LEXING ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 53-sept.-oct. 2013

LA CNIL MET EN ŒUVRE LE REGLEMENT « NOTIFICATION OF PERSONNAL DATA BREACHES »

La notification des violations de données à caractère personnel

▪ Un **règlement européen du 24 juin 2013** concernant les mesures relatives à la notification des violations de données à caractère personnel est entré en vigueur le 25 août dernier (1).

▪ En droit français, le **défaut de notification** par les fournisseurs de communications électroniques est puni de 5 ans d'emprisonnement et de **300 000 € d'amende** par l'article 226-17-1 du Code pénal et constitue un manquement à la loi Informatique et libertés (2).

▪ Le règlement précise les **modalités de notification** des violations intervenues sur les traitements de fourniture de communications électroniques aux abonnés, particuliers et autorités compétentes de protection des données.

▪ Il contient deux annexes qui répertorient les **informations devant être communiquées** par les fournisseurs de communications électroniques aux autorités compétentes ainsi qu'aux abonnés et particuliers.

▪ Il met par ailleurs à la charge des autorités compétentes (Cnil) l'obligation d'**adopter une procédure** visant à :

- mettre à disposition de tous les fournisseurs des états membres un moyen électronique sécurisé de notification des violations ;
- informer les fournisseurs des procédures d'accès et d'utilisation à ce moyen ;
- informer les autres autorités compétentes que des abonnés ou particuliers de leur pays sont concernés par la violation.

La téléprocédure mise en œuvre par la Cnil

▪ Conformément aux dispositions du règlement, la Cnil a lancé, le 23 août 2013, sa **procédure en ligne** de notification des violations de données à caractère personnel.

▪ Tout fournisseur de communications électroniques doit utiliser cette procédure de notification **dans les 24 heures de la constatation** d'une violation de données personnelles.

▪ Pour ce faire, un **formulaire est téléchargeable** sur le site internet de la Cnil qui peut être renvoyé par voie électronique ou postale.

▪ La Cnil met également à disposition des fournisseurs un **outil d'estimation du degré de gravité** de la violation. Ils doivent ainsi noter de 1 à 4 le **caractère identifiant** des données et le **caractère préjudiciable** pour les personnes concernées.

▪ Selon le résultat obtenu, **une note est attribuée à la violation** qui sera considérée comme négligeable (résultat < à 5), limitée (résultat = 5), importante (résultat =6) ou maximale (résultat > à 6).

Les enjeux

Les fournisseurs de communication électronique doivent réaliser une notification conforme à la procédure mise en place pour ne pas risquer de sanctions financières et pénales.

(1) Règlement européen 611/2013 du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel.

(2) Loi 78-17 du 6 janvier 1978, art. 34 bis.

Les conseils

- Réaliser en amont une analyse des risques techniques et juridiques.

- Etablir une procédure interne de gestion des notifications de violations de données personnelles.

- Sensibiliser, informer et former le personnel concerné.

POLYANNA BIGLE
CAROLINE MACE

OPERATION INTERNET SWEEP DAY : LA CNIL DRESSE LE BILAN DES AUDITS

Journée de balayage de l'internet

▪ La Cnil a commenté cet été les résultats de l'**audit** effectué en mai dernier de **250 sites internet** régulièrement fréquentés par les internautes français portant sur l'information délivrée aux internautes (1).

▪ Cet audit a été réalisé dans le cadre de l'« Internet Sweep Day », en français, la « **Journée de balayage de l'internet** », première opération internationale d'audit coordonnée des autorités membres du Global Privacy Enforcement Network (GPEN) (2).

▪ Pour rappel, le GPEN a été créé en 2007 en vue de renforcer la protection de la vie privée dans un contexte mondial.

▪ Au total, près de **19 autorités compétentes** en matière de protection des données personnelles ont évalué **2180 sites Internet** ou applications les plus visités.

▪ Les résultats de cette enquête montrent l'**insuffisance**, voire parfois l'absence, d'une **information claire** des internautes sur les conditions de traitement de leurs données personnelles.

Un constat pas entièrement négatif

▪ Au niveau mondial, il a été constaté que **plus de 20 % des sites Internet** et applications mobiles **audités** (50 % pour les seules applications mobiles) ne délivrent **aucune information à leurs visiteurs** relative à la politique de protection des données personnelles.

▪ En outre, les **mentions d'informations** délivrées par les autres sites sont apparues **incomplètes**, peu accessibles et peu compréhensibles.

▪ Du point de vue national, il a été constaté que **moins de 10% des sites web** audités ne fournissaient pas d'information sur leur politique de protection des données.

