COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

28 janvier 2016 : 10ème JOURNÉE EUROPÉNNE DE LA PROTECTION DES DONNÉES À CARACTERE PERSONNEL

La protection des données personnelles : une matière qui concerne tout le monde

LA CCIN VOUS ACCOMPAGNE

La Commission de Contrôle des Informations Nominatives (CCIN) a pour mission de veiller au respect des libertés et droits fondamentaux des personnes dans un domaine particulier : l'utilisation de leurs informations personnelles.

Elle s'assure ainsi que l'exploitation informatique qui en est faite ne porte pas atteinte à la vie privée des justiciables, à leur liberté d'aller et de venir, à leur liberté de conscience, (...).

Dans ce cadre, elle exerce :

- Une mission d'enregistrement et d'instruction des dossiers ;
- Une mission de conseil et de proposition ;
- Une mission de contrôle et d'investigation.

Toute personne dont les droits reconnus par la loi relative à la protection des informations nominatives ont été méconnus peut saisir la Commission afin que celle-ci prenne toutes les mesures visant à faire cesser la violation.

La CCIN est là pour accompagner toutes les entités publiques et privées dans l'accomplissement de leurs formalités.

Pour nous contacter :
12, Avenue de Fontvieille - 98000 - Monaco
Tél : (+377) 97.70.22.44 - Fax : (+377) 97.70.22.45
Email : ccin@ccin.mc
Horaires d'ouverture : du lundi au vendredi de 9h00 à 12h30 et de 13h30 à 17h30

Sommaire

L'explosion des objets connectés dans la vie de tous les jours et ses conséquences pour la protection des données personnelles.

Les objets qui nous entourent sont aujourd'hui de plus en plus connectés entre eux (TV, frigidaires, lunettes...) permettant ainsi aux entreprises de collecter toujours davantage de données sur les utilisateurs. Même le corps humain devient connecté via l'utilisation de capteurs corporels connectés (bracelets, tensiomètres...).

Les risques liés à l'utilisation de ces données sont réels. Une surveillance clandestine des utilisateurs peut ainsi s'exercer et des données sensibles, notamment de santé, peuvent être communiquées à des tiers, tels des assureurs et des banques.

L'utilisation de ces objets connectés nécessite donc l'implication de tous les acteurs – développeurs, utilisateurs et Autorités de protection des données – pour la mise en place de mesures de sécurité renforcées, de mesures organisationnelles adaptées et de mesures d'encadrement des relations contractuelles, parfois dès la conception des objets.

Les données de santé collectées par le biais des objets connectés : une manne pour les assureurs peu scrupuleux ?

Par le biais des montres, bracelets et autres objets connectés, il est possible aujourd'hui de mesurer le sommeil, le rythme cardiaque ou le nombre de calories brûlées lors d'une activité physique,... Ces données relatives au bien-être peuvent être considérées comme des données de santé ; données qui sont particulièrement sensibles et dont le traitement est par principe interdit, sauf dans des cas très encadrés.

Or, des assureurs américains ont déjà annoncé leur souhait d'utiliser les objets connectés dans le suivi de leurs clients et la prise en compte des données dans l'indemnisation en cas de dommage.

CCIN
COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

LA PROTECTION DES DONNÉES PERSONNELLES : UNE MATIÈRE QUI CONCERNE TOUT LE MONDE

Une erreur humaine à l'origine de la diffusion de l'identité de patients atteints du sida

En septembre dernier, l'hôpital de Chelsea et Westminster, une des cliniques les plus réputées de Londres dans le dépistage et le traitement du VIH (virus de l'immunodéficience humaine) a diffusé par erreur l'identité de près de 780 patients atteints du sida ou d'autres pathologies sexuellement transmissibles.

Des informations confidentielles telles que les noms, adresses emails et parcours de soins ont ainsi fuité lors de l'envoi d'une newsletter, intitulée « *Option E* », qui permet à chaque patient abonné de prendre rendez-vous et de recevoir ses résultats. Or, cette fois ci, en raison d'une erreur humaine, cette lettre électronique a révélé à chaque destinataire l'identité, normalement masquée, de tous les autres destinataires.

