Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

JURISTENDANCES INFORMATIQUE ET LIBERTES

n° 66 – Nov.– Déc. 2015

LE CORRESPONDANT INFORMATIQUE ET LIBERTES A 10 ANS

La Cnil a rassemblé en octobre dernier les Correspondants Informatique et libertés (CIL) afin de célébrer les 10 années d'existence de la fonction

▪ L'objectif de ce rassemblement était de permettre aux CIL d'échanger sur leurs **expériences**, pratiques, actions et procédures en matière de conformité à la réglementation Informatique et libertés. Le rassemblement avait également pour objet d'**anticiper l'adoption prochaine du règlement européen** et les changements envisagés des missions et moyens du CIL.

▪ En effet, le projet de règlement européen, encore en discussion à ce jour, positionne les CIL au **centre du dispositif de régulation** et prévoit notamment :

- d'alléger les formalités préalables à accomplir par les responsables de traitements ;
- de renforcer les droits des personnes concernées ;
- d'augmenter le montant des sanctions ;
- de mettre en place des outils et des procédures afin de mieux prendre en compte les principes de protection des données.

▪ La Cnil a déjà anticipé ces évolutions des missions et moyens du CIL en créant un **service dédié**. Le service CIL de la Cnil accompagne ainsi les CIL dans l'exercice de leurs missions et les guides dans l'application des dispositions de la réglementation Informatique et libertés grâce à des **outils dédiés**, une permanence téléphonique et des ateliers d'information.

▪ Ce service est mis à la disposition des CIL désignés par plus de **16300 organismes**, dont 53% dans le secteur privé et 47 % dans le secteur public.

Désigner un CIL : le préalable nécessaire à l'obtention du label « Gouvernance Informatique et libertés » de la Cnil

▪ Au-delà de l'organisation Informatique et libertés au sein des organismes et de la conformité à la réglementation Informatique et libertés, la désignation d'un CIL est également une étape préalable à l'**obtention du label CNIL** « Gouvernance Informatique et libertés ».

▪ Ce label a été adopté par la Cnil fin 2014. Il définit des règles et des **bonnes pratiques** afin de permettre aux organismes d'assurer une gestion de leurs données respectueuse des principes Informatique et libertés.

▪ L'obtention de ce label permet de **garantir** aux clients et utilisateurs **un bon niveau de conformité** à la réglementation Informatique et libertés et constitue un indicateur de confiance envers des produits et des procédures.

▪ Désigner un CIL et entamer une démarche d'obtention du label « Gouvernance Informatique et libertés » permet enfin aux organismes d'anticiper l'adoption du futur règlement européen et notamment le principe d'*accountability*.

L'enjeu

Garantie de conformité d'un organisme à la loi Informatique et libertés, le CIL témoigne également de l'engagement d'un organisme en faveur du respect de la vie privée et des droits des personnes dont l'organisme traite les données

Enfin, la désignation d'un CIL est également un facteur de simplification des formalités administratives

Les conseils

Identifier les personnes susceptibles d'être CIL pour votre organisme et les désigner auprès de la Cnil

EMELINE BISSONI
JULIE SCHWARTZ

© ALAIN BENSOUSSAN – 2015

SANCTION FINANCIERE PRONONCEE A L'ENCONTRE D'OPTICAL CENTER

Manquement à la sécurité et la confidentialité des données de ses clients

L'enjeu

L'enjeu principal, tant que le règlement européen n'a pas été adopté, reste l'image. Néanmoins des sanctions financières peuvent être prononcées en fonction de la gravité des manquements.

▪ Suite à une plainte formulée par une cliente d'**Optical Center** auprès de la Cnil le 8 juillet 2014 pour communication par téléphone de son **mot de passe d'accès** à son compte personnel, la Cnil a déclenché plusieurs missions de contrôle sur place conduisant alors à une sanction financière de **50 000 €** pour manquement à la sécurité et à la confidentialité des données de ses clients (1).

