je concerné ?

Cette obligation de conformité s'impose aux propriétaires de sites internet (secteur public ou privé) qui déposent des traceurs soumis au consentement. La CNIL précise que : *« Tous les cookies n'ayant pas pour finalité exclusive de permettre ou faciliter une communication par voie électronique ou n'étant pas strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur nécessitent le consentement préalable de l'internaute »*. Ces lignes directrices portent notamment sur l'information de l'utilisateur et le recueil de leur consentement.

S'agissant des cookies nécessitant un acte volontaire de l'utilisateur, on peut citer :

- Les cookies liés aux opérations relatives à la publicité ciblée,
- Les cookies des réseaux sociaux

Si vous utilisez ce type de cookies, ce qu'il vous appartient de vérifier auprès du concepteur de votre site, vous êtes concernés par les lignes directrices de la CNIL et l'obligation de mise en conformité de votre site.

Ces cookies s'opposent aux cookies utiles à la fourniture du services, tels que :

- Les cookies de paniers d'achat sur un site marchand,
- Les cookies d'identification de session,
- Les cookies d'authentification de services,
- Certains cookies d'analyse de mesures d'audience si les données sont anonymisées notamment, type Matomo
- …

Les grandes lignes directrices de la CNIL sur la mise en conformité des cookies :

- **Le consentement, la base :** il n'est plus possible de considérer qu'un utilisateur qui navigue sur votre site ait consenti implicitement au dépôt de cookies. Il faut un acte positif, qui laisse entendre un consentement libre, spécifique, univoque et éclairé.
  Ainsi, la poursuite de la navigation ne vaudra plus consentement.

- **L'information, visible et explicite :** pour que l'utilisateur donne son consentement il doit avoir eu une information avant le dépôt des cookies sur le navigateur. Cette information porte sur le cookie, sa finalité, sa durée d'enregistrement, l'identité du responsable de traitement… Elle doit être claire et tout de suite accessible, au moment de la demande de consentement. Cette information peut être parachevée dans une politique de cookies complémentaire.

- **Un choix, qui peut être modifié :** la CNIL précise encore que l'utilisateur informé des cookies et de la finalité de ces derniers, doit pouvoir accepter ou refuser chaque cookie ou chaque finalité individuellement ou tout accepter / tout refuser. Par principe, un cookie est temporaire, le consentement de l'utilisateur n'est donné que pour une durée maximale de 13 mois. Quoiqu'il arrive, il doit être aussi facile d'accepter que de refuser le cookie et l'utilisateur peut changer d'avis et modifier son choix à tout moment. Ceci implique d'expliquer la méthode pour retirer son consentement.

En pratique :

Attention à la preuve du consentement ! Le responsable de traitement doit pouvoir être en mesure de répondre à cette preuve par la production d'une preuve individuelle par utilisateur et horodatée. Certains outils permettent cette conservation. Une veille régulière de l'outil de consentement est nécessaire.

L'information au cœur de la mise en conformité RGPD.

Il est important de rappeler les obligations juridiques de mise en conformité des sites web :

1. **Des mentions légales détaillées :** la loi pour la confiance numérique de 2004 énonce les informations au titre des « mentions légales » qui constituent une obligation majeure pour l'information des utilisateurs d'un site internet. Elles sont obligatoires :
    - Identification des personnes physiques ou morales avec tous les éléments « d'identité » et de coordonnées (si activité commerciale, tout élément type n° TVA, RCS, activité…),
    - Le nom du responsable de publication,
    - L'identification de l'hébergeur…

Les conditions générales de vente (CGV) sont de même nature que les mentions légales. Elles sont obligatoires et doivent être accessibles sur chaque page du site marchand.

2. **Concevoir une politique de confidentialité :** il s'agit de la base de l'information de l'utilisateur d'un site quant au traitement de ses données personnelles. A partir du moment où il y a recueil, collecte, traçage de données personnelle, cette politique de confidentialité est obligatoire.

