ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 45 – Mai – Juin 2012

PRIVACY BY DESIGN

La protection des données personnelles dès la conception

Les enjeux

▪ Le concept de « Privacy by Design » (PbD) consiste à concevoir des produits et des services en prenant en compte **dès leur conception** les aspects liés à la protection de la vie privée et des données à caractère personnel (1).

▪ Il implique également le respect de ces valeurs **tout au long du cycle de vie de la technologie** concernée.

▪ Ce concept est une tendance très marquée, principalement dans les groupes internationaux et est amené à se développer de plus en plus chez les éditeurs.

Management du risque Informatique et libertés

▪ La pratique du Privacy by Design permet aux entreprises de s'assurer de la conformité des traitements qui seront mis en œuvre à la réglementation Informatique et libertés et constitue un outil de management du risque juridique.

▪ Elle constitue également un nouvel **outil de différenciation** face à la concurrence et un gage supplémentaire de qualité et de confiance pour les clients.

(1) Cf mon blog tendance

Un outil de management du risque juridique

Les conseils

▪ Le **potentiel intrusif** de certaines nouvelles technologies exige que la vie privée et la protection des données à caractère personnel soient prises en compte et protégées dès le départ, c'est-à-dire dès la conception de la nouvelle technologie et tout au long de son cycle de vie.

▪ Cette tendance est appelée à se généraliser, dans la mesure où elle correspond à l'esprit du **projet de règlement européen** visant à réformer la directive n° 95/46/CE relative à la protection des données à caractère personnel.

Etablir une méthodologie d''analyse des projets selon l'approche Privacy by Design.

▪ La Commission européenne prévoit ainsi de rendre obligatoire l'approche « protection des données personnelles dès la conception » et propose l'adoption du Privacy by Design pour tous les produits, services et systèmes exploitant ce type de données.

▪ La prise en en compte de la vie privée dès la conception des technologies d'information et de communication nécessite, dans un premier temps, l'élaboration d'une **méthodologie** permettant de l'intégrer concrètement dans les projets technologiques.

▪ Elle implique dans un deuxième temps, d'**analyser les traitements envisagés**.

▪ Cela permettra enfin, de déterminer très précisément dans le cahier des charges, au regard de la réglementation applicable, les **caractéristiques de l'application** afin que celles-ci soient en adéquation avec les modalités du traitement : durée de conservation, type de donnée pouvant être collectées, respect des principes de pertinence et d'adéquation (traitement des seules données nécessaires à chaque finalité spécifique), protection des tiers à l'égard des finalités du traitement, etc.

CHLOE TORRES

COMMENT ASSURER L'EGALITE DES CHANCES DANS LE CADRE DE LA LOI INFORMATIQUE ET LIBERTES ?

Mesurer la diversité sans discriminer

Les enjeux

▪ Il est difficile pour les entreprises de promouvoir l'égalité des chances alors que le recueil de données des salariés fait l'objet d'une surveillance étroite voir interdite pour certaines données.

▪ Les entreprises étaient partagées entre respecter strictement la loi Informatique et libertés et mener des politiques de diversité les exposant à des sanctions de la part de la Cnil.

▪ Pour mettre fin à ce dilemme, la Cnil et le défenseur des droits ont publié le « **guide méthodologique à l'usage des acteurs de l'emploi** ».

▪ L'objectif de ce guide est de permettre que la collecte des données à caractère personnel des employés serve **à mesurer la diversité, sans discriminer.**

▪ Ce guide vient encadrer sous la forme de fiches, les pratiques des responsables d'entreprise en matière de lutte contre les discriminations en lien avec les obligations issues de la loi Informatique et libertés.

▪ Il vient préciser **les conditions préalables à la mise en œuvre des traitements relatifs à la mesure des discriminations** notamment l'information des personnes concernées, le recueil du consentement des salariés pour la collecte de données sensibles, les mesures de confidentialité et de sécurité, ainsi que l'anonymisation.

Renforcer la collecte des données à caractère personnel pour mesurer la diversité dans l'entreprise, sans créer de discrimination.

