Juristendances Informatique et libertés

Lettre électronique bimestrielle réalisée par ALAIN BENSOUSSAN - AVOCATS

n° 24 – Nov. / déc. 2008

Etablir des règles internes de flux transfrontières intra groupe : le G29 prescrit des règles

Les transferts internationaux de données à caractère personnel

Les transferts internationaux de données à caractère personnel sont **strictement encadrés** par la directive 95/46/CE du 24 octobre 1995 et, en droit français, par la loi Informatique et libertés (1), en particulier lorsque ces transferts ont lieu vers des pays n'assurant pas un **niveau de protection des données suffisant**.

A moins d'entrer dans les **dérogations** définies de manière restrictive à l'article 69 de la loi de 1978 modifiée (2), les transferts sont normalement soumis individuellement à l'**autorisation** de la **Cnil**.

Lorsque ces **transferts** sont effectués **entre filiales d'un même groupe** situées au sein et hors de l'Union européenne, le groupe peut adopter des **règles internes** (BCR ou Binding Corporate Rules) ayant pour but d'encadrer l'ensemble des transferts dans le respect de la réglementation européenne.

Ces règles internes qui régissent les transferts de données au sein du groupe doivent avoir un **caractère contraignant** pour toutes les filiales et contenir un ensemble d'informations essentielles à l'obtention de l'**accord** de chaque autorité de protection des données compétente.

Le recueil de ces **accords** est **centralisé** par l'autorité de protection des données du pays du siège social du groupe, en France, la **Cnil**.

Etablir des règles internes contraignantes pour toutes les filiales

Pour aider les entreprises à établir des règles internes d'entreprise contraignantes (BCR) conformes aux exigences européennes, le **groupe de travail « article 29 »**, organe consultatif européen indépendant sur la protection des données et de la vie privée, a publié, le 24 juin 2008, **deux documents de travail** récapitulant l'ensemble des obligations leur incombant.

Le premier document de travail **WP 153** (3) est un tableau récapitulatif permettant de visualiser les informations qui doivent impérativement figurer dans les règles internes et les informations qui doivent être transmises à la Cnil en vue d'obtenir l'autorisation.

Le second document de travail **WP 154** (4), présente le squelette de règles internes qui pourraient être adoptées au regard de l'ensemble des informations impératives présentées dans le premier document.

Quoiqu'il en soit, il s'agit de **simples propositions** qu'il convient d'adapter au groupe, la Cnil n'acceptant aucun «copier – coller».

Les enjeux

Pouvoir effectuer des transferts de données à caractère personnel entre filiales d'un même groupe situées au sein et hors de l'Union européenne.

(1) Art. 68 à 70 de la loi du 6/01/78 modifiée.
(2) Cf. JTIL n°22, p.2.

Les perspectives

Les BCR doivent être adaptées afin de prendre en compte la structure du groupe auquel elles s'appliquent, les opérations de traitement que les filiales effectuent et les politiques et procédures qu'elles mettent en oeuvre pour protéger les données à caractère personnel.

(3) Document WP 153.
(4) Document WP 154.

Chloé Torres
Isabelle Pottier

Impact sectoriel

La Cnil modifie l'autorisation unique 005 encadrant le « crédit scoring »

L'assouplissement des contraintes formelles

- En matière d'octroi de crédit, les établissements bancaires évaluent le **risque de défaillance** des emprunteurs à l'aide de **modèles statistiques** établis par catégories d'emprunteur et de crédit.
- Cette technique, dite du « crédit scoring », implique le **traitement automatisé des données** à caractère personnel de l'emprunteur, des membres de son foyer et de ses garants. Le crédit sera ainsi octroyé à un demandeur lorsque le risque statistique de défaillance qui lui est attaché sera jugé satisfaisant.
- Dans la mesure où il s'agit d'un traitement susceptible « *d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire* », l'établissement de crédit concerné devra, conformément à l'article 25 de la loi Informatique et libertés, déposer une **demande d'autorisation** auprès de la Cnil.
- S'il satisfait aux conditions requises des traitements initiés pour l'analyse du risque encouru, l'établissement bancaire devra souscrire un simple **engagement de conformité** à l'autorisation unique. Dans le cas contraire, le dépôt d'une demande d'autorisation exposant les seules caractéristiques du traitement non conformes à l'autorisation unique 005 est requis.

Les innovations majeures du nouveau dispositif

- L'**autorisation unique**, modifiée le 9 juillet 2008, prohibe toute mention afférente au sexe de l'emprunteur, afin de lutter contre toute discrimination. Le **modèle de score** utilisé ne devra pas avoir pour conséquence d'exclure ou de disqualifier une demande sur le fondement d'une variable ne se rapportant pas à la **situation économique et financière** des personnes.
- En cas de refus du crédit, l'établissement doit accorder au demandeur un entretien visant à réexaminer sa demande de manière non automatisée.
- Les personnes concernées (demandeurs du crédit, garants, etc.) devront être informées des traitements constitués à des fins autres que **l'instruction et la gestion de la demande de crédit**.
- Lorsque la conclusion d'un contrat avec un commerçant est conditionnée à l'acceptation du crédit, les données de l'emprunteur ne sont susceptibles d'être utilisées qu'à la seule fin de finaliser le contrat, la **conservation des données** après la mise en place effective du financement **étant exclue**.
- Enfin, lorsque le dossier de demande de crédit est accessible en ligne, l'établissement a pour obligation de créer un **compte informatique provisoire et sécurisé** destiné au traitement de la demande de crédit.