Des pirates informatiques s'attaquent aux données des utilisateurs de sites de rencontre

Un groupe de pirates informatiques, se faisant appeler « *The Impact Team* », a rendu public l'été dernier, tout un ensemble de fichiers présentés comme représentant l'intégralité de la base de données du site de rencontre Ashley Madison.

Non contents de dénoncer les principes de ce site, leader mondial des rencontres extraconjugales, ainsi que ses utilisateurs qualifiés de « *salauds* » et de « *menteurs* », les pirates ont également reproché à Ashley Madison d'avoir menti : en effet, si le site propose une option payante pour qu'un utilisateur supprime toutes ses données enregistrées, ces données ne seraient en réalité pas supprimées.

Ashley Madison n'est pas le premier site de rencontres d'un soir à être victime d'un tel piratage : quelques mois auparavant, Adultfinder, avait également vu les profils de ses utilisateurs être mis en ligne.

Les jouets pour enfants deviennent également connectés

De nombreux fabricants proposent désormais des objets connectés pour enfants ; que ce soient des robots, des drones, des poupées ou des peluches. Comme pour les objets pour adultes, ces jouets fonctionnent en général avec un smartphone ou une tablette qui sert de télécommande pour les contrôler directement, mais également de relais pour échanger des données avec les serveurs du fabricant. Ces données sont alors consultables sur l'appareil mobile ou sur le service web de l'éditeur.

Le risque de réutilisation des données collectées (profilage publicitaire...) est ainsi très élevé.

Boulanger épinglé par la CNIL pour commentaires déplacés sur ses clients

« *Client très con* », « *fort accent africain* », « *juive* », « *n'a pas de cerveau* »...Voila juste quelques exemples des commentaires qui figuraient dans les fichiers clients du magasin Boulanger d'Annemasse, une société spécialisée dans l'électroménager et le multimédia.

Si le recours à des commentaires dans un fichier n'est pas interdit dans la mesure où il permet le suivi des clients, la Commission Nationale de l'Informatique et des Libertés (CNIL) a toutefois mis en demeure Boulanger de ne plus enregistrer de « *commentaires excessifs* » dans lesdits fichiers.

En effet, au total, ce ne sont pas moins de 5.828 commentaires déplacés qui ont été constatés par la CNIL lorsqu'elle a eu accès au fichier pendant une investigation dans un des magasins de l'enseigne, en février 2015.

Les voitures connectées, une révolution pour la conduite mais une atteinte à la vie privée

Après une expérimentation d'un an, les Autorités de la sécurité routière américaine ont récemment donné le feu vert aux véhicules connectés pour rouler sur les routes du Pays. Désormais, grâce au Wi-fi, ces voitures sont connectées en permanence les unes aux autres et peuvent ainsi échanger différentes informations, comme leur vitesse ou encore leur position. Si, sur le papier, cette initiative peut paraître révolutionnaire et attrayante pour certains, elle peut également se révéler particulièrement intrusive pour d'autres.

En effet, les organismes prêteurs ont trouvé l'arme idéale pour faire pression sur les mauvais payeurs. Une traite d'un crédit auto impayée et le prêteur peut localiser à distance, via le GPS du dispositif, la voiture et la récupérer très rapidement. Plus grave, grâce au coupe-démarrage électronique commandé à distance, il peut également empêcher le véhicule de redémarrer.

Nécessité de renforcer la sécurité des traitements de données obtenues au moyen des objets connectés

Les risques liés aux objets connectés sont de plus en plus nombreux et variés. Ainsi des pirates informatiques peuvent facilement détourner les informations relatives aux allées et venues des propriétaires, enregistrées par les serrures connectées par des applications smartphones dédiées et rien n'empêche de penser qu'un jour des personnes malveillantes puissent aller jusqu'à s'approprier la vie numérique et l'identité d'un individu.

