

La désignation du correspondant à la protection désormais possible

Le décret du 20 octobre 2005

▸ Le **décret d'application**, très attendu par la Commission Nationale de l'Informatique et des Libertés (CNIL) a été adopté le **20 octobre 2005**⁽¹⁾. Il permet la mise en application du correspondant à la protection des données à caractère personnel (CIL).

▸ Les entreprises qui souhaitent s'affranchir des formalités déclaratives vont ainsi pouvoir nommer un **CIL « interne »** ou « externe ». De nouvelles **opportunités** s'offrent ainsi aux entreprises pour se **positionner** sur le terrain de la **qualité « Informatique et libertés »**.

▸ Le décret achève ainsi la mise en place d'un dispositif global introduit par le législateur en août 2004⁽²⁾ en précisant d'une part, l'**organisation de la CNIL** et d'autre part, en fixant le **cadre définitif des formalités** préalables obligatoires (délais, dématérialisation des procédures...) pour les entreprises et organismes ainsi que les **pouvoirs de la CNIL**.

Un correspondant « interne » ou « externe » ?

▸ La loi Informatique et libertés permet aux entreprises ou organismes d'être **exemptés des formalités** les plus courantes devant la CNIL en contrepartie de la **désignation d'un correspondant** chargé d'assurer l'application de la loi et la tenue d'une liste des traitements existants.

▸ La loi ne précise pas le caractère « interne » ou « externe » de la fonction de CIL, ce qui n'exclut pas la possibilité pour les entreprises de désigner un correspondant autre qu'un salarié de l'entreprise.

▸ **Selon le décret** du 20 octobre 2005, le CIL **peut être externe** uniquement lorsque **50 personnes** sont chargées de la mise en œuvre ou ont directement accès aux traitements ou catégories de traitements.

▸ La **nomination peut être optimisée** dans le cadre de sociétés soumises à un même contrôle (ex : un GIE ou encore des organismes professionnels au sein d'un même secteur d'activité).

▸ L'avantage pour les entreprises qui désignent un CIL est de bénéficier d'un **allègement des formalités déclaratives** pour les traitements les plus courants. C'est aussi l'occasion pour les entreprises d'**e-mailing**, de se **positionner sur le terrain de la qualité**.

L'essentiel

Le décret précise en particulier :

- le cadre définitif des formalités préalables obligatoires
- l'articulation des rôles entre la CNIL et le procureur de la République
- la coopération avec les autorités de contrôle homologues de la CNIL
- les sanctions administratives ou financières
- les recours en cas de contrôles sur place, de vérification, d'audition
- les modalités d'application du CIL.

(1) Décret n°2005-1309, JO du 22 octobre 2005.

(2) Loi n°2004-801 du 06/08/2004, cf. «*Informatique, Télécoms, internet*», Ed. Fr. Lefebvre 2004.

Alain Bensoussan
alain-bensoussan@alain-bensoussan.com

Laurent Caron
laurent-caron@alain-bensoussan.com

Impact sectoriel

Les modalités d'archivage électronique dans le secteur privé

L'archivage électronique des données à caractère personnel

▸ La CNIL expose dans une **recommandation du 11 octobre 2005** les limites Informatique et liberté à prendre en compte en matière d'archivage électronique des données à caractère personnel ⁽¹⁾.

▸ Par archivage électronique de données à caractère personnel, la CNIL entend les **pratiques de conservation** des données visées à l'article 2 de la loi du 6 janvier 1978 modifiée, que celles-ci soient **collectées, reçues, établies** ou **transformées** sous forme électronique, par toute personne, service ou organisme privé dans l'exercice de son activité.

▸ La CNIL éclaire par ailleurs, la notion complexe de « **droit à l'oubli** » qui nécessite de déterminer des **durées limitées** et appropriées de conservation. Elle identifie **trois niveaux d'archives** : courantes, intermédiaires ou définitives et en déduit les **préconisations** à mettre en œuvre dans chacun des cas.

▸ Cette recommandation complète la recommandation du 10 mai 1988 dédiée aux administrations et organismes du **secteur public**.

Mettre en œuvre un plan d'archivage approprié

▸ La CNIL souhaite anticiper les **risques de diffusion**, d'accès, d'utilisation illicite ou d'accès non autorisé ou injustifié.

▸ Les entreprises doivent par conséquent s'appuyer sur les textes réglementaires fondateurs des traitements mis en œuvre pour **déterminer des durées appropriées**.

▸ Le **responsable du traitement** doit mettre en œuvre les mesures techniques et d'organisation appropriées pour **protéger les données** archivées contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

▸ Le non-respect de l'**obligation** de sécurité est sanctionné par l'article 226-17 du **Code pénal**.

▸ Les mesures de conformité ne peuvent être déterminées qu'au cas par cas dans le cadre d'un **plan d'archivage adapté**.

L'enjeu

Prendre en compte les limites Informatique et liberté en matière d'archivage électronique des données à caractère personnel.

(1) Délibération n° 2005-213, disponible sur le site de la Cnil.