(1) Guide "Mesurer pour progresser vers l'égalité des chances"
(2) Cnil, actualité du 11 mai 2012.

Les recommandations de la Cnil

Les conseils

▪ La recommandation essentielle du guide concerne **le recueil du consentement des salariés pour la collecte de données sensibles**.

▪ La collecte de ces données à l'initiative de l'entreprise est légale dés lors que la personne concernée a donné **son consentement exprès**. Elle soulève cependant certaines difficultés pratiques et surtout juridiques.

▪ En effet, la relation de travail suppose un lien de subordination. Comment dans ces conditions peut-on recueillir le **consentement libre et éclairé** du salarié ?

▪ Le guide apporte une réponse en recommandant de recourir à un **prestataire extérieur de l'entreprise** pour conduire l'enquête. Cette démarche permet d'apporter les garanties nécessaires : le consentement du salarié est donné dans des conditions qui garantissent sa liberté de ne pas répondre et la confidentialité de ses choix.

▪ En outre, l'entreprise devra s'assurer que les personnes concernées et les instances représentatives du personnel ont bien été informées. Il sera également nécessaire d'assurer **la confidentialité des données et leur sécurité**.

▪ Lors de la publication, les résultats de l'enquête doivent être produits sous une forme statistique agrégée de façon à **garantir l'anonymat des répondants**.

▪ Il est également conseillé d'associer les représentants du personnel lors de la diffusion des résultats.

Il est important pour les entreprises qui souhaitent mesurer la diversité de :

- recourir à un prestataire extérieur (garantie d'un consentement libre) ;

- assurer la confidentialité ;

- assurer les mesures de sécurité ;

- garantir l'anonymat ;

- informer les personnes concernées.

POINT SUR L'OBLIGATION DE NOTIFICATION DES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL

Quand y a-t-il violation de données à caractère personnel ?

Références

On entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques (1).

Une violation est constituée lorsqu'il y a destruction, perte, altération, divulgation ou accès non autorisé à des données à caractère personnel.

(1) Article 34 bis, I, de la loi du 6 janvier 1978.

Comment la notification à la Cnil doit-elle être faite?

Le décret du 30 mars 2012 précise les modalités pratiques des notifications à la Cnil et aux personnes concernées des violations de sécurité visées par la loi Informatique et libertés (2).

La notification à la Cnil doit être faite sans délai par lettre remise contre signature et doit contenir les éléments suivants :

- la nature et les conséquences de la violation ;
- les mesures déjà prises ou proposées pour remédier à la violation ;
- les personnes auprès desquelles des informations supplémentaires peuvent être obtenues ;
- lorsque cela est possible, l'estimation du nombre de personnes susceptibles d'être concernées.

(2) Décret n° 2012-436 du 30-3-2012 art. 25 et s.

Qu'entend-t-on par mesures de protection appropriées?

Les mesures de protection appropriées peuvent être toutes mesures techniques efficaces destinées à rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

La Commission nationale de l'informatique et des libertés vérifie dans un délai de deux mois si les mesures de protection appropriées ont été mises en œuvre et appliquées et apprécie la gravité au cas particulier de la violation de données à caractère personne (3).

(3) Décret n° 2012-436 du 30-3-2012, art. 26.

Outre l'obligation de notification, quelles sont les autres obligations du fournisseur ?

Le fournisseur doit également tenir à jour un inventaire des violations mentionnant ce qui s'est passé exactement, les conséquences des violations, et les mesures prises pour y remédier (4).

Cet inventaire peut être réalisé sous format papier ou numérique et doit être tenu à la disposition de la Cnil.

L'implémentation, par les fournisseurs de services de communications électroniques accessibles au public, d'une stratégie interne relative à la possibilité d'informer la Cnil de la mise en œuvre de mesures de protection afin bénéficier de l'exception de notification, semble donc à envisager.

(4) Article 34 bis, III, de la loi du 6 janvier 1978.

MAROC : période de grâce pour effectuer les formalités préalables

La loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel a introduit une obligation pour les responsables de traitement d'effectuer des formalités préalables auprès de la Commission Nationale de la Protection des Données Personnelles (CNDP).