Par ailleurs, les risques liés à la confidentialité et au nécessaire respect de la vie des personnes ne sont pas négligeables puisque ces objets connectés révèlent les habitudes de leurs propriétaires.

Les technologies de géolocalisation comme les montres et voitures connectées offrent aujourd'hui la possibilité de suivre à la trace leur propriétaire par l'intermédiaire des cartes et itinéraires qu'elles proposent, conduisant à un risque toujours plus grand de surveillance généralisée.

Face à tous ces risques, un « *droit à la désactivation* » pour les consommateurs devient une nécessité.

Des règles simples mais efficaces pour sécuriser ses données de santé dans un monde connecté

Dans son numéro de janvier 2016, le magazine 60 millions de consommateurs a publié une liste de conseils afin de permettre aux utilisateurs d'objets connectés (montres, tensiomètres...) de sécuriser leurs données de santé.

Ces conseils qui sont au nombre de trois sont essentiels pour « *un usage modéré et éclairé des applications ou logiciels liés aux objets de santé, mais aussi des innombrables applis autonomes proposées par Android et IOS* ».

1 - Ne pas trop se dévoiler : afin d'éviter de donner trop de détails sur son identité il convient, par exemple d'utiliser un pseudonyme, de mettre une date de naissance différente, d'utiliser une adresse de messagerie électronique dédiée à l'objet connecté, et, bien entendu, de changer régulièrement son mot de passe sur toute application mobile.

2 - Ne pas partager tous azimuts : ces données sont souvent utilisées à des fins commerciales, en conséquence, si elles se retrouvent automatiquement sur les réseaux sociaux, pensez à désactiver l'option de partage automatique.

3 - Choisir une application de qualité : il est important de bien étudier les caractéristiques et options des applications avant de les acheter et de préférer celles qui ont des conditions générales et informent, par exemple, sur la localisation de leur serveur de stockage.

CCIN
COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

FOIRE AUX QUESTIONS

Qu'est-ce qu'une information nominative ?

C'est une information, sous quelque forme que ce soit, qui permet d'identifier une personne physique déterminée ou déterminable de manière directe ou indirecte notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propre(s) à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Nom, prénom, numéro de téléphone, de matricule, de client, de plaque d'immatriculation, adresse postale, adresse IP,...

Qu'est-ce qu'un traitement automatisé d'informations nominatives ?

C'est toute opération ou ensemble d'opérations portant sur de telles informations : la collecte, l'enregistrement, l'organisation, la modification, la conservation, l'extraction, la consultation, la destruction, l'exploitation, l'interconnexion, le rapprochement, la communication d'informations par transmission, diffusion ou toute autre forme de mise à disposition.

Toute action portant sur une information nominative effectuée sur tout support numérique.

Qu'est-ce que le droit d'accès ?

Le droit d'accès est le droit pour toute personne concernée d'obtenir du responsable d'un traitement la confirmation que les données la concernant font l'objet d'un traitement ainsi que des informations sur la finalité dudit traitement, les catégories d'informations sur lesquelles il porte et les destinataires auxquels les informations sont communiquées.

Ce droit permet également à la personne concernée d'obtenir la communication de ces informations, sous une forme écrite, non codée et conforme au contenu des enregistrements.

Qu'entend-on par « *consentement de la personne concernée* » ?

Le consentement est un terme important dans la législation sur la protection des données : le consentement est l'un des critères permettant de légitimer le traitement de données à caractère personnel.

Le consentement peut être donné oralement, par écrit ou sous toute autre forme appropriée. Avant de pouvoir considérer que la personne concernée a donné librement son consentement à un traitement spécifique, celle-ci doit avoir reçu des informations suffisantes pour être en mesure de comprendre la portée et les conséquences de son consentement, y compris les avantages et/ou désavantages du traitement.

