Bonnes pratiques en matière de sites Internet

Le site internet est désormais un outil incontournable de la vie économique. Les entreprises, les commerçants, les entrepreneurs individuels, les personnes exerçant une activité libérale et même les personnes privées mettent en place leur site internet afin de se faire connaître, informer, présenter leurs services et produits ou encore proposer de la vente à distance.

Le site internet joue également un rôle important pour attirer des clients et entretenir une relation avec eux.

Aussi, que le site internet soit un simple « *site vitrine* » ou bien un « *site marchand* », il implique dans l'immense majorité des cas une collecte de données personnelles par le biais d'une rubrique contact, d'un formulaire en ligne, de la création d'un compte client ou encore de la mise en place de cookies de navigation.

Site vitrine	Site marchand
Un « ***site vitrine*** » sert à présenter une entreprise, une administration, une association (…), son activité, ses services et/ou ses produits. Il peut également proposer d'autres fonctionnalités comme par exemple : • un formulaire de contact ; • un abonnement à une lettre d'informations (Newsletter).	Un « ***site marchand*** » ou « ***site de vente en ligne*** » sert principalement à proposer des services et/ou des produits à la vente. Une autre alternative peut également être un « ***site marketplace*** » dont la fonction principale est l'intermédiation de vente à distance par la vente de produits de commerçants ainsi que leur présentation. L'internaute peut ainsi effectuer ses achats chez divers commerçants sur un même site internet avec un seul compte client.

La vocation de cette fiche pratique est donc d'aider les responsables du traitement à adopter les bonnes pratiques pour assurer la **confidentialité** et la **sécurité** des données collectées par le biais des sites Internet.

Une maîtrise des données personnelles collectées

Tous les sites internet ne collectent pas le même nombre de données ni les mêmes catégories. Cela dépend des finalités des sites créés.

Une fois ces fonctionnalités identifiées, il appartiendra au responsable du traitement de déterminer quelles données sont réellement nécessaires pour chacune de ces fonctionnalités et d'appliquer des durées de conservation adaptées à chacune des catégories de données ainsi collectées.

➢ **Sur les finalités des sites internet**

Les données personnelles peuvent être collectées pour **plusieurs finalités**, à condition que ces finalités soient :

- **déterminées** ;
- **explicites** ;
- **légitimes**.

Exemple :

- présentation de l'entreprise et de ses services
- mise à disposition des visiteurs d'une rubrique contact
- inscription à une newsletter
- création d'un compte client
- paiement en ligne

Si un site comporte des espaces de discussion, les sujets qui y seront abordés devront être maîtrisés afin d'éviter toute mise en cause de la responsabilité fondée sur des propos tenus par des utilisateurs (pédophilie, incitation à la violence, à la haine raciale, etc.). Cela passera par la désignation d'un modérateur.

➢ **Sur les données collectées**

Conformément aux dispositions de l'article 4 de la Loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles, les données à caractère personnel collectées doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

Le responsable du traitement doit donc faire attention à ne collecter que les seules informations dont il a besoin pour chacune des fonctionnalités de son site internet. Si celui-ci est déjà en place, il convient de passer en revue les données collectées et de supprimer celles qui ne sont pas ou plus nécessaires.

Cela peut se traduire par exemple par un ajustement des formulaires permettant de collecter les données personnelles des internautes.

➢ **Sur la durée de conservation des données collectées**

Conformément à l'article 4 de la Loi n° 1.565 du 3 décembre 2024, les données à caractère personnel objets du traitement ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant **une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées**.

