Juristendances Informatique et libertés

Lettre électronique bimestrielle réalisée par ALAIN BENSOUSSAN - AVOCATS

n° 26 – Mars / Avril 2009

Une nouvelle clause pour encadrer l'« outsourcing » de données à caractère personnel

Le transfert de données personnelles vers les pays tiers

Les transferts internationaux de données à caractère personnel **hors de l'Union européenne** ou vers des pays n'ayant pas fait l'objet d'une reconnaissance par la Commission européenne d'une protection adéquate, nécessitent un **encadrement spécifique**.

Sont notamment concernés, le recours à un **centre d'appels** étranger avec transfert du fichier correspondant pour réaliser les opérations de prospections ou encore la centralisation d'une base de données **CRM** ou **RH**.

De tels flux doivent faire l'objet d'une **autorisation de la Cnil** qui demande à ce titre, la conclusion d'une **convention de flux** de transfert de données, établie à partie de **clauses contractuelles types** élaborées par la Commission européenne (1).

Le G 29 propose une clause spécifique pour la « sous-traitance »

Confronté au phénomène croissant de l'**externalisation des données** personnelles vers des pays tiers, le **G 29** (Groupe de l'article 29) a constaté que les sous-traitants procédaient eux-mêmes à des **transferts ultérieurs** des données vers des "**sous-sous-traitants**" établis hors de l'Union européenne.

Or les clauses contractuelles types ne prévoient pas de tels **transferts complexes**. Cette situation est particulièrement dangereuse lorsque des données sensibles sont transférées.

Par conséquent, la Commission européenne (2) propose d'insérer dans les clauses contractuelles types, une **clause « sous-traitance »** qui imposerait :

- d'obtenir le consentement préalable et écrit de l'exportateur de données ;
- d'effectuer le traitement pour le compte de l'exportateur selon ses instructions ;
- de conclure un contrat écrit avec le sous-traitant mettant à la charge de ce dernier les mêmes obligations que celles mises à la charge de l'importateur des données ;
- lorsque le sous-traitant manque à ses obligations en matière de protection des données conformément au contrat écrit, l'importateur de données assume l'entière responsabilité à l'égard de l'exportateur.

L'essentiel

Doter les entreprises d'un cadre juridique leur permettant de faire face aux mécanismes contractuels actuels en cas de recours à des transferts ultérieurs des données vers des "sous-sous-traitants".

(1) Clauses contractuelles types 2002/16/CE.

Les conseils

- réaliser un avenant aux conventions déjà conclues ;

- Intégrer d'ores et déjà la clause « sous-traitance » dans les nouvelles conventions.

(2) Avis 3/2009 du G 29.

Chloé Torres

Impact sectoriel

Les hébergeurs de données de santé de nouveau soumis à agrément

Comment poursuivre l'activité d'hébergeur de données de santé ?

- Le délai de deux ans pendant lequel les hébergeurs de données de santé (à l'exclusion des hébergeurs de dossiers médicaux personnels) étaient dispensés de l'agrément visé à l'article L.1111-8 du Code de la santé publique est arrivé à **expiration le 1er février 2009**, jour de la publication de la loi du 30 janvier 2007 (1).
- Pour poursuivre leur activité d'hébergement de données de santé, les hébergeurs doivent avoir impérativement formé une **demande d'agrément** auprès du ministère de la santé **avant le 30 janvier 2009**.
- Dans la mesure où un dossier a d'ores et déjà été déposé par l'hébergeur auprès de la Cnil, conformément aux dispositions de la loi relative à l'informatique, aux fichiers et aux libertés, une simple **lettre RAR** à l'attention du **comité d'agrément** faisant référence à l'autorisation de la Cnil, semble nécessaire.
- Le comité d'agrément se trouve au sein de la **Mission pour l'informatisation du système de santé**, du ministère de la santé.

Comment devenir hébergeur de données de santé ?

- Pour les entités qui souhaitent devenir hébergeur de données de santé depuis le 1er février 2009, un **dossier d'agrément complet** doit être adressé au ministère de la santé (Mission pour l'informatisation du système de santé).
- Le ministre chargé de la santé se prononce **après avis de la Cnil** et du comité d'agrément placé auprès de lui.
- La **Cnil** dispose, à compter de la réception du dossier, d'un délai de deux mois, renouvelable une fois, pour se prononcer.
- Le **comité d'agrément** rend son avis dans le mois qui suit la réception du dossier transmis par la Cnil. Ce délai peut être prolongé d'un mois.
- Le ministre chargé de la santé rend son avis dans un délai de deux mois maximum suivant l'avis du comité d'agrément.
- Aux termes de l'article R.1111-10 du Code de la santé publique, à l'issue de ce délai, son **silence vaut décision de rejet**.
- Héberger des données de santé à caractère personnel recueillies auprès de professionnels ou des établissements de santé ou directement auprès des personnes qu'elles concernent sans être titulaire de l'agrément ou sans respecter les conditions de l'agrément obtenu est puni de **trois ans d'emprisonnement** et de **45 000 euros d'amende** (2).

L'enjeu

Garantir la confidentialité et la sécurité des données de santé des patients.

(1) Loi n°2007-127 du 30 janvier 2007.

Les conseils

Bien constituer son dossier d'agrément qui doit comprendre :

- un dossier administratif et financier ;
- un dossier technique relatif à la politique de confidentialité et sécurité ;
- les modèles de contrats conclus avec les personnes à l'origine du dépôt ;
- les modèles de fiche d'information sur l'activité de l'hébergeur.