Outre le fait qu'il doit être donné librement, le consentement doit être spécifique et il ne doit y avoir aucun doute quant au fait qu'il ait été donné ou non. Par ailleurs, le consentement est strictement lié au traitement dont la personne concernée a été informée. Il ne peut, par la suite, faire l'objet d'une extension accordée par quelqu'un d'autre et ne peut donc jamais être donné pour quelque chose dont la personne concernée n'était pas informée.

Quels sont les pouvoirs de la CCIN ?

- Une possibilité de retirer les autorisations qu'elle a délivrées ;
- Un pouvoir d'instruction des plaintes et des pétitions ;
- Un pouvoir d'investigation, d'office ou sur plainte ;
- Un pouvoir de sanction administrative : avertissement, mise en demeure ;
- La faculté de saisir le Président du Tribunal de Première Instance si la mise en demeure est restée infructueuse ;
- L'obligation de dénoncer au Procureur Général toute irrégularité constitutive d'une infraction pénale ;
- La possibilité de publier ses sanctions.

Tout manquement à la Loi n° 1.165 constitue une infraction pénale passible d'une amende de 9.000 à 18.000 et d'un emprisonnement d'1 à 6 mois.

Nouveaux pouvoirs d'investigation : qu'est ce qui change ?

Suite à trois décisions du Tribunal Suprême d'octobre 2013, la CCIN avait perdu ses pouvoirs d'investigation.

La Loi n° 1.420 du 1er décembre 2015 *portant modification des articles 18 et 19 de la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives*, les a réintroduits en tenant compte des impératifs procéduraux nécessaires à un contrôle garantissant des droits suffisants aux personnes investiguées.

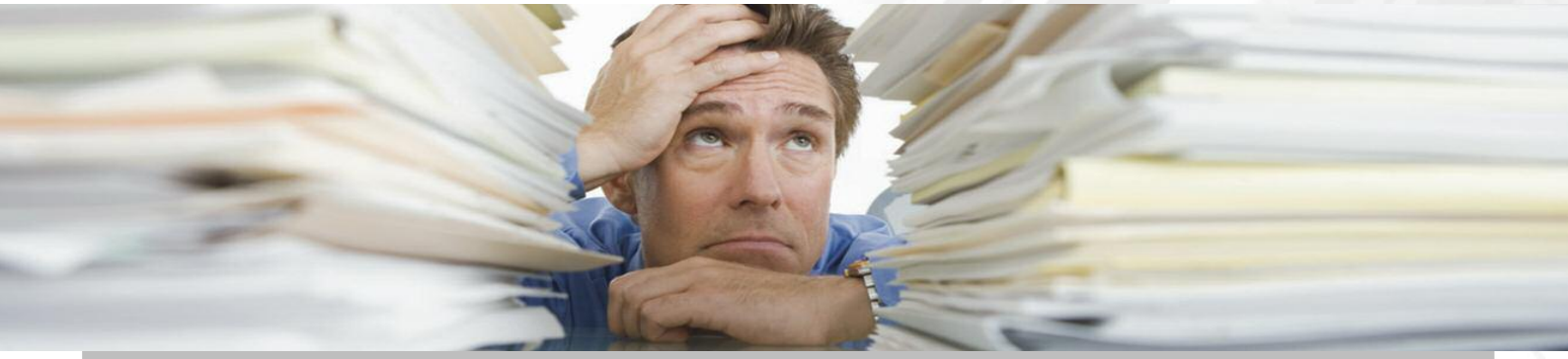
De fait, la Loi susvisée a introduit des changements notables par rapport aux précédents pouvoirs de contrôle :

- L'existence de 2 procédures d'investigation différentes, selon que le contrôle est effectué à titre « *préventif* » ou suite à une plainte ;
- L'introduction d'un droit d'opposition à l'entrée des investigateurs dans les locaux professionnels privés du responsable de traitement, sauf « *urgence ou risque imminent de destruction ou de disparition de pièces ou de documents* », afin de ne pas porter une atteinte disproportionnée au principe de l'inviolabilité du domicile consacré par l'article 21 de la Constitution ;
- Un contrôle par le Juge renforcé ;
- La consécration claire du contradictoire par l'ajout à l'article 19 d'un délai d'un mois permettant au responsable de traitement de faire valoir ses observations sur les manquements qui lui sont reprochés.