Exemple : les informations des salariés d'une entreprise sur un site Internet doivent être supprimées dès que ceux-ci ne sont plus en poste

Ainsi, il est important de respecter les règles suivantes :

- supprimer les données et le contact d'un internaute qui ne donne pas de réponse aux sollicitations du responsable du traitement durant un délai de **3 ans maximum** ;

- conserver les données relatives à la navigation d'un internaute pendant **13 mois maximum**, à compter de la date de dépôt du cookie ;

- supprimer les données non-nécessaires à la réalisation d'un objectif interne, une fois celui-ci atteint ;

- supprimer systématiquement les données des personnes ayant demandé à ne plus être sollicitées par le responsable du traitement, ou les archiver selon les cas à des fins de paiement ou de prescription si des transactions ont eu lieu.

Cas particulier de la conservation des données bancaires
Les données bancaires peuvent être conservées pour une finalité de preuve en cas d'éventuelle contestation de la transaction, en archives intermédiaires, treize mois suivant la date de débit. Ce délai peut être étendu à quinze mois afin de prendre en compte la possibilité d'utilisation de cartes de paiement à débit différé. Ces données peuvent être conservées plus longtemps sous réserve d'obtenir **le consentement exprès** du client, préalablement informé de l'objectif poursuivi (faciliter le paiement des clients réguliers, par exemple). Ce consentement peut être recueilli par l'intermédiaire d'une case à cocher, et **non pré cochée par défaut,** et ne peut résulter de l'acceptation de conditions générales. Les données relatives au cryptogramme visuel ne doivent pas être stockées. Lorsque la date d'expiration de la carte bancaire est atteinte, les données relatives à celle-ci doivent être supprimées.

Cas particulier de la conservation des copies des documents d'identité
Les copies des documents d'identité pourront être conservées au maximum 6 mois lorsqu'elles servent de justificatifs relatifs à la vérification de l'identité d'un titulaire de carte bancaire, et doivent être détruites dès que la vérification de l'identité de la personne concernée est effectuée s'agissant des demandes de remboursement ou de paiement à distance.

Un devoir d'information sur la collecte de données personnelles

Les personnes concernées doivent être informées, dans les conditions générales et/ou dans une rubrique dédiée à la politique de confidentialité des données personnelles sur le site, de leurs droits en application de l'article 10 de la Loi n° 1.565 du 3 décembre 2024.

- **Sur les personnes concernées**

La personne concernée par un traitement de données personnelles est **la personne physique** à laquelle **se rapportent les données** qui font l'objet du traitement.

En matière de sites Internet, les personnes suivantes peuvent ainsi être concernées :

« *Tous les visiteurs du site* » : notamment en cas de présence de cookies, de sites de vente en ligne ;
« les salariés » : lorsque leurs données personnelles sont affichées sur le site ou font l'objet d'une traçabilité (par exemple : nom, prénom, fonction, contact, photo, login, logs de connexion) ;
« les clients » : notamment en cas de création de comptes.

- **Sur les mentions d'information à fournir**

En vertu de l'article 10 de la Loi n° 1.565 du 3 décembre 2024, le responsable du traitement doit prendre les **mesures appropriées** pour fournir à la personne concernée toute information sur l'utilisation de ses données et lui faciliter l'exercice de ses droits.

Parmi ces informations, figurent :

- **l'identité et les coordonnées professionnelles du responsable du traitement**, et le cas échéant de son **représentant** établi à Monaco, ou à défaut, au sein d'un Etat membre de l'Union européenne ;
- **l**es **finalités** du traitement et son **fondement juridique** ;
- les **catégories de données** personnelles concernées ;
- **la durée de conservation** des données ou, lorsque cela n'est pas possible, **les critères utilisés** pour déterminer cette durée ;
- **l**orsque le traitement est fondé sur le **consentement** de la personne, le droit de celle-ci de retirer ce consentement **à tout moment** ;
- les **destinataires** ou **catégories** de destinataires ;
- les moyens d'exercer ses **droits d'accès, d'opposition, de rectification, d'effacement, de limitation** ou **de portabilité** ;
- le **droit de s'opposer à l'utilisation pour le compte de tiers**, ou à **la communication** à des tiers de données personnelles la concernant **à des fins de prospection,** notamment commerciale.

