

BONNES PRATIQUES EN MATIERE 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 une 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.

La vocation de cette fiche pratique est donc d'aider les responsables de traitement à adopter les bonnes pratiques pour assurer la confidentialité et la sécurité de ces données.

Site vitrine	Site marchand
<p>Un « site vitrine » sert à présenter une entreprise, une administration, une association (...), son activité, ses services et/ou ses produits.</p> <p>Il peut également proposer d'autres fonctionnalités comme par exemple :</p> <ul style="list-style-type: none">• un formulaire de contact ;• un abonnement à une lettre d'informations (Newsletter).	<p>Un « site marchand » ou « site de vente en ligne » sert principalement à proposer des services et/ou des produits à la vente.</p> <p>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.</p>

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 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

- **Sur les personnes concernées**

En vertu de l'article 1^{er} de la Loi n° 1.165 qui dispose que « *La personne concernée par un traitement d'informations nominatives est celle à laquelle se rapportent les informations qui font l'objet du traitement* », les données suivantes des internautes sont le plus souvent collectées par les sites internet :

« **Tous les visiteurs du site** » : notamment en cas de présence de cookies, de sites de vente en ligne ;

« **les salariés** » : lorsque leurs informations nominatives 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 14 de la Loi 1.165, « *Les personnes auprès de qui des informations nominatives sont recueillies doivent être averties :*

- *de l'identité du responsable du traitement et le cas échéant de celle de son représentant à Monaco ;*
- *de la finalité du traitement ;*
- *du caractère obligatoire ou facultatif des réponses ;*
- *des conséquences à leur égard d'un défaut de réponse ;*
- *de l'identité des destinataires ou des catégories de destinataires ;*
- *de leurs droits d'opposition, d'accès et de rectification relativement aux informations les concernant ;*
- *de leur droit de s'opposer à l'utilisation pour le compte de tiers, ou à la communication à des tiers d'informations nominatives les 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 facilement sur le site internet.

Il existe toutefois plusieurs situations dans 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.

① 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 d'annulation 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 notamment 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 la CCIN.

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.

La Commission 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 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.

La Commission 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.

La Commission 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 de traitement.

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 fonctionnalités des sites créés.

Une fois ces fonctionnalités identifiées, il appartiendra au responsable de 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 fonctionnalités des sites internet

Le tableau ci-dessous présente les fonctionnalités les plus souvent rencontrées :

Site vitrine	Site marchand
<ul style="list-style-type: none">• Présenter l'entreprise, l'association (...);• Trombinoscope;• Transmettre les informations aux prospects et aux clients sur la société et/ou sur les produits, aux visiteurs sur l'association, ...;• Diffuser les actualités de l'entreprise, l'association (...);• Communiquer les coordonnées;• Mettre à disposition un formulaire de contact;• Inscription à une Newsletter;• Communiquer les liens vers les réseaux sociaux;• Protection ReCaptcha;• Communiquer les liens hypertextes ou les références à d'autres sites internet;• Produire des statistiques d'audience et analyser le trafic web	<ul style="list-style-type: none">• Présenter l'entreprise;• Trombinoscope;• Transmettre les informations aux prospects et aux clients sur la société et/ou sur les produits;• Diffuser les actualités de l'entreprise;• Communiquer les coordonnées de l'entreprise;• Mettre à disposition un formulaire de contact;• Inscription à une Newsletter;• Communiquer les liens vers les réseaux sociaux;• Protection ReCaptcha;• Communiquer les liens hypertextes ou les références à d'autres sites internet;• Produire des statistiques d'audience et analyser le trafic web (par exemple par le biais de Google Analytics -cookies);

Site vitrine	Site marchand
(par exemple par le biais de Google Analytics -cookies).	<ul style="list-style-type: none"> • Vente à distance (achat en ligne, traiter les commandes, réaliser les livraisons, historique des achats, etc.) ; • Création et/ou gestion d'un compte client ; • Mise à disposition d'un panier pour les achats en ligne ; • Paiement en ligne ; • Etablissement de factures ; • Permettre de transmettre à la société des réclamations et gestion du SAV ; • Suivi de la relation client (réalisation d'actions de fidélisation, de prospection, de sondage, de test produit et de promotion).

Attention : 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**

L'article 10.1 de la Loi 1.165 demande que les informations traitées soient : « **adéquates, pertinentes et non excessives** au regard de la finalité pour laquelle elles sont collectées et pour laquelle elles sont traitées ultérieurement (...). »

Le responsable de 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.

Ci-dessous les catégories de données les plus souvent collectées :

Site vitrine	Site de vente en ligne
Catégorie « <i>Identité</i> » : <ul style="list-style-type: none"> • <u>Salariés</u> : nom, prénom, photo ; 	Catégorie « <i>Identité</i> » : <ul style="list-style-type: none"> • <u>Salariés</u> : nom, prénom, photo ; • <u>Personnes tierces</u> : nom, prénom, photo des événements