▪ Pour autant, lorsque qu'elle est fournie, cette information n'est ni facilement accessible (pour près de la moitié des sites et applications mobiles concernés), ni suffisamment claire et compréhensible (pour près d'un tiers des sites audités).

▪ Le constat de la Cnil n'est toutefois pas entièrement négatif.

▪ En effet, de **bonnes pratiques** ont pu être constatées sur certains sites, notamment :

- l'existence de questions/réponses (FAQ),
- l'organisation thématique de l'information,
- l'indication de points de contacts en charge de répondre spécifiquement aux interrogations relatives à la protection des données personnelles.

Les enjeux

Apprécier le niveau d'information des internautes en vue de renforcer la protection de leur vie privée.

(1) Cnil, actualité du 13-8-2013.

(2) Global Privacy Enforcement Network (GPEN).

Les conseils

Les constats effectués par la Cnil doivent encourager les éditeurs de sites internet et d'applications mobiles à s'assurer du niveau de conformité de leur politique d'information concernant la protection des données.

CELINE AVIGNON
RAOUF SAADA

Partenariat entre la Cnil et les Archives de France

Sources

▪ La Cnil et le service interministériel des Archives de France ont signé une convention de partenariat le **10 septembre 2013** sur la collaboration en matière de détermination des **durées de conservation des données** à caractère personnel avant la mise en œuvre du sort final (1).

▪ La coopération prévoit diverses **actions mutuelles** visant à bien articuler l'application croisée des obligations liées d'une part à la loi n°78-17 du 6 janvier 1978 et au Code du patrimoine.

(1) Cnil, actualité du 16-9-2013.

Vidéosurveillance : mise en demeure pour surveillance excessive des salariés

▪ Le **12 juillet 2013**, une mise en demeure à l'encontre d'une entreprise a été **rendue publique** au regard du nombre de manquements et du **caractère particulièrement intrusif** du dispositif de vidéosurveillance installé dans les locaux de l'entreprise (2).

▪ La Cnil a jugé que ce dispositif était **disproportionné** au regard des principes Informatique et Libertés du fait de son **ampleur** et dans la mesure où il filme les accès aux toilettes, aux vestiaires, au cabinet médical et aux salles de pause des salariés.

▪ Ce dispositif permettait également de placer des salariés sous **surveillance permanente** alors qu'ils se situent à leur poste de travail. La Cnil a également constaté que contrairement à ce qui lui avait été indiqué, ce dispositif était utilisé pour **contrôler les horaires** des salariés puisque certaines séquences vidéo extraites du dispositif concernent des salariés au moment de leurs pointages.

(2) Cnil, actualité du 12-9-2013.

Un projet de règlement européen pour l'identification électronique

▪ La Commission européenne a rendu public cet été un projet de règlement créant un cadre européen pour l'identification électronique (3).

▪ Son objectif est de **promouvoir la confiance dans les transactions électroniques**, et ainsi d'encourager la dématérialisation des transactions dans le marché intérieur, vecteur de développement économique.

▪ La législation de l'UE existant en la matière, à savoir la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques, ne couvre que les signatures électroniques. L'UE ne dispose encore d'**aucun cadre transnational** et intersectoriel complet pour des transactions électroniques sûres, fiables et aisées, qui recouvre l'identification, l'authentification et les signatures électroniques.

(3) Document de base législatif 2012/0146(COD) - 04/06/2012.

La JTIL est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 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-petit-dejeuner-juristendance

POINT SUR LES VIOLATIONS DE SECURITE (PERSONNAL DATA BREACHES)

Qu'est-ce qu'une violation de données à caractère personnel ?

▪ Une violation de données personnelles est définie comme « *des violations de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans l'Union* » (1).

▪ Cette définition a été introduite en droit français lors de la transposition la directive « Paquet Telecom » à l'article 34 bis de la loi Informatique et libertés (2).

Qui doit notifier les violations de données personnelles ?

▪ Seuls les **fournisseurs** de services de **communications électroniques** accessibles au public sont débiteurs de cette obligation.

▪ Le **projet de règlement européen** relatif à la protection des données à caractère personnel **prévoit d'étendre l'obligation** de notification à tous les responsables de traitement (3).

Comment notifier une violation de données personnelles ?

▪ Il convient de remplir le **formulaire en ligne** et de le renvoyer à la Cnil dans les 24 heures, celle-ci peut être complétée par tout document de nature à l'informer des mesures adoptées.