Pour les sites internet, cette information doit se faire par le biais des **Conditions Générales** et/ou d'une **page consacrée à la politique de confidentialité des données personnelles** accessible(s) facilement sur le site internet.

Il existe toutefois plusieurs situations pour lesquelles l'information ne suffit pas. Il faut ainsi expressément demander l'accord de l'internaute dans le cadre de la prospection commerciale par courrier électronique et dans certains cas, lors de l'utilisation de cookies.

ⓘ **Information**
Les cookies sont de petits fichiers qui sont insérés sur l'ordinateur d'un internaute par le site web au moment de sa consultation. Ces fichiers enregistrent ensuite des informations concernant l'internaute, il peut s'agir d'informations nominatives le concernant. Les informations ainsi collectées peuvent ensuite être analysées afin de faciliter la navigation sur le site, proposer des publicités ciblées et analyser les habitudes de navigation. Néanmoins, les cookies n'ont pas accès au contenu de l'ordinateur de l'internaute. Il existe plusieurs types de cookies : - les cookies techniques/fonctionnels (dont cookies de mesure d'audience) ; - les cookies d'applications tierces ; - les cookies de partenaires publicitaires ; - les cookies optionnels.

Lorsque le consentement est nécessaire, il convient de prévoir une possibilité simple et rapide de retrait de celui-ci.

- **Cas des transferts de données vers un pays ne disposant pas d'un niveau de protection adéquat**

Un tel transfert des données collectées par les sites internet, notamment vers les Etats-Unis d'Amérique, peut survenir par exemple lorsque lesdits sites utilisent des prestataires pour les services suivants :

- Statistiques, cookies, Google Analytics ;
- Newsletter ;
- Hébergement ;
- ReCaptcha ;
- Paiement en ligne.

NB : La liste des pays disposant d'un niveau de protection adéquat est disponible sur le site Internet de l'APDP.

L'internaute devra alors être averti de ce transfert, le plus souvent y consentir, et des mesures devront impérativement être prises pour assurer la confidentialité et la sécurité des données transférées.

Exemples :

Google Analytics
Lorsqu'un site internet utilise **Google Analytics**, les données suivantes sont envoyées à Google Inc., aux Etats-Unis : adresse IP, nom de domaine internet de l'internaute, pages visitées et leur nombre, nombre d'affichage par page, durée passée sur chaque page, nombre de clics, nom et version du navigateur web de l'internaute, système d'exploitation de l'internaute, horodatage d'accès au site et des pages visitées sur le site. L'APDP a les exigences suivantes : - qu'un bandeau « *Cookies* » soit impérativement mis en place afin de permettre à l'internaute d'accepter ou de refuser le dépôt des cookies sur son terminal ; - ce bandeau d'information doit impérativement apparaître à l'ouverture du site avant le dépôt de tout cookie et sans que l'internaute n'ait à effectuer une quelconque démarche ; - ce bandeau doit informer les internautes du transfert de leurs données vers les Etats-Unis, pays ne disposant pas d'un niveau de protection adéquat ; - en cas de refus de dépôt de cookies, l'internaute doit être informé que sa demande a effectivement été prise en compte. Il doit également pouvoir poursuivre sa navigation ; - l'internaute, dans la rubrique dédiée à la politique cookie, doit pouvoir changer ses paramètres et revenir ainsi à tout moment sur son consentement. Il existe toutefois des alternatives européennes (Union européenne) à Google Analytics. Leur utilisation ne nécessite pas la mise en place d'un **bandeau** relatif aux cookies sur le site internet car il n'y a pas de transfert de données vers un pays ne disposant pas d'un niveau de protection adéquat. Par ailleurs, si les deux derniers octets de l'adresse IP sont anonymisés, il n'y a pas lieu non plus d'obtenir le consentement de l'internaute pour la collecte de données statistiques.