Elle doit être rédigée en termes précis et clairs. Elle comporte notamment (liste non exhaustive) :

- L'identité du responsable de traitement et du DPO éventuel,
- La base juridique,
- Le type de données collectées,
- Les destinataires,
- Le transfert éventuel,
- La durée de conservation,
- L'exercice des droits…

L'information présente ne dispense pas le responsable de traitement d'ajouter des mentions d'informations sous chaque collecte de traitement (formulaire de contact, inscription newsletter…)

3. **La politique de cookies est indispensable** tant l'information du bandeau est certes explicite, mais trop concise pour être suffisante. Ce document, souvent intégré à la politique de confidentialité, permet au responsable de traitement d'insister sur les finalités, d'expliquer les différentes procédures de retrait du consentement mais également d'informer l'utilisateur de tous autres cookies ou traceurs déposés sur le navigateur et nécessaires à l'utilisation du service, quand bien même ceux-ci ne nécessitent pas de consentement.

En effet, l'absence de consentement n'entraîne pas absence d'information.

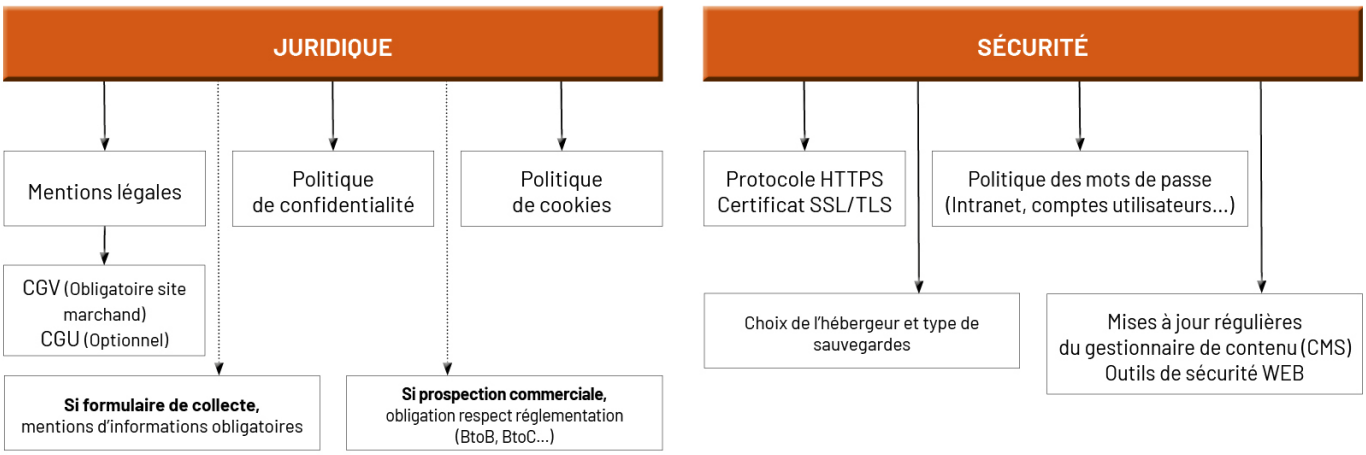
Tous ces éléments doivent être accessibles sur chaque page du site.

Le responsable de traitement du site internet se rappellera enfin que, si son site internet doit être conforme, sa politique de prospection commerciale doit l'être également. **Quelques brefs rappels :**

- En matière de prospection commerciale entre professionnels, la CNIL rappelle que l'existence **d'un lien direct avec l'activité professionnelle du prospect** est nécessaire pour justifier d'un intérêt légitime et dispenser l'entreprise d'un consentement du professionnel ;
- La prospection commerciale à l'attention d'un particulier sans consentement est illicite ;
- Il doit toujours être donné la possibilité au prospect (professionnel ou particulier) de revenir sur son consentement ou simplement de se désabonner de toute campagne publicitaire et même de toute communication à caractère informatif (type newsletter).
- Le responsable de traitement doit toujours être en mesure d'apporter la preuve du consentement (lorsqu'il est requis) et notamment lorsqu'il a acheté des bases de données

En résumé

VOTRE SITE WEB RGPD



Les consultants en données personnelles de DPO Consulting Bourgogne-Franche-Comté sont à votre disposition pour la mise en conformité de vos sites internet et plus généralement sur toutes vos questions RGPD. N'hésitez pas à prendre contact.

Stéphanie BROGGINI
Consultante DPO Bourgogne-Franche-Comté
stephanie.broggini@dpo-consulting.com

Florine GIACOMUZZI
Stagiaire étudiante Master II «Droit du numérique»
Université de Franche-Comté