ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 30 – nov. – déc. 2009

LES 10 CONSEILS DE LA CNIL POUR SECURISER SON SYSTEME D'INFORMATION

Cnil publie 10 conseils en matière de sécurité

▪ Les 10 conseils s'inscrivent dans le cadre de la **loi Informatique et libertés**, laquelle organise la gestion des données personnelles autour de quatre axes :

- les formalités préalables (déclarations normales, simplifiée, autorisations) ;
- le droit des personnes (à l'information, d'accès, de modification, etc.) ;
- les flux transfrontières de données ;
- la sécurité des traitements et de leurs données.

▪ Ce dernier axe relatif à la **sécurité**, bien trop souvent ignoré, repose essentiellement sur les articles 34 et 35 de la loi Informatique et libertés.

▪ L'**article 34** fait peser sur le responsable du traitement l'obligation de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour **préserver la sécurité** des données et, notamment, d'empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

▪ L'**article 35** vise les cas où le responsable du traitement sous-traite tout ou partie du traitement auprès d'un tiers et définit les relations entre le **sous-traitant** et le responsable du traitement, pour ce qui concerne la sécurité.

Un référentiel de « bonnes pratiques »

▪ Si la Cnil s'est déjà prononcée de très nombreuses fois sur les questions de sécurité lorsqu'un dossier ou un projet lui est soumis, c'est en revanche l'une des premières fois qu'elle le fait sur cette question en l'abordant selon une approche générale.

▪ Il s'agit de « **conseils** » et non d'une « délibération », mais leur **portée juridique** ne sauraient être pour autant sous-estimée. A tout le moins, ils s'intègrent dans ce qu'on peut qualifier de référentiel de « **bonnes pratiques** ».

▪ Sans y être contraintes, les entreprises sont vivement invitées à suivre ces conseils de la Cnil, gardienne de l'application de la loi Informatique et libertés. Ainsi, le **conseil n°2** « Concevoir une procédure de création et de suppression des comptes utilisateurs » doit être mis en place au sein des entreprises, mais également intégré dans la charte de l'utilisation des systèmes d'information.

▪ Les **conseils n°9 et 10**, respectivement « Anticiper et formaliser une politique de sécurité du système d'information » et « Sensibiliser les utilisateurs aux risques informatiques et à la loi informatique et libertés », imposent à l'entreprise de dépasser le stade de la simple charte.

▪ Ils nécessitent de passer au stade d'une véritable **gouvernance de la sécurité** au sein de laquelle on retrouvera la charte des personnels pour l'utilisation des systèmes d'information mais aussi la charte « administrateur», la charte « accès » ou encore la charte « Informatique et libertés ».

▪ Le **conseil n°10** impose le passage d'une gouvernance statique à une **gouvernance dynamique** à travers des plans de formations ou de sensibilisation encore bien peu nombreux dans les entreprises.

Les enjeux

Dresser la liste de l'ensemble des mesures que les détenteurs de fichiers doivent mettre en œuvre, essentiellement par l'intermédiaire de leur direction des systèmes d'information (DSI) ou de leur responsable informatique pour sécuriser le système d'information.

(1) www.cnil.fr/ actualité du 12-10-2009.

Les conseils

Ces 10 conseils s'intègrent dans le cadre des conditions d'application des articles 34 et 35 de la loi.

Pour plus d'informations, ces dix conseils seront abordés lors du petit déjeuner-débat le 18 novembre 2009 relatif à la question de la sécurité des systèmes d'information.

ERIC BARBRY
EMMANUELLE NAHUM

LA CNIL DISPENSE DE DECLARATION LES TRAITEMENTS RELATIFS A LA PANDEMIE GRIPPALE

Quelles informations personnelles peut-on recenser auprès des salariés ?