▪ Des manquements à la loi Informatique et libertés ont été constatés par la Cnil qui a alors **mis en demeure** la société en décembre 2014 de se conformer aux exigences de la loi Informatique et libertés et en particulier de :

- mettre en œuvre une durée de conservation des données ;
- informer les personnes concernées des traitements de données opérées ;
- assurer la sécurité et la confidentialité des données collectées par elle et gérées par ses prestataires et notamment chiffrer le canal de communication, établir une authentification du site distant lors de l'accès au site web, améliorer la robustesse des mots de passe de ses clients et salariés, verrouiller automatiquement les postes des salariés en cas d'inactivité prolongée;
- insérer une clause relative à la sécurité et à la confidentialité des données dans le contrat conclu avec son prestataire
- répercuter l'ensemble de ces mesures dans ses différents magasins.

▪ Suite à une **mise en conformité partielle** d'Optical Center, une seconde mission de contrôle a alors été menée par la Cnil en février 2015 qui a été suivie, après une audition devant la Cnil, par la rédaction d'un rapport détaillant les non-conformités.

Les manquements constatés notamment en matière de sécurité et de confidentialité

▪ Si la Cnil soulève la question de la mise en œuvre d'une **durée de conservation** des données en rappelant que les durées de conservation indiquées dans les normes simplifiées n°48 (2) et n°54 (3), doivent être mises en œuvre, cette dernière ne retient pas la caractérisation du manquement.

▪ Les manquements caractérisés sont relatifs à la **sécurité** et la **confidentialité** des données collectées par elle et gérées par ses prestataires.

▪ En effet, les articles 34 et 35 de la loi Informatique et libertés imposent au responsable du traitement de prendre **toutes précautions utiles** afin de protéger les données des clients et à son sous-traitant de présenter des garanties suffisantes.

▪ Si la société avait effectué certaines modifications, la Cnil relève que tel n'était pas le cas le jour de l'expiration du délai de mise en conformité.

▪ La Cnil rappelle que la **sécurité** à mettre en œuvre est à la fois **logique**, par la mise en œuvre de mots de passe robustes par exemple, mais également **physique**, notamment par le verrouillage des postes de travail des salariés.

▪ Enfin la Cnil constate que le **contrat** entre la société et son **sous-traitant** ne comporte pas de **clause relative à la sécurité** et à la **confidentialité** des données, à savoir une clause précisant les obligations du sous-traitant et que ce dernier ne peut agir que sur instruction du responsable du traitement.

▪ La sanction financière prononcée par la Cnil est peu courante et s'explique par le nombre de personnes concernées et la **sensibilité des données**.

(1) Délib. Cnil 2015-379 du 5-11-2015.

(2) Délib Cnil du 21-06-2012.

(3) Délib Cnil du 21-12-2006.

Les conseils

Il est recommandé :

- d'effectuer régulièrement des audits relatifs aux mesures de sécurité mises en œuvre par les sous-traitants afin de se conformer aux exigences de la réglementation Informatique et libertés ;

- de s'assurer que les contrats conclus avec les prestataires comportent bien une clause relative à la sécurité et à la confidentialité des données.

ORIANE ZUBCEVIC

© ALAIN BENSOUSSAN – 2015

LA DESIGNATION D'UN CORRESPONDANT INFORMATIQUE & LIBERTES

Pourquoi désigner un Cil ?

Depuis la parution du décret d'application de la loi Informatique et libertés en 2005, la fonction de Correspondant Informatique et libertés (Cil) est en plein essor et il est devenu un acteur incontournable de la protection des données à caractère personnel.

Tous les organismes, responsables de traitement, peuvent désigner un Cil, qu'ils soient publics ou privés, qu'il s'agisse de petites entreprise ou de grands Groupe, les avantages sont nombreux et cette désignation permet notamment :

- de réduire les risques juridiques de manquement à la loi Informatique et libertés,
- à un allègement des formalités,
- de bénéficier d'une relation privilégiée avec la Cnil (services dédiés, ateliers d'information, extranet dédié),
- d'améliorer l'image de marque de l'organisme,
- d'améliorer la politique de sécurité informatique de l'organisme,
- de réduire les coûts de traitement des informations.

Référence

(1) Cnil, Guide du correspondant informatique et libertés (CIL).

Comment désigner un Cil ?

Le Cil peut être une personne physique ou morale, employé ou non de l'organisme. La fonction de Cil peut également être mutualisée entre différents organismes dès que ceux-ci sont liés par des intérêts économiques communs ou appartiennent à un même secteur d'activité.