Les enjeux

- Favoriser la lutte contre toute forme de discrimination en restreignant l'inscription à des éléments susceptibles d'une appréciation objective ;

- Maîtriser l'impact de la modélisation et la gestion du risque de crédit sur la rentabilité des établissements financiers.

(1) Autorisation unique n° AU-005 modifiée

L'essentiel

Les variables du modèle de score ne se rapportant pas à la situation économique et financière des personnes physiques ne doivent pas recevoir une pondération susceptible d'avoir « un effet d'exclusion absolu ou disqualifiant ».

Les FAQ juristendances

Quelles sont les situations susceptibles de générer des transferts internationaux ?

Références

Un transfert de données vers un pays tiers est toute communication, copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, copie ou déplacement de ces données d'un support à un autre, quel que soit le type de ce support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire.

Ainsi des entreprises françaises qui communiquent avec des partenaires, des sociétés filiales ou mères ou qui ont des activités situées hors de l'Union européenne sont des situations dans lesquelles se produiront des transferts internationaux de données à caractère personnel.

De même, la centralisation intra-groupe de la base de données de gestion des commandes et de la comptabilité clients, la centralisation intra-groupe de la base de données de gestion des ressources humaines d'un groupe multinational, la délocalisation de centres d'appel et le transfert le fichier correspondant pour démarchage ou qualification ou le recours à des systèmes internationaux de maintenance informatique constituent autant de situations qui entraîneront des transferts de données à caractère personnel hors des frontières communautaires.

A quelles conditions peut-on effectuer un transfert de données ?

Un responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à l'Union européenne que si cet Etat assure un niveau de protection adéquat ou suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

La loi Informatique et libertés (2) prévoit également la possibilité de transférer des données à caractère personnel vers des Etats n'appartenant pas à l'Union européenne, dans l'un des deux cas suivants :

- la personne à laquelle se rapportent ces données doit avoir consenti expressément à leur transfert ;
- le transfert des données doit être nécessaire à l'une des six conditions suivantes : sauvegarde de la vie de la personne, sauvegarde de l'intérêt public, respect des obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice, consultation d'un registre public destiné à l'information du public et ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime, exécution d'un contrat entre le responsable du traitement et l'intéressé, conclusion ou exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement ou un tiers.

Un Guide « transfert de données vers les pays n'appartenant pas à l'Union européenne » contenant toute l'information indispensable sur les transferts de données hors Union européenne est disponible sur le site de la Cnil (3).

(2) Art. 69 Loi du 6/01/78 modifiée.

(3) Guide pratique transfert d'informations hors Union européenne

Actualité

Sources

Prospection commerciale via bluetooth : la Cnil prend position

- Lors d'une séance plénière, la commission a conclu que la loi Informatique et libertés était applicable aux données techniques traitées dans le cadre du protocole de communication bluetooth (1).
- Elle considère que l'**adresse physique** de l'interface du portable et l'identifiant bluetooth du téléphone sont des **données à caractère personnel**.

(1) Communiqué de presse du 12 novembre 2008.

Lancement du passeport biométrique

- Le ministre de l'Intérieur, Michèle Alliot-Marie, a remis le 31 octobre 2008 le **premier passeport biométrique français** à Chantilly (Oise), première ville équipée du matériel nécessaire à son élaboration (2).
- Le déploiement des machines a connu des difficultés et a pris du retard. L'Etat doit les déployer dans près de **2000 mairies d'ici juin 2009**.

(2) Communiqué du Ministère de l'intérieur du 31 octobre 2008

Rejet du référé-suspension contre le fichier Edvige

- Le Conseil d'Etat a rejeté le 29 octobre 2008, le recours en référé-suspension déposé le 27 octobre par plusieurs associations et syndicats (3).
- Le gouvernement ayant pris la décision de procéder au **retrait du décret** portant création d'un traitement automatisé de données à caractère personnel dénommé « Edvige », le juge des référés du Conseil d'Etat rejette pour **défaut d'urgence** la demande de suspension de l'exécution de ce décret.

(3) CE, référé, 29 octobre 2008, n° 321413, 321705 et 321774.

Lutte contre la récupération de données personnelles sensibles

- Une **proposition de loi** a été déposée à l'Assemblée Nationale le 15 octobre 2008 par M. André Wojciechowski pour lutter contre la récupération de données personnelles sensibles par le biais de l'usurpation d'identité adaptée au **support numérique** (4).
- Le texte n'est **pas encore édité** et a été renvoyé à la commission des lois constitutionnelles, de la législation et de l'administration générale de la république.

(4) Doc. Ass. nat. n° 1172.

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