Les conseils

- Mettre en œuvre les mesures techniques et d'organisation propre à assurer la sécurité

- Identifier les niveaux d'archives courantes, intermédiaires ou définitives

- Déterminer des durées limitées appropriées à chaque type d'archive

Les FAQ juristendances

Sources

Un refus d'autorisation de la CNIL est-il susceptible de recours ?

▸ **Oui**, les traitements soumis à **autorisation préalable** et qui ne peuvent être mis en œuvre du fait d'une prise de décision défavorable par la Cnil peuvent faire l'objet d'un **recours devant le Conseil d'Etat**.

▸ Ce dernier a déjà considéré qu'un **avis défavorable** de la Cnil faisant grief constituait une décision susceptible de recours (1).

(1) CE 5 juin 1987, n° 59674.

Le correspondant à la protection des données peut-il être sanctionné par l'employeur ?

▸ **Non**, il ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions (2).

▸ En revanche, en cas de **manquement** constaté à ses devoirs, il peut être **révoqué**, sur demande ou **après consultation de la Cnil** et le responsable du traitement sera alors enjoint de procéder lui-même à la déclaration prévue à l'article 23.

(2) Loi n°78-17 de la loi du 6 janvier 1978 modifiée, art. 22.

Le correspondant à la protection des données peut-il être externe ?

▸ **Oui**, le correspondant à la protection des données à caractère personnel (CIL) peut être externe mais uniquement lorsque **50 personnes** sont chargées de la mise en œuvre ou ont directement accès aux traitements ou catégories de traitements (3).

(3) Décret n°2005-1309 du 20 octobre 2005.

▸ La **nomination** du CIL peut par ailleurs **être optimisée** dans le cadre de sociétés soumises à un même contrôle (ex : un GIE ou encore des organismes professionnels au sein d'un même secteur d'activité).

Peut-on s'opposer à une action de la Cnil ?

▸ **Non**, aucun responsable de traitement, même ministre, ne peut s'opposer à son action. Il doit au contraire prendre toutes mesures utiles afin de faciliter sa tâche (4).

▸ Le **délit d'entrave** à l'action de la Cnil est passible d'un an d'emprisonnement et de **15 000 euros** d'amende (art. 51).

(4) Loi n°78-17 de la loi du 6 janvier 1978 modifiée, art. 21.

Actualité

Sources

Externalisation du recrutement du correspondant à la protection

▸ Le **décret d'application du 20 octobre 2005** achève la mise en place d'un dispositif global introduit par la loi du 6 août 2004 modifiant la loi Informatique et libertés. Outre des dispositions ayant trait au fonctionnement et à l'organisation de la Cnil, il comporte des mesures qui présentent un impact direct sur l'application de la loi par les entreprises et organismes publics.

▸ Il instaure un **seuil** à l'intérieur duquel une entreprise ou un organisme peut uniquement désigner un **correspondant interne** (50 personnes chargées de la mise en oeuvre ou ayant directement accès aux traitements concernés) et au-delà, la possibilité d'**optimiser la désignation d'un correspondant externe** dans le cadre de groupes de sociétés, d'un GIE ou d'organismes professionnels ou regroupant des responsables de traitements ⁽¹⁾.

(1) Décret n°2005-1309 du 20 octobre 2005, *JO* du 22/10/2005.

Un guide des formalités de désignation du CIL

▸ Après la sortie du décret définissant les dispositions applicables au correspondant à la protection des données à caractère personnel (CIL) du 20 octobre 2005, la CNIL publie un **guide de procédure** dédié au CIL ⁽²⁾.

▸ Ce guide formalise la **liste des missions** qui lui incombent et dresse la liste des **compétences** et **qualifications** nécessaires à cette nouvelle fonction. La désignation d'un CIL se fait à l'aide du **formulaire annexé** au guide et qui permet de recueillir toutes les informations nécessaires.

(2) Disponible sur le site de la Cnil, <http://www.cnil.fr/>

La position de la CNIL sur les systèmes d'alerte et de dénonciation

▸ Les entreprises doivent prendre en compte la position de la CNIL concernant les dispositifs d'alerte professionnelle (« **whistleblowing** »), dans l'éventualité de la mise en oeuvre de tels dispositifs ⁽³⁾.

▸ La CNIL admet la possibilité d'une dénonciation anonyme mais exige l'intervention de **spécialistes**. Elle rappelle que de tels dispositifs sont soumis à son **autorisation préalable**, laquelle a été refusée en mai 2005, à la société McDonald's France et à la Compagnie européenne d'accumulateurs ⁽⁴⁾.

(3) Cnil, Echos des séances 15/11/2005 <http://www.cnil.fr/>

(4) Délib. n°2005- 110 et n°2005- 111.

Directeur de la publication : Bensoussan Alain
Rédigée et animée par Laurent Caron et Isabelle Pottier
Diffusée uniquement par voie électronique
ISSN (en cours)
Abonnement à : avocats@alain-bensoussan.com