Les modalités de désignation du Cil sont les suivantes :

- information des représentants du personnel et des salariés,
- notification de la désignation à la Cnil ; la désignation du Cil prendra effet un mois après la date de réception de la notification par la Cnil.

Quelles sont les principales missions du Cil ?

- Tenir la liste des traitements et assurer son accessibilité.
- Veiller au respect de la loi en diffusant une culture Informatique et libertés au sein de l'organisme et en proposant des formations.
- Elaboration d'une politique de protection des données à caractère personnel.
- Rendre compte de son action à travers un bilan annuel.

CONSTANCE FAGOT – DE MAGNEVAL

© ALAIN BENSOUSSAN – 2015

Prochain petit-déjeuner

Tendances Numériques 2015-2016 : 9 décembre 2015

▪ Éric Barbry et Isabelle Galy, Directrice déléguée aux opérations du Learning Lab « Human Change » au Cnam.

▪ Un tour d'horizon 360° des tendances numériques pour réussir sa transition numérique :

- Qu'est-ce que Uber, AirBnB et Blablacar vont changer au droit ?
- Pourquoi les lois Hamon, Lemaire et Macron sont-elles parfois contradictoires ?
- Comment nos juges s'adaptent-ils à ces changements ?

▪ Le petit-déjeuner « Tendances numériques » est l'un des temps forts du Cabinet pendant lequel nous vous proposons de faire avec nous le point des transformations et des résistances juridiques induites par l'impact des technologies numériques.

▪ Éric Barbry fera un bilan complet des évolutions législatives, contractuelles ou jurisprudentielles et en présence de notre grand témoin Isabelle Galy, Directrice déléguée aux opérations du Learning Lab « Human Change » au Cnam, nous aborderons les nouvelles problématiques juridiques posées par un droit qui doit encore s'adapter aux plateformes, aux systèmes intelligents et devenir agile.

▪ **Lieu :** de 9h30 à 11h30 (accueil à partir de 9h00) dans nos locaux, 58 bd Gouvion-Saint-Cyr, 75017 Paris.

▪ **Inscription gratuite** (sous réserve des places disponibles).

▪ L'enregistrement en ligne est obligatoire pour y assister : formulaire en ligne.

Catalogue de formation inter et intra-entreprise 2016

▪ Le Cabinet a la qualité d'organisme de formation professionnelle depuis 30 ans. Il propose une **quarantaine de formations** dans chacun des domaines figurant au catalogue.

▪ Ces formations sont assurées par les avocats du cabinet et s'appuient sur de nombreux outils pédagogiques, tels que des cas pratiques personnalisés, des quizz de validation, des FAQ, ou encore des fiches réflexes.

▪ Le cabinet a obtenu le label Cnil « **Lexing® formation informatique et libertés** » pour la plupart des formations informatique et libertés figurant au catalogue (JO du 27 juin 2012).

▪ Catalogue 2016 :

- version feuilletable en ligne
- liste des formations par fiches.

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 2014

ISSN 1634-0698

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

© ALAIN BENSOUSSAN – 2015

NOTRE RESEAU DE CORRESPONDANTS ORGANIQUES LEXING VOUS INFORME

Projet de loi sur la protection de l'information d'Etat en Afrique du Sud

▪ Le **projet de loi** sur la protection de l'information traite de la classification et la protection des informations d'Etat, **POSI** (*Protection of sensitive state information*) (1).

▪ Il vise à assurer la protection des informations « **sensibles** » de l'Etat contre l'altération, la destruction, la perte ou la divulgation illégale et prévoit un système de **classification**, **reclassement** et **déclassification** des informations d'état. Il réglemente la manière dont ce type d'informations peut être protégé.

▪ En préambule, il reconnait que le **droit d'accès à toute information détenue par l'État** peut être limité lorsque cela est nécessaire pour des raisons de sécurité nationale.

▪ Mais il souhaite placer la protection des informations d'Etat dans un cadre législatif **transparent** et **durable** visant à promouvoir la libre circulation des informations au sein d'une société ouverte et démocratique, sans compromettre la sécurité nationale de la République.

▪ Il abrogera le Protection Information Act de 1982 (Loi n ° 84 de 1982).