Mailchimp
Mailchimp est une plateforme de marketing automation et un service de marketing par courriel. Elle propose à ses clients de créer des campagnes de communication par courriel. L'utilisateur a la possibilité de personnaliser ses campagnes en fonction de critères de segmentation de sa base de contacts. La plate-forme propose également l'envoi de courriels automatiques en fonction d'événements ou de caractéristiques associées à un contact. Ladite plateforme est située aux Etats-Unis et implique donc un transfert de données vers un pays ne disposant pas d'un niveau de protection adéquat dès lors qu'un site internet l'utilise. L'APDP demande en conséquence que toute personne souhaitant s'abonner à une lettre d'information gérée par cette plateforme soit avertie par un message que ses données seront hébergées par le prestataire Mailchimp basé aux Etats-Unis.

Elle demande également que cette personne puisse se désinscrire à tout moment de la lettre d'information et revenir ainsi sur son consentement.

ReCaptcha Google

La fonctionnalité « *ReCaptcha* » distingue les humains des robots. Elle correspond à une case « *je ne suis pas un robot* » à cocher, très souvent complétée par un test de reconnaissance d'images.

L'APDP interdit l'utilisation de ce ReCaptcha Google qui entraîne un transfert des informations nominatives vers les Etats-Unis si le consentement des utilisateurs n'est pas au préalable recueilli.

Pour distinguer un humain d'un robot, des solutions proposées par des pays disposant d'un niveau de protection adéquat et similaires à ce ReCaptcha, sont toutefois disponibles sur le marché.

Une fonctionnalité de ReCaptcha peut également être développée en interne par les départements techniques des responsables du traitement.

Une obligation de sécurité des données

L'article 31 de la Loi n° 1.565 du 3 décembre 2024 précise les obligations de sécurité mises à la charge du responsable du traitement.

Celui-ci doit ainsi prendre des **mesures techniques et organisationnelles appropriées** afin de garantir un **niveau de sécurité adapté aux risques** pour les droits et libertés des personnes concernées.

L'adoption de ces mesures nécessite une **analyse** permettant d'identifier les risques puis de déterminer leur **niveau de probabilité** et de **gravité**.

Conformément à la Loi, les risques encourus sont notamment :

- la destruction de données ;
- la perte de données ;
- l'altération de données ;
- la divulgation non autorisée de données ;
- l'accès non autorisé à des données personnelles.

Ces risques peuvent se produire de manière **accidentelle** ou **illicite.**

C'est ainsi qu'en matière de sites internet, le responsable du traitement doit prendre des mesures assurant non seulement la **confidentialité des données** mais également **leur sécurité**.

➢ **Des mesures pour assurer la confidentialité des données**

- l'accès aux données est réservé uniquement aux seules personnes ayant à en connaître. En fonction de leur activité, ces personnes ne pourront avoir accès qu'à certaines catégories de données (le service comptable par exemple pourra n'avoir accès qu'à l'identité et à l'adresse d'un internaute ainsi qu'aux informations liées à l'achat qu'il doit facturer sans nécessairement avoir accès aux autres informations potentiellement collectées sur le client).

- **l'accès aux outils et interfaces d'administration doit être réservé aux seules personnes habilitées. Il convient en particulier de** limiter l'utilisation des comptes administrateurs aux équipes en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent.

- les habilitations et les mots de passe doivent régulièrement être mis à jour afin de garantir que seules les personnes habilitées peuvent accéder aux données nécessaires à la réalisation de leurs missions.

- un mécanisme de **journalisation des opérations et des accès** effectués sur le traitement doit être mis en place.

- les interventions de maintenance doivent faire l'objet d'une **traçabilité** et le matériel remisé ne devra plus contenir de données personnelles Il convient d'être particulièrement vigilant lors de changements d'équipements, notamment de disques durs, qui sont une source de fuite de données si ces supports ne sont pas correctement effacés lors de leur mise au rebut.

