avocats
Data Protection Officers

L'ENGAGEMENT POUR LA PROTECTION DES DONNÉES & DE LA VIE PRIVÉE

Où en êtes-vous de votre conformité ?

Le CIL a vocation à intervenir à la fois comme conseil en sécurité informatique et juridique, formateur, auditeur et médiateur des questions Informatique et Libertés.

LES MISSIONS DU CIL DANS VOTRE ENTREPRISE

- PILOTER la mise en conformité
- SIMPLIFIER les formalités administratives
- RENFORCER la sécurité informatique
- CONSEILLER sur la bonne pratique en matière d'utilisation de données personnelles
- PROTÉGER et VALORISER le patrimoine informationnel
- AFFIRMER un engagement éthique et citoyen
- PRÉSERVER la e-réputation de l'entreprise

avocats

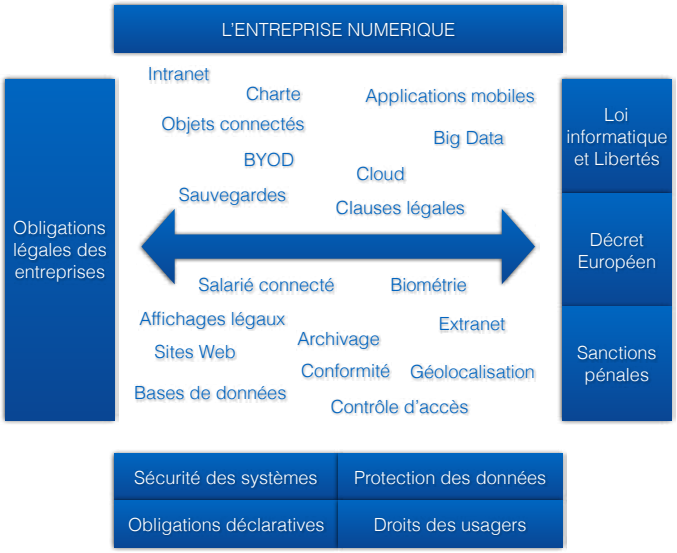
Pour répondre aux besoins de conformité juridique et technique de ses adhérents, la FESP et le SESP proposent de mettre à leur disposition, par la désignation d'un CIL mutualisé, un dispositif spécifique légal d'allègement de leurs formalités, leur permettant à la fois de se conformer à la bonne application de la loi et de les dispenser de la plupart des formalités règlementaires et administratives prévues par les textes.

Introduit en août 2004 à l'occasion de la refonte de la Loi Informatique et Libertés, la désignation par un organisme (entreprise, société, association, fédération, etc.) d'un correspondant à la protection des données (DPO ou CIL) constitue un moyen efficace de veiller à la bonne application de la loi et d'assurer le respect du droit fondamental à la protection des données personnelles, tout en se protégeant de sanctions éventuelles.

Les entreprises de service à la personne gèrent au quotidien des données à caractère personnel, souvent sensibles. Elles interviennent quotidiennement au domicile des bénéficiaires, parfois auprès de publics fragiles (enfants, personnes âgées, personnes dépendantes) et sont amenées à traiter quotidiennement des données classées par la Loi comme sensibles (données de santé des enfants ou des personnes dépendantes, casiers judiciaires des intervenants, etc.) ainsi que d'autres données confidentielles (codes d'accès au domicile, codes des alarmes, etc.).

Depuis quelques années, le débat sur la protection des données à caractère personnel prend de l'ampleur et préempte de plus en plus le débat public.

Le développement croissant des outils, des services et des moyens informatiques utilisés par les entreprises dans le cadre de leurs activités, conduit à un accroissement des traitements de données à caractère personnel.



Ne pas se conformer à la Loi Informatique et Libertés présente des risques réels et sérieux pour les entreprises et notamment :

- Risque pénal avec peines de prison (jusqu'à 5 ans) et d'amendes (jusqu'à 1,5 million d'euros) ;
- Risque civil avec dommages et intérêts et restriction ou interdiction d'usage du ou des fichiers concernés ;
- Risque de sanction administrative par la CNIL avec amendes (jusqu'à 3 millions d'euros), arrêt du traitement concerné, etc. ;
- Risque social (actions prud'homales, IRP, etc.) ;
- Risque commercial avec la publicité de la sanction de la CNIL sur le site Internet de l'entreprise.

