Association Data Protection Officers

**MME. HÉLÈNE LEGRAS**
**Vice présidente de l'ADPO**

Data Protection Officer Orano depuis le 25 mai 2017, veillant à la conformité informatique et libertés. Formations internes. Interventions dans des séminaires/conférences. Groupes de travail. Rédactions d'articles pour revues (Ex : **Cahiers de droit de l'entreprise n° 6**, Novembre 2013 –Lexis/Nexis – dossier sur le CIL avec Chloé Torrès - Directrice Cabinet Bensoussan ; **Archimag N° 304** de mai 2017 « du correspondant informatique et libertés au délégué à la protection des données » ; **IT for business : entretien pour le N° 2218 de juin 2017** « démarrez au plus tôt votre projet de conformité au RGPD » ; **Revue pratique de la prospective et de l'innovation - LexisNexis – N° 4 d'octobre 2017** « Data Protection Officer et mise en conformité selon le RGPD »)

## DE LA LIL AU RGPD ET DU CIL AU DPO

La loi 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978 est le pilier légal français de la protection des données nominatives, devenues données à caractère personnel avec la loi 2004-801 du 6 août 2004. Les données à caractère personnel sont celles qui permettent d'identifier directement ou indirectement une personne. C'est le nom d'une personne, mais c'est aussi son adresse postale ou électronique, c'est le matricule d'un salarié, son numéro de sécurité sociale ou son adresse Internet Protocol, ce qu'a confirmé la Cour de Cassation dans son arrêt du 3 novembre 2016. La donnée à caractère personnel peut aussi être qualifiée de sensible et sa collecte et son traitement par les entreprises seront alors interdits. Ce sont celles qui font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou enfin celles relatives à la santé ou à la vie sexuelle. La loi informatique et libertés continue de s'appliquer en France malgré l'adoption du Règlement Général sur la Protection des Données (RGPD) 2016-679 du 27 avril 2016 . Elle est même en cours de révision et le nouveau texte devrait être adopté en mai 2018. Le RGPD concerne les données à caractère personnel définies dans son article 4 et interdit avec son article 9 la collecte des données dites sensibles. La loi de 1978 ne donnait pas de définition de la donnée de santé. Le RGPD indique que c'est la donnée révélant des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée.

La loi de 1978 s'applique en France. Le RGPD est européen et même mondial puisqu'il concerne les données personnelles traitées sur le territoire européen et/ou de citoyens européens. Ainsi une filiale américaine qui traitera des données de salariés français devra respecter le RGPD. Il faut aussi noter que ce règlement destiné à l'origine à harmoniser et uniformiser les législations européennes cohabite avec ces dernières du fait de leurs particularités.

### NOTE

*(1) Arrêt n° 1184 du 3 novembre 2016 (15-22.595) - Cour de cassation - Première chambre civile - ECLI:FR:CCASS:2016:C101184.*

*(2) Règlement no 2016/679, dit Règlement Général sur la Protection des Données (RGPD).*

Ainsi la loi française pour une république numérique appelée « loi Lemaire » et adoptée le 7 octobre 2016 permet aux personnes concernées de donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès.. Elle oblige aussi chaque responsable de traitement à informer la personne dont les données sont collectées sur la durée de conservation desdites données. Si cela se révèle impossible, il devra indiquer les critères utilisés permettant de déterminer cette durée.

De même la BDSG allemande oblige à recueillir l'accord du Word Council, équivalent du «Comité d'Entreprise» français devenu «Comité Social et Economique» en 2018 , pour les données Ressources Humaines.

Le RGPD représente un enjeu fort pour les entreprises car le système déclaratif précédent disparaît au profit d'une conformité que les entreprises devront être en mesure de prouver. Ce défi est d'autant plus important que les sanctions pécuniaires associées ont été fortement augmentées. Selon la nature de la non-conformité elles pourront être de 10 ou 20 millions d'euros ou 2 % voire 4 % du chiffre d'affaires mondial. Mais la sanction la plus importante sera celle pour l'image de marque de l'entreprise, qui sera altérée par la publication de la sanction financière.

Les entreprises avaient pu nommer des Correspondants Informatique et Libertés facultatifs grâce à la loi de 2004 et son décret d'application de 2005 . Au lieu de déclarer leurs traitements automatisés de données à caractère personnel à la Commission Nationale de l'Informatique et des Libertés, les entreprises les déclaraient à leur CIL nommé, qui tenait un registre.