▪ Le projet de loi POSI porte expressément sur la **sécurité nationale** et ne doit pas être confondue avec le POPI (*Protection of Personal Information Act*), qui est la loi de protection des données à caractère personnel de l'Afrique du Sud.

▪ Le projet POSI est lié à la loi Cybercriminalité et la Cybersécurité **CaC** (*Cybercrimes and Cybersecurity Bill*) publié le 28 août 2015, en ce qu'il traite également de la sécurité nationale.

▪ D'un côté, il y a le POSI et le CaC et de l'autre, le DPAI (*Promotion of Access to Information Act*) et le POPI, tous deux destinés à s'équilibrer l'un l'autre.

(1) Actualité du 27-11-2015, par John Giles.

Lexing Afrique du Sud

REPUBLIC OF SOUTH AFRICA

PROTECTION OF STATE INFORMATION BILL

(As presented by Ad Hoc Committee on Protection of Information Bill (National Assembly))
(introduced as Protection of Information Bill [B 6—2010])
(The English text is the official text of the Bill))

(MINISTER OF STATE SECURITY)

© ALAIN BENSOUSSAN – 2015

Loi applicable au responsable de traitement de données à caractère personnel

▪ La Cour de justice de l'Union européenne avait été saisie d'une **question préjudicielle** par la Cour Suprême hongroise relative à la loi applicable en matière de données à caractère personnel. Dans un arrêt rendu le 1er octobre 2015 (1), la Cour précise les critères permettant de déterminer si un responsable de traitement dispose d'un établissement sur le territoire d'un Etat membre, critère pouvant être retenu pour **déterminer la loi applicable**.

▪ La Cour retient, dans cet arrêt, une définition large de la notion d'« **établissement** ». Ainsi, elle indique que la législation d'un Etat membre sur la protection des données à caractère personnel peut être appliquée à une société étrangère dès lors que celle-ci exerce dans l'Etat membre une **activité réelle et effective**, même minime, au moyen d'une **installation stable**.

▪ A défaut de remplir ces critères, le responsable de traitement ne sera pas soumis à la loi de l'Etat membre dans lequel il exerce son activité.

▪ En revanche, l'autorité nationale de l'Etat membre dans lequel l'activité est exercée pourra tout de même être saisie, même si le droit applicable au traitement est celui d'un autre Etat membre. La Cour souligne toutefois que cette autorité nationale ne pourra pas exercer les pouvoirs de sanction qu'elle détient de son droit national.

(1) CJUE, A-10-2015, Affaire C-230/14 du 1-10-2015.

Clôture de la mise en demeure de la société Boulanger

▪ Le 26 juin 2015, la société Boulanger avait été mise en demeure par la Présidente de la Cnil de se conformer à la loi Informatique et libertés suite à un contrôle sur place qui avait révélé que les fichiers de la société comportaient de nombreux **commentaires excessifs** (2).

▪ La société Boulanger s'est depuis conformée à la réglementation Informatique et libertés en mettant notamment en place un système de détection automatique des commentaires excessifs et un modérateur ainsi qu'une formation de ses salariés. La Présidente de la Cnil a en conséquence procédé à la clôture de la décision de mise en demeure.

(2) Communiqué Cnil du 9-9-2015.

Adoption d'une nouvelle autorisation unique dans le secteur bancaire

▪ La Cnil a adopté l'**autorisation unique (AU-045)** pour les traitements de données à caractère personnel aux fins de consultation du répertoire national d'identification des personnes physiques (RNIPP) mis en œuvre par les établissements du secteur bancaire et financier soumis aux obligations relatives aux comptes bancaires inactifs et des coffres inactifs ou par une personne mandatée à cet effet (3).

▪ La finalité des traitements mis en œuvre sera d'assurer l'identification des **titulaires de comptes et coffres inactifs décédés**.

▪ De tels traitements pourront être mis en œuvre par les établissements de crédit et de paiement, les établissements de monnaie électronique, les prestataires de services d'investissement ou de services connexes ou encore les personnes mandatées.

(3) Délib. Cnil 2015-229 du 9-07-2015

JULIE SCHWARTZ
OLIVIANNE JUES

© ALAIN BENSOUSSAN – 2015