Site vitrine	Site de vente en ligne
<ul style="list-style-type: none"> • <u>Personnes tierces</u> : nom, prénom, photo des événements (si oui, le consentement a-t-il été obtenu ?). <p>Catégorie « <i>Rubrique Contact</i> » :</p> <ul style="list-style-type: none"> • nom, prénom, adresse email, raison sociale, contenu du message. <p>Catégorie « <i>Données d'identification électronique</i> » :</p> <ul style="list-style-type: none"> • logs de connexion des administrateurs, des prestataires et éventuellement des clients. <p>Catégorie « <i>Cookies de Google Analytics</i> » :</p> <ul style="list-style-type: none"> • adresse IP, nom du domaine internet de l'internaute, pages visitées et leur nombre, nombre d'affichages 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. 	<p>(si oui, le consentement a-t-il été obtenu ?).</p> <p>Catégorie « <i>Rubrique Contact</i> » :</p> <ul style="list-style-type: none"> • nom, prénom, adresse email, raison sociale, contenu du message. <p>Catégorie « <i>Données d'identification électronique</i> » :</p> <ul style="list-style-type: none"> • logs de connexion des administrateurs, des prestataires et éventuellement des clients. <p>Catégorie « <i>Cookies de Google Analytics</i> » :</p> <ul style="list-style-type: none"> • adresse IP, nom du domaine internet de l'internaute, pages visitées et leur nombre, nombre d'affichages 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 ; <p>Catégorie « <i>Informations temporelles, horodatage</i> » :</p> <ul style="list-style-type: none"> • Horodatage des transactions, commandes, échanges de service clients et autres communications avec les clients, fournisseurs et sous-traitant. <p>Catégorie « <i>Vente en ligne/informations bancaires</i> » :</p> <ul style="list-style-type: none"> • nom, prénom, numéro de carte bancaire. <p>Catégorie « <i>Panier</i> » :</p> <ul style="list-style-type: none"> • nom, prénom, adresse, détails des achats.

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

L'article 10.1 de la Loi 1.165 précise que les informations traitées doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant « **une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées** ou pour laquelle elles sont traitées ultérieurement* ».

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 de traitement durant un délai de 3 ans maximum ;
- conserver les données relatives à la navigation d'un internaute pendant 13 mois seulement, 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 de traitement, ou les archiver selon les cas à des fins de paiement ou de prescription si des transactions ont eu lieu.

A titre d'exemple, le tableau ci-dessous récapitule les durées recommandées par la Commission pour les catégories de données les plus communément rencontrées :

Site vitrine	Site de vente en ligne
<p>Catégorie « <i>Identité</i> » :</p> <ul style="list-style-type: none"> • <u>Salariés</u> : tant que la personne est en poste ; • <u>Personnes tierces</u> : selon le consentement/tant que le site est en place /politique d'archivage/autres. <p>Catégorie « <i>Rubrique Contact</i> » :</p> <ul style="list-style-type: none"> • Le temps de traitement de la demande. <p>Catégorie « <i>Données d'identification électronique</i> » :</p> <ul style="list-style-type: none"> • 1 an maximum à compter de la collecte. <p>Catégorie « <i>Cookies de Google Analytics</i> » :</p> <ul style="list-style-type: none"> • 13 mois maximum conformément à la délibération n° 2019-083 du 15 mai 2019 portant recommandation sur les modalités de dépôt et la 	<p>Catégorie « <i>Identité</i> » :</p> <ul style="list-style-type: none"> • <u>Salariés</u> : tant que la personne est en poste ; • <u>Personnes tierces</u> : selon le consentement/tant que le site est en place /politique d'archivage/autres. <p>Catégorie « <i>Rubrique Contact</i> » :</p> <ul style="list-style-type: none"> • Le temps de traitement de la demande. <p>Catégorie « <i>Données d'identification électronique</i> » :</p> <ul style="list-style-type: none"> • 1 an maximum à compter de la collecte. <p>Catégorie « <i>Cookies de Google Analytics</i> » :</p> <ul style="list-style-type: none"> • 13 mois maximum conformément à la délibération n° 2019-083 du 15 mai 2019 portant recommandation sur les modalités de dépôt et la

Site vitrine	Site de vente en ligne
<p>durée de conservation des cookies et autres traceurs sur les terminaux d'utilisateurs de réseaux de communication électronique (NB : cette durée maximum vaut de manière générale pour tous les cookies).</p> <p>Catégorie « <i>Newsletter</i> » :</p> <ul style="list-style-type: none"> • Tant que la personne est inscrite. 	<p>durée de conservation des cookies et autres traceurs sur les terminaux d'utilisateurs de réseaux de communication électronique (NB : cette durée maximum vaut de manière générale pour tous les cookies).</p> <ul style="list-style-type: none"> • <p>Catégorie « <i>Newsletter</i> » :</p> <ul style="list-style-type: none"> • Tant que la personne est inscrite. <p>Catégorie « <i>Informations temporelles, horodatage</i> » :</p> <ul style="list-style-type: none"> • Jusqu'à effacement du compte client sur demande du client et expiration du droit de garantie sur les produits ou services achetés. <p>Catégorie « <i>Vente en ligne/informations bancaires</i> » :</p> <ul style="list-style-type: none"> • Attention en cas de collecte de cartes bancaires. Les données relatives aux cartes bancaires doivent en effet être supprimées une fois la transaction réalisée. Les factures peuvent en revanche être conservées 10 ans. <p>Catégorie « <i>Panier</i> » :</p> <ul style="list-style-type: none"> • Si la personne ne passe pas commande, les données ne doivent pas être conservées au-delà de 10 jours.

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 précochée 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.

Une obligation de sécurité des données

L'article 17 de la Loi 1.165 dispose que « *Le responsable de traitement ou son représentant est tenu de prévoir **des mesures techniques et d'organisation appropriées pour protéger les informations nominatives** contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions d'informations dans un réseau, ainsi que contre toute autre forme de traitement illicite* ».

C'est ainsi qu'en matière de sites internet, il 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 d'informations nominatives. 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 données liées à la carte bancaire

Les données nécessaires à la réalisation d'une transaction à distance par carte de paiement sont 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 de 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 de 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 de 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.

Cas particulier de la protection des copies des documents d'identité

S'agissant des **documents d'identité** la Commission 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 informations nominatives 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.

La Commission 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. C'est pourquoi elle a adopté par délibération n° 2015-113 une recommandation sur la collecte et la conservation de la copie de documents d'identité officiels, qui est disponible sur son site Internet www.ccin.mc.

La Commission 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.

➤ 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.