Le RGPD institue le Data Protection Officer/ Délégué à la Protection des Données, qui remplacera le CIL le 25 mai 2018. Le DPO n'aura pas le même profil que le CIL. Il devra piloter, coordonner, contrôler, organiser la conformité de son organisme. Obligatoire dans les organismes publics, ceux traitant des données à grande échelle ou traitant des données sensibles, il apparaît comme l'élément essentiel de la conformité. Véritable chef d'orchestre, la CNIL indique qu'il est la première étape de la route de la conformité. Le G29, qui regroupe les CNIL européennes recommande sa nomination.

## NOTE

*(3) Loi pour une République numérique n° 2016-1321 du 7 octobre 2016.*

*(4) Bundesdatenschutzgesetz (Federal Data Protection Act) du 30 octobre 2017.*

*(5) Décret d'application n° 2017-1819 du 29 décembre 2017 organise le Comité Social et Economique (entré en vigueur le 1er janvier 2018).*

*(6) Décret n°2005-1309 du 20 octobre 2005, pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

L'Association Data Protection Officers, recommande aussi de désigner ce communicant qui connaît son organisme, le droit et l'informatique et qui est capable d'animer son réseau interne constitué d'experts de la « Privacy ». Il travaillera aussi bien avec sa Direction des Ressources Humaines, sa Direction de la Communication, sa Direction de l'audit interne, que sa Direction des risques et assurances, sans compter sa Direction des Systèmes d'Information et son Responsable de la Sécurité des Systèmes d'Information.

Effectivement, le RGPD oblige tous les responsables de traitement à notifier leurs violations de données à caractère personnel à l'autorité de contrôle et ce dans un délai de 72 heures à compter de la découverte de la faille. La faille ne sera pas toujours le résultat d'une malveillance externe mais peut être aussi due à une négligence interne. DPO et RSSI seront vigilants, main de la main, surtout qu'il faudra aussi informer les personnes concernées en cas de risque pour leurs droits et libertés.
Le DPO sera associé de manière appropriée et en temps utile à toutes les questions touchant à la protection des données personnelles ; il est soumis au secret professionnel et sera indépendant dans ses fonctions.

Le RGPD indique aussi qu'il ne doit pas avoir de conflit d'intérêts dans l'exercice de ses missions. La CNIL bavaroise, la « Bavarian Data Protection Authority », a condamné le 20 octobre 2016, sur la base de la loi allemande, pour conflit d'intérêt une société ayant nommé DPO son DSI. L'homologue allemande de la CNIL a en effet considéré

qu'il existait un conflit d'intérêt dans le fait pour un DSI d'être également nommé DPO, car cela reviendrait à ce qu'il s'auto-surveille. Cette décision confirme que le DPO ne peut être responsable de traitement. Cela limite les profils de personnes pouvant être nommées DPO. Le pilotage du RGPD est un pilotage juridique et un juriste, un responsable conformité ou un qualiticien me semblent les personnes idoines. Un DPO externe pour les petites structures est aussi une excellente solution financière, permettant d'éviter un éventuel conflit d'intérêt.

Le RGPD va nécessiter pour les entreprises des bouleversements organisationnels internes avec la mise en place de nouvelles procédures, la réforme des contrats avec les sous-traitants qui pourront désormais être co-responsables de la conformité à mettre en place. Il faudra nommer des DPO qui devront avoir les moyens financiers, techniques et humains pour exercer leurs missions.

Le RGPD entré en vigueur le 25 mai 2018 concerne les nouveaux traitements et ceux ayant subis des modifications substantielles. Mais il ne s'agit pas seulement d'être en conformité à cette date, il faudra poursuivre l'exercice tout au long de la vie des traitements. Mon conseil en forme de conclusion : nommez un DPO conducteur de la route de la conformité, qui sauras négocier les virages et mener son entreprise à destination.


*Co-auteur du Data Protection Officer aux éditions Bruylant Larcier (1ère et 2ème éditions)*

**MME. HÉLÈNE LEGRAS**

# Le Guide
## de la vidéoprotection

2019

**DES CONTENUS ESSENTIELS**
études de cas
analyses juridiques
avis d'experts
informations pratiques

**DES PRESTATAIRES RÉFÉRENCÉS**
conseils et formations
constructeurs hardware
éditeurs software
distributeurs
intégrateurs
drône
cloud
contrôle d'accès, protection périmétrique et détection d'intrusion
télésurveilleurs
IoT


www.an2v.org

# SOMMAIRE