LES TEXTES APPLICABLES

La Loi Informatique et Libertés et ses différents décrets d'application, disposent que tout fichier ou traitement de données à caractère personnel doit s'opérer dans un cadre réglementaire strict et faire l'objet des formalités requises auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL). Chaque déclaration qui doit être faite à la CNIL comporte également l'engagement que le traitement satisfait aux exigences de la loi (Loi 78-17 du 6 janvier 1978 modifiée).

Le Règlement Européen entrera en vigueur en mai 2018, alourdissant les obligations à la charge des entreprises et augmentant notamment les droits des usagers, en plus de la réglementation existante, déjà contraignante. (Règlement adopté le 14 avril 2016 et publié au JO de l'Union Européenne le 27 avril 2016)

Ce règlement européen s'adapte aux nouvelles réalités du numérique. Dans un objectif de protection des droits des personnes et de leurs données personnelles, face à l'ampleur exponentielle du phénomène « Big Data », les autorités nationales et européennes s'organisent pour sauvegarder les libertés publiques et individuelles.

Trois objectifs sont définis dans le cadre du renforcement des obligations de protections des données :

- Renforcer les droits des personnes ;
- Responsabiliser les entreprises traitant des données à caractère personnel ;
- Renforcer la régulation grâce à une coopération renforcée entre les autorités de protection des données (contrôles et sanctions).

Les principales évolutions opérationnelles sont, par exemple :

- La réduction de deux à un mois du délai de traitement des demandes relevant des droits d'accès aux données personnelles ;
- L'obligation de documenter et déclarer les cas de violation de données, ou de piratage (vol, virus, etc.) ;

Entraînant ainsi la nécessité d'organiser :

- La communication des notifications de violation de données aux Commissions Nationales et à tous les intéressés ;
- La réalisation d'études d'impacts préliminaires ;
- La tenue de documentations attestant de la conformité des processus et de leur suivi qualitatif ;
- Le renforcement des dispositions de sécurité informatique.

QUI EST CONCERNÉ ?

Toutes les structures exploitant des données, ont l'obligation de respecter les règles de protection des données personnelles.

Sont également concernées les structures exploitant ces données à partir des objets connectés, ou ayant l'ambition de préempter ce marché.

Les TPE-PME sont les moins préparées et aguerries à ces domaines très techniques et présentent des disparités importantes. Toutes ou presque se retrouvent dans l'une des trois situations suivantes :

- aucune déclaration, aucun traitement conforme, aucune protection, aucune sauvegarde ;
- une pluralité de sous-traitants qui, trop souvent, organisent une opacité technique et technologique qui empêche visibilité du système, maîtrise des coûts et coordination de la chaîne de valeur ;
- un début d'exécution mais inabouti donc inefficient : une simple déclaration à la CNIL, un CIL nommé parmi le Back-Office livré à lui-même et trop souvent sans réelle latitude d'action, des procédures de sauvegarde des données mises en place sans coordination interne, etc.

Les coûts induits de cette méconnaissance sont pourtant importants pour les entreprises.

LE RÔLE DU CIL DANS VOTRE ENTREPRISE

Assure la conformité de vos obligations légales

Garantir votre sécurité juridique	Accès privilégié aux services de la CNIL	Dispense de la plupart des déclarations à la CNIL
Assure le suivi des droits d'accès, de modification de suppression et de portabilité des données	Conseille les décideurs et les opérationnels sur les pratiques réglementaires en matière de données personnelles	Tient à la disposition des tiers et de la CNIL le registre légal des traitements de l'entreprise

Renforce la sécurité de votre organisme

Garantir la sécurité informatique Organise, pilote et suit dans le temps la mise en conformité	Informe le personnel interne, les sous-traitants, partenaires, clients, salariés, intervenants, familles	Valorisation du patrimoine informationnel
		Audits réglementaires Veille juridique, informatique et technique

Valorise votre image aux yeux des tiers

Engagement éthique et citoyen de l'entreprise Préserve votre réputation

La plupart des PME ne sont pas en conformité avec la Loi. Elles ont, de plus, un délai très court pour se conformer à la nouvelle règlementation.

avocats

Data Protection Officers

Plus d'infos : www.republique-numerique.fr

GDPR
EU General Data Protection Regulation

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Plus d'infos : www.cnil.fr

Conception : L. Corchia

Un service proposé par :

Syndicat des entreprises de services à la personne

Fédération du SERVICE AUX PARTICULIERS

Dézavelle-Livowsky & Associés
DPO-AVOCATS
11, rue Théodule Ribot
75017 PARIS

Téléphone : +331 4227 7349
Contact : cil@dezavelle.com