Cas particulier de la protection des copies des documents d'identité
S'agissant des **documents d'identité**, l'APDP est particulièrement vigilante quant aux modalités de leur collecte. L'objectif est de lutter contre le vol et l'usurpation d'identité, l'utilisation illicite des données personnelles contenues dans ces documents et les conséquences que cela peut induire pour les victimes. En ce qui concerne les sites marchands, la collecte n'est permise qu'aux fins de s'assurer de l'identité d'un titulaire de carte bancaire ou pour gérer les demandes de paiement ou de remboursement suite à la participation à un jeu. L'APDP demande que les modalités de collecte à distance soient protégées et notamment

que les copies de documents d'identité soient déposées sur une page sécurisée. Elle recommande également que les personnes dont les copies de documents d'identité sont collectées soient invitées à transmettre celles-ci en noir et blanc et barrées, afin d'en rendre difficiles d'éventuelles reproductions.

Cas particulier de la protection des données liées à la carte bancaire

Les données nécessaires à la réalisation d'une transaction à distance par carte de paiement sont le nom du titulaire, le numéro de la carte, la date d'expiration et le cryptogramme visuel.

L'utilisation de moyens de paiements en ligne et la conservation de numéros de cartes bancaires doivent faire l'objet de mesures de traçabilité permettant de détecter *a posteriori* tout accès illégitime aux données et de l'imputer à la personne ayant accédé illégitimement à ces données. En effet, les données de cartes bancaires étant particulièrement sensibles, il convient de savoir quelles personnes au sein du personnel du site marchand ont pu y avoir accès.

Le responsable du traitement doit prendre les mesures organisationnelles et techniques appropriées afin de préserver la sécurité, l'intégrité et la confidentialité des numéros de cartes bancaires contre tout accès, utilisation, détournement, communication ou modification non autorisés en recourant à des systèmes de paiement sécurisés conformes à l'état de l'art et à la réglementation applicable. Ces données doivent être notamment chiffrées par l'intermédiaire d'un algorithme réputé fort.

Lorsque le responsable du traitement conserve les numéros de carte bancaire pour une finalité de preuve en cas d'éventuelle contestation de la transaction, ces numéros doivent faire l'objet de mesures techniques visant à prévenir toute réutilisation illégitime, ou toute ré identification des personnes concernées. Ces mesures peuvent notamment consister à stocker les numéros de carte bancaire sous forme hachée avec utilisation d'une clé secrète.

En outre, compte tenu de la sensibilité de cette donnée, le numéro de la carte de paiement ne peut être utilisé comme identifiant commercial.

Le responsable du traitement, ou son prestataire, ne doit pas demander la transmission de la photocopie ou de la copie numérique du recto et/ou du verso de la carte de paiement même si le cryptogramme visuel et une partie des numéros sont masqués.

Lorsque la collecte du numéro de la carte de paiement est effectuée par téléphone, il est nécessaire de mettre en place des mesures de sécurité telle que la traçabilité des accès aux numéros des cartes. Une solution alternative sécurisée, sans coût supplémentaire, doit être proposée aux clients qui ne souhaitent pas transmettre les données relatives à leurs cartes par ce moyen.

- **Des mesures pour assurer la sécurité des données**

Des mesures de sécurité des locaux et des systèmes d'information doivent être mises en place afin d'empêcher que les fichiers soient déformés, endommagés ou que des tiers non autorisés y aient accès.

Le protocole TLS (en remplacement de SSL) doit être mis en œuvre sur tous les sites web, en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre.

L'utilisation de TLS doit être obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques.

Seuls les ports de communication strictement nécessaires au bon fonctionnement des applications installées doivent être conservés. Si l'accès à un serveur web passe uniquement par HTTPS, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port 443 et bloquer tous les autres ports.

Le nombre de composants mis en œuvre doit être limité et mis à jour.

Une veille technique doit être mise en place afin d'assurer que la sécurité est **toujours** à jour.