Les enjeux

▪ Depuis le **10 septembre 2009**, même en l'absence de Cil et de déclaration de fichier de gestion du personnel, les responsables d'un traitement mis en œuvre dans le cadre d'un plan de continuité de l'activité (PCA) permettant de faire face à une épidémie grippale de grande ampleur ne sont plus tenus d'effectuer de formalités préalables s'ils respectent les dispositions de la dispense n°14 (1).

▪ En août 2009, la Cnil publiait ses **recommandations** relatives aux traitements de données à caractère personnel dans le cadre de l'établissement et du suivi du PCA devant permettre de faire face à une épidémie grippale de grande ampleur.

▪ Elle indiquait que sous réserve que les données collectées ne soient pas soumises à un régime particulier, le traitement mis en œuvre dans ce cadre pouvait bénéficier d'une **dispense de déclaration** en cas de désignation d'un correspondant à la protection des données par l'organisme responsable du traitement ou être déjà couvert par une déclaration de fichier de gestion du personnel si une telle déclaration a déjà été effectuée par l'organisme (2).

▪ Un tel traitement est considéré comme légitime par la Cnil mais, afin de bénéficier de la dispense, il ne peut intervenir qu'à la condition que la France ait atteint le seuil d'alerte de **situation 4**. Lorsque le seuil d'alerte de situation 7 (fin de pandémie) est atteint, les données nominatives doivent être supprimées.

La dispense a un **effet immédiat** puisqu'à ce jour, le seuil d'alerte de situation 4 (cas groupés humains) a été dépassé, la France se trouvant en **situation 5**, à savoir une situation dans laquelle il existe une « transmission interhumaine d'un virus grippal dans au moins deux pays non limitrophes d'un même continent.

Simplifier les obligations des employeurs mettant en œuvre un traitement d'informations personnelles des salariés lié à un plan de continuité de l'activité (PCA) en cas de Pandémie grippale.

(1) Délib. Cnil 2009-476 du 10-9-2009, norme simplifiée n°14.

(2) Délib. Cnil 2005-002 du 13-1-2005, norme simplifiée n°46.

Quelles sont les conditions de la dispense de déclaration auprès de la Cnil ?

Les conseils

▪ La dispense n°14 vise les traitements ayant pour finalités :

- l'élaboration d'un plan de continuité de l'activité dans le contexte d'une pandémie grippale en identifiant les **personnes susceptibles d'être indisponibles** en raison de leur situation familiale ou / et de leur mode de déplacement ;

- l'**information du personnel** quant aux mesures prises par l'organisme ;

- la réalisation de **traitements statistiques** non nominatifs liés à l'élaboration et à l'activation du plan dans l'entreprise.

▪ Les données traitées dans ce cadre ne peuvent en aucun cas comprendre le numéro de sécurité sociale ni **aucune donnée relative à la santé** des personnes.

▪ Seules pourront être traitées un **nombre restreint de données** énumérées par la dispense, par exemple, celles relatives à l'identité et aux coordonnées personnelles, à la présence au foyer d'enfants de moins de trois ans (sous la forme de réponse oui et non uniquement) ; aux caractéristiques du poste (contact avec le public, déplacements etc.), à la volonté de travailler à distance en cas de pandémie ou encore au mode de transport habituel et alternatif.

Quand bien même l'ensemble de ces dispositions serait respecté, la dispense ne s'appliquera pas en cas de mise en œuvre de **transferts de données** à caractère personnel à destination de pays tiers. La mise en œuvre de tels transferts devra faire l'objet d'une demande d'**autorisation préalable**.

Comme tout traitement de données à caractère personnel, celui mis en œuvre dans le cadre d'un PCA destiné à lutter contre la pandémie grippale doit faire l'objet d'une information conforme à l'article 32 de la loi Informatique et libertés portée à la connaissance des personnes concernées.

CELINE AVIGNON
CLAIRE ALBREKTSON.

Peut-on avoir accès à toutes informations contenues dans un fichier ?