Toutefois, une période de grâce est prévue : en effet, pour les traitements de données à caractère personnel mis en œuvre avant le 5 mars 2009, date d'entrée en vigueur de la loi, les responsables de traitement disposent d'un délai de 2 ans pour se mettre en conformité.

Bien que le point de départ de ce délai de deux ans ne soit pas très clairement identifié, il est recommandé de retenir comme date butoir le 31 août 2012, soit 2 ans après la date d'installation de la CNDP.

CHINE : les fournisseurs de services Internet désormais soumis à une règlementation sur la protection des données

Depuis le 15 mars 2012, les fournisseurs de services Internet doivent se conformer à un règlement sur la protection des données à caractère personnel.

Ce règlement contient les principes fondamentaux à respecter pour le traitement des données : bonne foi, limitation de la collecte à ce qui est nécessaire, information des utilisateurs des services, limitation du traitement à la finalité pour laquelle les données sont collectées, obligation générale de sécurité et notification des failles de sécurité aux autorités.

En revanche, aucune disposition ne figure dans le règlement quant aux droits des personnes concernées.

AFRIQUE DU SUD : le projet de loi sur la protection des données bientôt adopté

Le projet de loi sur la protection des données, dont la cinquième version est actuellement en discussion devant le Parlement, devrait être adopté cette année. Les notions de traitement et de donnée à caractère personnel sont définies largement.

Le traitement de certaines catégories spécifiques de données (telles que religion, opinions philosophiques, etc.) est par principe interdit, sous réserve d'exceptions prévues par le texte. En particulier, une exception spécifique concerne le traitement de données relatives à la race, afin de ne pas compromettre l'application des lois anti-discrimination.

Huit principes régissent les traitements de données à caractère personnel : responsabilité, finalité, restriction du traitement, restriction des traitements ultérieurs, qualité des données, transparence, sécurité, participation des personnes concernées. Par ailleurs, l'autorité de protection est investie de pouvoirs importants et des sanctions pénales sont également prévues.

Prochains événements

L'I-marque ou comment assurer la protection de l'image de marque sur Internet : 13 juin 2012

▪ **Virginie Brunot**, **Anne-Sophie Cantreau** animeront aux côtés de **Christophe Gérard** de la société Melbourne IT un petit déjeuner sur la protection de l'image de marque sur Internet.

▪ Le développement de nouvelles pratiques marketing, du référencement sur Internet à la publicité sur les réseaux sociaux en passant par les nouvelles extensions de noms de domaine et les nouvelles règles de nommage des noms de domaine, constitue un levier de croissance des marques et accroît leur visibilité.

▪ Ce même phénomène engendre corrélativement de nouveaux types d'atteinte aux mêmes marques.

▪ Face à la diversification des atteintes : quels réflexes adopter pour protéger et défendre ses marques au regard de l'évolution jurisprudentielle ? Quels processus internes mettre en place ? Quelles procédures judiciaires ou extra-judiciaires envisager ?

▪ Le petit déjeuner sera l'occasion de partager l'expérience de la société Melbourne IT sur les nouvelles procédures instaurées dans le cadre des nouvelles extensions de noms de domaine.

▪ Nous aborderons également les dernières évolutions jurisprudentielles sur la protection des marques inspirées de la jurisprudence de la Cour de justice en matière de référencement sur Internet, ainsi que les modifications apportées aux règles de nommage et aux procédures extra-judiciaires en matière de noms de domaine.

▪ **Inscription gratuite** sous réserve de confirmation avant le 11 juin 2012 par courrier électronique en indiquant vos coordonnées et le nombre de personnes qui assisteront au petit déjeuner débat à l'adresse suivante : invitation-conference@alain-bensoussan.com ou en faxant le bulletin d'inscription en ligne au 01 41 33 35 36.

L'hébergement des données de santé : 12 septembre 2012

▪ **Marguerite Brac de la Perrière** animera un petit déjeuner consacré au cadre juridique de l'hébergement de données de santé à caractère personnel.