▪ Si dans le délai de 24 heures, le fournisseur ne dispose pas de tous les éléments d'information, il doit procéder à une seconde notification 3 jours après la première (4).

Quelles recommandations ?

▪ Effectuer une analyse précise des risques techniques et juridiques.

▪ Adopter des mesures techniques et organisationnelles pour prévenir, détecter et empêcher les violations de données.

▪ Préparer une documentation spécifique à communiquer à la Cnil à l'appui du formulaire de notification.

▪ Anticiper la publication du règlement européen relatif à la protection des données personnelles qui en l'état du projet met à la charge de tout responsable de traitement une obligation de notification des violations de données personnelles.

▪ Sensibiliser, informer et former le personnel en charge d'intervenir techniquement et juridiquement dans le cadre d'une procédure de notification d'une violation de données à caractère personnel.

Références

(1) Directive européenne n°2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

(2) Loi 78-17 du 6 janvier 1978 modifiée.

(3) Projet de règlement 2011/0011 COD du 25 janvier 2012 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(4) www.cnil.fr, Rubrique « Vos obligations »

Prochains événements

Nouveaux noms de domaine, nouvel internet ? Bilan et perspectives : 9 octobre 2013

▪ **Anne-Sophie Cantreau**, **Virginie Brunot** et **Isabel Toutaud**, Directrice Juridique et Politiques de Registre de l'Afnic animeront un petit déjeuner sur le programme mondial d'élargissement du système des noms de domaine prévu par l'ICANN et qui va se concrétiser à partir du 2ème semestre 2013.

▪ Les noms de domaine rencontrent aujourd'hui de nombreux bouleversements, dus à l'arrivée de très nombreux generic Top Level Domains dans les semaines et mois à venir, cumulée à la mise en place de nouvelles procédures extra-judiciaires de suspension, de radiation et de récupération des noms de domaine portant atteinte aux droits de marque.

▪ L'Afnic, régulateur français du nommage sur Internet, y consacre son 11ème dossier thématique intitulé « Nouvelles extensions Internet : un nouveau Big Bang pour les noms de domaine ».

▪ Dans ce contexte, tout acquéreur (entreprise, collectivité, communauté, etc.) doit revisiter sa politique de gestion et de défense des noms de domaine et des marques.

▪ Ce petit-déjeuner sera l'occasion d'examiner les questions suivantes :

- quelles réflexions mener pour adapter sa politique de gestion de ses noms de domaine ?

- dans quels cas inscrire ses marques dans la Trademark Clearing House ?

- quelles procédures mettre en place pour défendre mes marques et noms de domaine face aux noms de domaine de tiers les reproduisant ou les imitant ?

- quelles sont les évolutions jurisprudentielles récentes (Afnic, tribunaux et centres d'arbitrage) ?

▪ **Inscription gratuite** sous réserve de confirmation avant le 7 octobre 2013 à l'aide du formulaire en ligne.

Les nouvelles mesures fiscales en matière d'innovation : 13 novembre 2013

▪ **Pierre-Yves Fagot** animera un petit déjeuner sur les nouvelles mesures fiscales en matière d'innovation.

▪ La France a engagé, depuis déjà quelques années, une politique volontariste destinée à offrir, aux entreprises qui innovent, un environnement fiscal et réglementaire favorable.

▪ A cet égard, le Gouvernement actuel, qui a fait de la compétitivité l'une des priorités de sa politique, s'est attaché à développer cet environnement favorable à l'innovation.

▪ Cette politique a conduit à renforcer, récemment, les mesures d'aide à l'innovation en faveur des entreprises, ainsi qu'à leur création et leur développement en leur offrant, notamment, de nouveaux dispositifs fiscaux pour leur permettre de répondre à un marché toujours plus concurrentiel.

▪ A l'occasion de ce petit-déjeuner, nous vous proposons de faire le point sur l'état des nouvelles mesures adoptées par le Gouvernement en matière d'innovation et notamment :

- les aménagements apportés au crédit d'impôt recherche ;

- le crédit d'impôt innovation ;

- le crédit d'impôt pour la compétitivité des entreprises ;

- la création de la Banque Publique d'Investissement (BPI).

▪ Il sera également l'occasion d'évoquer l'avis et le rapport du Conseil National du Numérique sur la fiscalité du numérique remis à Bercy, le 10 Septembre 2013.

▪ **Inscription gratuite** sous réserve de confirmation avant le 8 novembre 2013 à l'aide du formulaire en ligne.

Formations intra-entreprise : 2e semestre 2013

Le cabinet a la qualité d'organisme de formation professionnelle depuis 30 ans[1].