Source

▪ **Oui** La personne qui décide d'exercer son droit d'accès n'a aucune justification à donner pour ce faire. De même, qu'elle n'a pas à justifier d'un contentieux quelconque. Ce droit n'a pas besoin d'être motivé.

Cependant, afin de limiter l'usage abusif de ce droit qui peut apparaître dans certains cas comme un acte visant délibérément à gêner l'entreprise détentrice du fichier, la Cnil a le pouvoir de délier l'entreprise concernée de ses obligations en matière de droit d'accès (1).

Pour limiter les demandes de droits d'accès abusives et répétées, le législateur a retenu le principe du paiement d'une redevance pour obtenir la copie des informations. Le montant ce cette redevance est fixé par arrêté ministériel.

(1) Cf. la jurisprudence disponible sur notre site.

Pour les données « sensibles », la loi prévoit un droit d'accès « indirect » défini par les articles 40 à 42 de la loi du 6 janvier 1978. Ainsi, l'accès aux informations médicales s'exerce par l'intermédiaire d'un médecin.

Peut-on exiger que soient modifiées certaines informations contenues dans un fichier ?

▪ **Oui** Le droit de rectification est un droit complémentaire au droit d'accès. Il n'est, cependant, pas soumis aux mêmes conditions d'exercice, lesquelles sont fixées par l'article 40 de la loi du 6 janvier 1978.

La personne qui a demandé le droit d'accès n'a pas tous pouvoirs sur les informations qui la concerne. Elle peut seulement les compléter, les mettre à jour, les clarifier ou en demander l'effacement.

Contrairement au droit à l'information et au droit à la communication pour lesquels la personne n'a pas besoin de se justifier ou de motiver sa démarche, l'exercice effectif de rectification est soumis à des conditions précises (2).

(2) Cf. la jurisprudence disponible sur notre site.

L'entreprise peut-elle avoir recours à des technologies d'identification et de surveillance ?

▪ **Oui** Les technologies d'identification et de surveillance doivent faire l'objet d'une déclaration ou d'une autorisation, selon la nature des technologies.

▪ En milieu professionnel, la mise en œuvre de ces techniques suppose le respect des règles suivantes :

- information des instances représentatives du personnel sur l'introduction de nouvelles technologies ;
- information des instances représentatives du personnel sur les dispositifs de contrôle et de surveillance des salariés ;
- information des personnes concernées au moyen d'une charte d'utilisation des systèmes d'information annexée au règlement intérieur.

En effet, dans la majeure partie des cas l'introduction d'une nouvelle technologie élargit le champ des contrôles pouvant être opérés par l'employeur.

Prochains événements

Sécurité des systèmes d'information, la nouvelle donne juridique : 18 novembre 2009

▪ **Eric Barbry** animera un petit-déjeuner débat consacré à la nouvelle donne juridique en terme de sécurité des systèmes d'information.

L'année 2009 marque à n'en pas douter une « nouvelle donne » dans le droit de la sécurité des systèmes d'information en plaçant « l'abonné » au cœur du dispositif, comme en témoigne la récente loi Hadopi ou encore le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure, Loppsi.

A titre d'exemple, l'article 11 de l'Hadopi modifiant l'article 336-3 du Code de la propriété intellectuelle prévoit que « La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits (...) lorsqu'elle est requise ».

En environnement professionnel la personne titulaire de l'accès sera, sans nul doute, l'entreprise. De fait, c'est à elle qu'il appartient de veiller à ce que l'accès à internet ne fasse pas l'objet d'une utilisation de nature à réaliser des actes de contrefaçon.

De même, la « nouvelle donne » se matérialise par un ensemble de nouvelles menaces qui dépassent de loin, le système d'information de l'entreprise. Il importe aujourd'hui tout autant de s'intéresser à ce qui se passe au sein du SI de l'entreprise, qu'à ce qui peut se dire à son sujet, au sein des réseaux sociaux, nouveau terrain de prédilection des pirates en tout genre ou des concurrents peu scrupuleux.