▪ Préalable indispensable au développement de l'e-santé en France, l'hébergement de données de santé à caractère personnel ne peut être réalisé qu'en conformité avec les dispositions du décret n°2006-6 du 4 janvier 2006 et après obtention d'un agrément délivré, pour une durée de trois ans, par le ministre chargé de la santé après avis motivé d'un comité d'agrément et de la Cnil.

▪ A l'heure où la Cnil a annoncé son ambition de multiplier les contrôles auprès des hébergeurs de données de santé, un point sur la réglementation, les bonnes pratiques et les relations contractuelles propres à l'activité d'hébergement s'imposent.

▪ **Inscription gratuite** sous réserve de confirmation avant le 10 septembre 2012 par courrier électronique en indiquant vos coordonnées et le nombre de personnes qui assisteront au petit déjeuner débat à l'adresse suivante : invitation-conference@alain-bensoussan.com ou en faxant le bulletin d'inscription en ligne au 01 41 33 35 36.

Petit-déjeuner Lexing : 28 septembre 2012

▪ Après le succès de l'événement qui s'est tenue à Paris le 20 janvier 2012, les membres du réseau Lexing se réuniront de nouveau, cette fois à Barcelone, pour discuter de questions d'actualité sur les nouvelles technologies.

▪ L'événement aura lieu à Barcelone, le vendredi 28 septembre, 2012 de 9h à 11h et sera ouvert à tous les clients du réseau.

▪ Les modalités d'inscription seront diffusées très prochainement sur notre site.

Expertise technique sur la sécurité des cartes bancaires sans contact

Sources

▪ La Cnil a annoncé mener des investigations techniques sur les éventuels problèmes de sécurités présentés par les cartes bancaires sans contact (1).
▪ En effet, d'après la Cnil « des tests auraient démontrés que ces cartes seraient susceptibles de communiquer sur plusieurs mètres des informations relatives à leur porteur ou aux transactions effectuées par celui-ci».

(1) Cnil, actualité du 10-5-2012

Adoption de l'autorisation unique n°AU-029

▪ La Cnil a adopté l'autorisation unique relative aux traitements de données à caractère personnel contenues dans des informations publiques aux fins de communication et de publication par les services d'archives publiques (2).
▪ Les traitements pouvant faire l'objet d'un engagement de conformité à l'autorisation unique sont uniquement ceux mis en œuvre par les conseils municipaux, les conseils généraux, le ministère de la culture, le ministère des affaires étrangères et le ministère de la défense.

(2) Délibération n°2012-113 du 12-4-2012

Dispense de déclaration n°16

▪ La Cnil a adopté le 29 mars 2012 une dispense de déclaration pour les traitements automatisés de données personnelles mis en œuvre aux fins de consultation de données issues de la matrice cadastrale par toute commune, groupement et organisme privé ou public chargé d'une mission de service public ainsi que la diffusion sur internet de base géographique de référence au sens du Code de l'environnement (3).
▪ La nouvelle dispense ajoute à la liste des traitements pouvant faire l'objet de la dispense de formalité ceux dont la finalité est de « diffuser sur internet des bases de données géographiques de référence, locale ou nationale, au sens du Code de l'environnement ».

(3) Délibération n°2012-088 du 29 mars 2012

Cette dispense abroge la dispense de déclaration n°04-074 du 21 septembre 2012.

Traitement d'antécédents judiciaires

▪ Un traitement de données à caractère personnel relatif aux « antécédents judiciaires » vient d'être créé par décret le 4 mai 2012 pour remplacer deux fichiers existants : le système de traitement des infractions constatées (STIC) de la police nationale et le système judiciaire de documentation et d'exploitation de la gendarmerie nationale (JUDEX) (4).
▪ Ce traitement mutualise les deux fichiers d'antécédents judiciaires existants de la police et de la gendarmerie nationale.

(4) Délibération n°2012-652 du 4-5-2012.

La JTIL est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 29, rue du colonel Pierre Avia 75015 Paris, président : Alain Bensoussan

Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier.

Diffusée uniquement par voie électronique – gratuit – ©Alain Bensoussan 2012

ISSN 1634-0698

Abonnement à partir du site : http://www.alain-bensoussan.com/outils/abonnement-juristendance