Aussi, les investigations pourront dès 2016 permettre de limiter les atteintes aux droits des personnes concernées, tout en respectant les droits des responsables de traitement, avec pour objectif que la Commission européenne puisse reconnaître à Monaco le niveau de protection adéquat en matière de traitement des informations nominatives.

CCIN
COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

COMMENT SE METTRE EN CONFORMITÉ ?



Soumettre à la CCIN, préalablement à leur mise en exploitation, tous les traitements automatisés d'informations nominatives.

Catégories de personnes dont je traite les données et pourquoi je traite ces données ?

Ne pas raisonner en termes de logiciels mais de finalités

Salariés :
- gestion des habilitations,
- gestion de la paie,
- gestion administrative des salariés,
- élection des Délégués du Personnel,
- contrôle d'accès aux locaux (badge nominatif, vidéosurveillance, système biométrique),
- téléphonie fixe / mobile, ...

Clients / Fournisseurs :
- fichiers clients / prospects, fournisseurs,
- messagerie électronique,
- site Internet, vente en ligne.

Ai-je des traitements liés à mon activité ?

Lutte contre le blanchiment,
Enregistrement des conversations téléphoniques,
Données « *sensibles* »,
Organisme d'assurance...

Combien de temps je conserve les informations ?

Les informations doivent être conservées pour une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles ont été collectées.

La CCIN diminue fréquemment les durées de conservation.

Quelles catégories de données je traite ?

Données « *courantes* » : nom, prénom, coordonnées postales, téléphoniques, bancaires, situation de famille, ...

Données « *sensibles* » : faisant apparaître directement ou indirectement des opinions ou des appartenances politiques, raciales ou ethniques, religieuses, philosophiques, ou syndicales, ou encore des données relatives à la santé, y compris les données génétiques, à la vie sexuelle, aux mœurs, aux mesures à caractère social : principe d'interdiction de traitement automatisé ou non.

Exceptions à ce principe d'interdiction de traitement des données « *sensibles* » :

- Consentement écrit et exprès,
- Motif d'intérêt public pour les Autorités Publiques ou les Sociétés Concessionnaires,
- Membres d'une institution ecclésiale ou d'un groupement politique, religieux ...
- Médecine préventive, administration de soins, intérêt de la recherche...
- Informations rendues publiques par la personne concernée,
- Constatation, exercice ou défense d'un droit en justice, ou réponse à une obligation légale.

Je transmets des données à l'étranger ?

Ce Pays offre-t-il un niveau de protection adéquat en termes de protection des informations nominatives ?

Si tel n'est pas le cas, ce transfert d'informations est soumis à l'autorisation préalable de la CCIN.

Attention l'autorisation n'est pas systématique, le transfert doit présenter des garanties suffisantes. Il s'agit d'un élément à prendre en compte notamment dans le choix d'un prestataire.

Les formalités à accomplir : 4 types de formalités en fonction :

De l'entité qui exploite les traitements :

- société privée : **déclaration simplifiée ou déclaration ordinaire**
- entité publique et assimilée : organisme de droit privé investi d'une mission d'intérêt général ou concessionnaire de service public : liste fixée par Arrêté Ministériel (Monaco Télécom, SMEG, ...) : **demande d'avis**

De la finalité du traitement (que si société privée même assimilée au public) :

- soupçons d'activités illicites, infractions, mesures de sûreté,
- données biométriques nécessaires au contrôle de l'identité des personnes,
- mis en œuvre à des fins de surveillance : **demande d'autorisation**
- recherche dans le domaine de la santé secteur privé et public (sauf recherche biomédicale) : **demande d'avis.**