Nouvelles menaces, nouvelle donne, nouvelle régulation en termes de sécurité des systèmes d'information, sont les principaux thèmes qui seront abordés lors de notre prochain petit-déjeuner.

Nous vous remercions de bien vouloir confirmer votre présence avant le 9 novembre 2009 par courrier électronique en indiquant vos coordonnées et le nombre de personnes assistant au petit-déjeuner à l'adresse suivante : invitation-conference@alain-bensoussan.com ou en faxant le bulletin d'inscription au 01 41 33 35 36.

Droit à l'oubli numérique

▪ **Alain Bensoussan** participera à l'atelier du 12 novembre 2009 organisé par Nathalie Kosciusko-Morizet, secrétaire d'état chargée de la prospective et du développement de l'économie numérique.

Les débats sont animés par Bernard Benhamou,

Délégué aux usages de l'Internet

L'atelier se tiendra de 9h00 à 12h30

SciencesPo

Amphithéâtre Emile Boutmy

27,rue Saint Guillaume

75007 Paris

Télécharger le programme

▪ **Inscription gratuite** auprès du Centre d'analyse stratégique

10 conseils en matière de sécurité

▪ La Cnil dresse une liste de l'ensemble des mesures que les détenteurs de fichiers doivent mettre en œuvre, essentiellement par l'intermédiaire de leur direction des systèmes d'information (DSI) ou de leur responsable informatique pour **sécuriser le système d'information de l'entreprise** (1).

Source

(1) www.cnil.fr/ actualité du 12-10-2009.

Deux fichiers de prévention des atteintes à la sécurité publique

▪ Création de **deux traitements** de données à caractère personnel relatifs respectivement à la prévention des atteintes à la sécurité publique aux enquêtes administratives liées à la **sécurité publique** (2). La Cnil a rendu un **avis favorable** sur ces deux projets de décrets encadrant mieux les fichiers de renseignement (3).

(2) Décret n° 2009-1249 et n° 2009-1250 du 16-10-2009.
(3) Délib. n° 2009-355 et n° 2009-356 du 11-6-2009.

Contrôle de la condition de résidence par l'assurance maladie

▪ Création d'un traitement de données à caractère personnel relatif au contrôle de la condition de résidence des ressortissants du régime général d'assurance maladie (4).

▪ La Cnil a rendu un **avis favorable** sur les traitements mis en oeuvre par la Caisse nationale d'assurance vieillesse des travailleurs salariés (CNAVTS) et la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) et relatifs à une **interconnexion de fichiers** à des fins de contrôle de la condition de résidence pour l'attribution de droits relatifs aux prestations sociales (5).

(4) Décret n° 2009-1305 du 26-10-2009.
(5) Délib. n° 2009-325 Cnil du 14-5-2009.

Echange des informations concernant les données biométriques

▪ Etablissement des spécifications en matière de résolution et d'utilisation des empreintes digitales à des fins de vérification et d'**identification biométriques** dans le système d'information sur les visas (6).

(6) Décision 2009/756/CE du 9-10-2009.

Un fichier des inventions du personnel du ministère de la défense

▪ Création par le ministère de la défense (délégation générale pour l'armement) d'un traitement automatisé de données à caractère personnel relatif à la gestion des produits entrant dans le cadre de la propriété industrielle dénommé « GAPI » (7).

(7) Arrêté du 25-8-2009.

La loi informatique et libertés et les collectivités locales : 50 questions

▪ La Cnil a publié un guide sous la forme de « 50 questions » qui rappelle l'ensemble des obligations qui incombent aux collectivités locales (8).

(8) 50 questions sur la loi I et L.

Directeur de la publication : Bensoussan Alain
Rédigée par les avocats et juristes de ALAIN BENSOUSSAN SELAS
Animée par Chloé Torres et Isabelle Pottier, avocat
Diffusée uniquement par voie électronique
ISSN 1634-0698
Abonnement à : paris@alain-bensoussan.com