(2) Article L.1115-1 du code de la santé publique.

Les FAQ juristendances

Certains traitement doivent-ils être extressément autorisés par la Cnil ?

Oui. Certains traitements sensibles ou à risque sont soumis à des formalités particulières d'autorisation et non à une simple déclaration :

- soit en raison des données enregistrées (données génétiques, infractions, etc.),
- soit parce qu'ils poursuivent des finalités spécifiques,
- soit parce qu'ils comportent des transferts de données hors de l'Union Européenne (1).

Ainsi, les entreprises qui se sont dotées de mécanismes permettant l'analyse du risque financier de leurs clients doivent soumettre leur traitement de données à l'autorisation préalable de la Cnil. De même, les entreprises qui ont investi dans des systèmes de gestion intégrée leur permettant de gérer en un point central leurs actifs devront soumettre leur traitement à l'autorisation préalable de la Cnil car elles interconnectent des fichiers ayant des finalités différentes (production, clientèle, marketing, ressources humaines, etc.).

Les traitements de paie et de gestion du personnel contenant le numéro de sécurité sociale doivent faire l'objet d'une demande d'autorisation à la Cnil.

Remarques

(1) Art. 25, 54 et 64 de la loi du 6-1-1978 modifiée.

La Cnil se prononce dans les deux mois suivant la réception de la demande d'autorisation, ce délai peut être renouvelé une fois sur décision motivée de son président. Si la Cnil ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.

Peut-on s'adresser à la Cnil pour obtenir des conseils, de l'information ?

Oui. La Commission nationale de l'informatique et des libertés met à disposition sur son site web des conseils et de l'information sur l'institution, les formalités à remplir, etc.

Deux rubriques ont un contenu informatif : « Découvrir » qui présente aux personnes concernées par l'application de la loi et aux responsables de traitement leurs droits et obligations, et « Approfondir » qui permet de consulter des dossiers thématiques, les principales délibérations de la Cnil, les textes officiels, etc.

Le site offre également la possibilité de télécharger de la documentation, des guides et des rapports (2).

(2) http://www.cnil.fr

On peut également téléphoner au 01 53 73 22 22 ou écrire à la CNIL : 21 rue St-Guillaume 75340 Paris cedex 07.

Y a-t-il des formalités allégées pour les fichiers courants de gestion des ressources humaines ?

Oui. Les fichiers courants de gestion des ressources humaines peuvent faire l'objet d'une déclaration simplifiée sous réserve de respecter la norme simplifiée n° 46 (3).

En outre, si l'organisme ou l'entreprise a désigné un correspondant informatique et libertés, il n'a aucune formalité à effectuer pour ce type de fichiers.

(3) Délib. n° 2005-277 du 17-11-2005 modifiant la norme simplifiée n° 46.

Actualité

Sources

Partage des données de santé à caractère personnel

- La Cnil a eu à connaître d'un **projet d'arrêté** sur la création d'un traitement dénommé « Répertoire partagé des professionnels de santé » (RPPS) entrant dans le champ d'application de l'article 27 de la loi (consultation du RNIPP).
- Il vise permettre d'identifier les **professionnels de santé**, suivre leur exercice, contribuer aux procédures de délivrance et de mise à jour des cartes de professionnel de santé et la réalisation d'études et de recherches anonymisées.
- La Commission a considéré que le projet d'arrêté n'appelait **pas d'observations particulières** au regard de la protection des données (1).

(1) Délib. 2008-075 du 27-3-2008, *JO* du 10-2-2009.

La directive vie privée et communications électroniques bientôt modifiée…

- Le **Groupe de l'article 29** qui réunit les représentants des autorités européennes de protection des données, a publié, le 10 février 2009, un nouvel avis sur la proposition de directive visant à modifier, notamment, la directive 2002/58/CE "vie privée et communications électroniques" (2).
- Il indique être favorable à un accroissement de la **responsabilité des fournisseurs des services** de la société de l'information en matière de protection des données, ainsi qu'à l'inclusion des technologies telles que MMS, RFID et NFC dans le champ d'application de la directive, notamment s'agissant de l'envoi de communications non sollicitées.

(2) G29, Avis du 10-2-9

Première opération de contrôle du fichier STIC

- La Cnil fait état d'une première opération de contrôle, entreprise par ses services afin d'interroger les acteurs faisant usage du Système de Traitement des Infractions Constatées (STIC) et intervenant dans son fonctionnement (3).
- La Cnil à formuler **onze propositions**, dont la mise en œuvre devrait faire l'objet d'un prochain contrôle d'ici le 31 décembre 2011.

(3) Cnil, rapport du 20-1-2009.

Identité et adresse mél : la Cour de cassation se prononce

- La Cour de cassation considère que les constatations visuelles et les adresses IP recueillies par un agent assermenté désigné par la SACEM ne constituent pas un traitement de données à caractère personnel relatif aux infractions, soumis à l'autorisation préalable de la Cnil (4) dès lors que l'agent n'a pas eu recours, pour la collecte des adresses IP, à un traitement préalable de surveillance automatisé.

(4) Cass. crim. 13-1-2009.

Directeur de la publication : Bensoussan Alain
Rédigée et animée par Chloé Torres et Isabelle Pottier
Diffusée uniquement par voie électronique
ISSN 1634-0698
Abonnement à : paris@alain-bensoussan.com