Il a en outre obtenu le label Cnil « Lexing® formation informatique et libertés » pour son catalogue de formations informatique et libertés.

Informatique et libertés

▪ **Informatique et libertés (niveau 1)** : Identifier et qualifier les intervenants et les responsabilités, prévenir les risques et cerner les formalités obligatoires.	13-09-2013
▪ **Cil (niveau 1)** : Permettre au Cil de maîtriser les obligations et responsabilités qui lui incombent et de savoir les mettre en œuvre.	27-09-2013
▪ **Informatique et libertés secteur bancaire** : Sensibiliser les opérationnels sur les risques Informatique et libertés liés aux traitements du secteur bancaire.	22-10-2013
▪ **Informatique et libertés collectivités territoriales** : Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés.	18-10-2013
▪ **Sécurité informatique et libertés** : Connaître les exigences issues de la réglementation Informatique et libertés en matière de sécurité des données personnelles et sensibiliser aux risques liés à une faille de sécurité.	11-10 et 03-12-2013
▪ **Devenir Cil** : Mettre en œuvre une politique de protection des données efficace (accountability, etc.) et résoudre les questions complexes (réseaux sociaux, etc.).	05-07 et 04-10-2013
▪ **Cil (niveau 2 expert)** : Perfectionnement et résolution de questions complexes ; acquisition de méthodologie pour exercer l'activité selon l'approche Privacy by Design.	03-07 et 18-09-2013
▪ **Informatique et libertés gestion des ressources humaines** : Donner aux membres de la direction des ressources humaines les clés pour utiliser les outils et les traitements de données personnelles mis en œuvre en matière de gestion des ressources humaines.	20-09 et 29-11-2013
▪ **Flux transfrontières de données** : Présenter les dispositions qui régissent ces flux et élaborer une stratégie de gestion des flux conformément à la loi.	06-09 et 15-11-2013
▪ **Contrôles de la Cnil** : Connaître l'étendue des pouvoirs de la Cnil et ses moyens de contrôle, apprendre à dialoguer avec la Cnil (notamment par le biais d'un jeu de rôle).	17-09 et 26-11-2013
▪ **Informatique et libertés secteur santé** : Sensibiliser aux risques Informatique et libertés liés aux traitements du secteur santé et assurances et apporter des éléments de benchmark permettant de positionner son niveau de conformité.	25-10 et 13-12-2013
▪ **Formation intra entreprise Informatique et libertés à l'attention du comité exécutif** : Sensibiliser les membres du comité exécutif aux risques Informatique et libertés liés à leur activité.	Selon demande

[1] Catalogue de nos formations 2013 sur : http://www.alain-bensoussan.com/secteurs-dactivites/formation-intra-entreprise

5e édition : Informatique, Télécoms, Internet (actualisée au 10-09-2012)

Informatique, Télécoms, Internet, Editions Francis Lefebvre 5e éd. 2012

▪ Comme pour les quatre premières éditions, l'ouvrage expose toutes les règles juridiques à connaître applicables à l'économie des systèmes d'information et confronte le monde de l'informatique :

- au droit du travail (contrôle des salariés, évaluation professionnelle, etc.) ;

- à la fiscalité (conception et acquisition de logiciels, crédit d'impôt recherche, avantages de l'infogérance, etc.) ;

- aux assurances ;

- au domaine de la santé (carte santé et secret médical, etc.) ;

- à internet et au commerce électronique.

▪ Cette nouvelle édition intègre toutes les nouveautés les plus récentes et notamment :

- les nouveaux contrats d'externalisation (de la virtualisation au cloud computing) ;

- le nouveau CCAG des marchés de l'information et de la communication (TIC) ;

- le nouveau régime de la vidéoprotection issu de la LOPPSI 2 ;

- la E-réputation de l'entreprise (blogs et réseaux sociaux) ;

- la régulation des activités commerciales sur internet ;

- le téléchargement illégal sur internet ;

- l'usurpation d'identité numérique, la régulation des activités commerciales sur internet, etc.

▪ Cette nouvelle édition innove en ajoutant les référentiels normatifs qui font pleinement partie du cadre juridique applicable aux différents systèmes qui traitent l'information : référentiels de système de management de la qualité, de l'environnement et de la sécurité ou d'ingénierie logicielle (CMMI, ISO 20000-1, ITIL, famille ISO 9000, etc.).

▪ Les mises à jour apportées à l'édition 2012 de l'ouvrage Informatique, Télécoms, Internet sont disponibles en ligne.

[2] Nos publications : http://www.alain-bensoussan.com/espace-publication/bibliographie