LES 12 GRANDS PRINCIPES DE LA SÉCURITÉ DES TRAITEMENTS

1. Connaître le système d'information et ses utilisateurs ;
2. Maîtriser le réseau ;
3. Authentifier les utilisateurs ;
4. Sécuriser les équipements terminaux ;
5. Sécuriser le réseau interne ;
6. Protéger le réseau interne de l'Internet ;
7. Superviser et contrôler les systèmes ;
8. Sécuriser l'administration du réseau ;
9. Contrôler l'accès aux locaux et la sécurité physique ;
10. Définir les règles d'utilisation des imprimantes et photocopieuses ;
11. Organiser la réaction en cas d'incident ;
12. Sensibiliser les utilisateurs aux règles d'hygiène informatique élémentaires et faire auditer la sécurité.

COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

NOTRE ACTUALITÉ

Ce qui change en 2016 :

Pré-dépôt des formulaires en lignes, grâce à l'adjonction sur notre site Internet d'un nouvel outil didactique. Des explications, définitions ou exemples sont ainsi fournis aux déclarants et demandeurs afin de les guider dans leurs démarches jusqu'à l'envoi électronique du dossier à la CCIN.

Des formulaires plus intuitifs : Si le contenu des informations demandées ne change pas, les nouveaux formulaires disponibles sur le site Internet ont été complètement repensés et les responsables de traitements sont désormais davantage accompagnés dans leurs démarches.

De nouvelles recommandations : Conformément à l'article 2-10° de la Loi n° 1.165, la CCIN peut *« formuler toutes recommandations entrant dans le cadre des missions qui lui sont conférées par la loi »*.

Ces recommandations constituent un cadre de référence utile aux responsables de traitement souhaitant déposer les formalités y afférentes, et détaillent par exemple les fonctionnalités et les informations nominatives qui peuvent y être exploitées. Aussi, la Commission a prévu d'adapter certaines recommandations existantes et d'en adopter de nouvelles, afin d'accompagner au plus près les responsables de traitements dans l'accomplissement de leurs formalités.

Un champ d'application des déclarations simplifiées élargit : La Commission peut également proposer au Gouvernement Princier d'édicter par voie réglementaire des normes fixant les caractéristiques auxquelles doivent répondre des catégories déterminées de traitements ne comportant manifestement pas d'atteinte aux libertés et droits fondamentaux, lesquels traitements pouvant alors faire l'objet d'une déclaration simplifiée de conformité, ou être dispensés de toute obligation de déclaration, dans conditions prévues par l'Arrêté Ministériel ad hoc.

Ouvrir la possibilité de dispenser de toute formalité les traitements les plus usuels et les moins intrusifs au regard des données traitées.

Un dialogue intensifié avec les responsables de traitement par l'organisation de réunions par secteur d'activité.

Un site internet modernisé pour répondre à toutes vos questions : www.ccin.mc

MM. Jean-Yves Peglion ; Florestan Bellinzona ; Rainier Boisson ; Guy Magnan ; Mme Agnès Lepaulmier ; MM. Philippe Blanchi ; Jean-Patrick Court.

Les Membres de la Commission

Les Membres de la Commission ont été nommés pour cinq ans par Ordonnance Souveraine en date du 6 juin 2014.

Le Président et le Vice-Président de la Commission ont été élus le 26 juin 2014 lors de la première session plénière de la Commission.

Président de la CCIN
M. Guy MAGNAN

Vice-Président de la CCIN
M. Rainier BOISSON

Membres de la CCIN
M. Florestan BELLINZONA
M. Philippe BLANCHI
M. Jean-Patrick COURT
M. Jean-Yves PEGLION

Le Secrétariat Général

Secrétaire Général
Agnès Lepaulmier

Division Informatique
Jean SISTI
Stéphane RODRIGUEZ

Division Juridique
Benjamin AOUIZERAT
Céline ANSQUER
Aurore CAMPANA
Florence DUBOSC
Florian MENINI

Division Administrative
Elodie FEA
Florence ZUODAR

www.ccin.mc