Nos collègues du CREAI Grand Est ont publié un article traitant de la protection des données personnelles, que vous trouverez ci-dessous. Nous les remercions d'en faire bénéficier notre réseau.

La protection des données personnelles au regard du règlement européen : de l'obligation préalable à une responsabilisation des acteurs

par **Jessica BOIVIN,**
Directrice-adjointe du CREAI Grand-Est

En France, la protection des données personnelles est opérée par la loi Informatique et Libertés du 6 janvier 1978 et orchestrée par la Commission Nationale Informatique et Libertés (CNIL). Les mécanismes en place actuellement vont se modifier en profondeur avec l'entrée en vigueur du règlement européen en mai prochain. Il va en effet se produire un vrai changement de logique, à l'image de ce que la loi de 2002 a opéré dans le secteur social et médico-social.

Mais pour comprendre ce changement, voici un aperçu du régime de protection des données personnelles tel qu'il existe sous l'empire de la loi de 1978.

Aujourd'hui, la protection des données se réalise par un **contrôle a priori de la part de la CNIL**. Lorsque qu'une institution procède à un traitement[1] de données, elle doit procéder à des formalités préalables : la déclaration (normale ou simplifiée) ou la demande d'autorisation, suivant les données traitées[2]. Pour tenir compte de la réalité du secteur, la CNIL a émis des autorisations uniques permettant aux établissements et services sociaux et médico-sociaux de collecter, conserver et traiter des données dans le cadre de la constitution des dossiers de suivi des personnes accueillies et accompagnées. Un engagement de conformité est alors la seule démarche à opérer.

Pour simplifier et sécuriser la politique de protection des données personnelles en son sein, la structure peut décider de **nommer un Correspondant informatique et libertés (CIL)**, chef d'orchestre et conseil de la direction. Il renseigne un registre des traitements pour toutes les formalités de déclarations normales et simplifiée. La structure bénéficie alors d'une dispense pour ces traitements. Elle restera toutefois soumise à l'obligation de demande d'autorisation pour les traitements de données sensibles.

Le règlement général sur la protection des données[3] entrera en vigueur le 25 mai 2018. Il va opérer un renversement de la logique de protection des données personnelles. Si les droits individuels sont maintenus, voire renforcés, pour chaque individu, **le régime de contrôle a priori va être remplacé par une politique de transparence et de responsabilisation**.

---

[1] Constitue un traitement de données personnelles toute opération portant sur des données personnelles, quel que soit le procédé utilisé, informatique ou traitement papier. Il s'agit ainsi de la collecte, de l'enregistrement, de l'organisation, et de la conservation. Constituer et utiliser un dossier papier pour un usager est un traitement de données relevant de la loi Informatique et libertés.

[2] Une donnée personnelle est une donnée se rapportant à une personne physique, qui peut être identifiée quel que soit le moyen utilisé. Il s'agit de données directement ou indirectement identifiantes (l'identification est issue d'un recoupement d'informations)

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Le règlement européen est d'application directe. La législation nationale n'a pas besoin d'être modifiée pour intégrer ses dispositions. Hormis les options possibles dans le cadre du texte (comme c'est le cas dans le cadre du devenir du régime de l'autorisation pour le traitement des données sensibles), la législation nationale ne peut édicter de dispositions contraires.

Cette harmonisation des régimes juridiques des différents états membres est fondée sur l'idée d'une obligation pour les structures de mettre en place toutes les mesures, techniques et organisationnelles pour assurer une protection optimale des données personnelles. A cela, le Parlement européen complète en ajoutant un **principe de « minimisation »**, les structures devront veiller à limiter la quantité de données collectées à ce qui est strictement nécessaire. Ce principe était déjà présent en France et inscrit dans les autorisations uniques propres aux différents secteurs, et était sous-jacents dans la mise en œuvre des droits individuels.

Concrètement, **les formalités déclaratives obligatoires préalables vont disparaître**. Les structures ne procèderont plus à la déclaration de leurs traitements.

Par conséquent, **les structures devront pouvoir justifier à tout moment de la conformité de leur démarche de protection**. Des outils seront ainsi mobilisés : le registre des traitements, dans lequel figure les caractéristiques et modalités des différents traitements dans la structure, l'adhésion à des codes de conduites, la constitution d'une documentation (à l'image de la bibliothèque de preuves constituée dans le cadre de l'évaluation interne par exemple).

Pour ce qui relève actuellement du régime de l'autorisation, pour les traitements de données dites sensibles (données de santé par exemple), les états membres pourront choisir soit de maintenir le régime de l'autorisation, soit de mettre en place un **mécanisme d'étude d'impacts sur la vie privée (EIVP)**[4]. Le droit européen met en place ainsi une procédure visant à évaluer les risques d'atteinte à la vie privée pour les individus concernés par le traitement des données et à penser les différents mécanismes et réponses à adopter.

La responsabilisation passe également par la **nomination d'un Délégué à la protection des données (DPD)**[5]. Elle est obligatoire dans trois situations (facultative en dehors de ces cas) :

- Pour les structures appartenant au secteur public
- Pour les structures mettant en œuvre des traitements à grande échelle, dans le cadre de leur activité principale et en ayant une utilisation régulière et systématique
- Pour les structures mettant en œuvre des traitements avec des données sensibles (données de santé) ou relatives à des condamnations pénales ou des infractions.

Dans cette hypothèse, le DPD aura ainsi les missions suivantes :

- **L'information et le conseil** de la direction et des professionnels
- **Le contrôle du respect du règlement européen et du droit national** : il tiendra le registre des traitements, il réalisera les EIPV, il s'assurera des différentes mentions légales dans les différents supports …
- **La coopération avec la CNIL et interlocuteur de ses agents** : il facilite l'accès aux documents et aux informations dans le cadre de l'exercice des missions et pouvoir de la CNIL.

[4] A l'heure actuelle, la France n'a pas fait d'option explicite pour l'une ou l'autre des procédures. La CNIL a toutefois déjà mis en ligne des supports d'information et méthodologique pour la réalisation des EIVP.

[5] Le règlement européen parle de DPO pour Data Protection Officier, Délégué à la protection des données en français.

La transparence s'exerce, quant à elle, principalement au regard de l'**obligation de notification des failles de sécurité**. En effet, les structures doivent techniquement assurer la sécurité de leurs systèmes d'information. Sécurité et confidentialité doivent être garanties. Lorsqu'une violation des données personnelles est constatée, la direction doit en informer la CNIL, ainsi que les personnes concernées lorsqu'il apparait un risque élevé pour leurs droits et libertés.

La contrepartie de ce régime de responsabilisation est le pouvoir de sanction de l'autorité de contrôle. La CNIL peut en effet prononcer des sanctions administratives à l'encontre des structures défaillantes :

- Avertissement ;
- Mise en demeure l'entreprise ;
- Limitation temporaire ou définitive du/des traitement(s) ;
- Suspensions des flux de données ;
- Injonction de satisfaire aux demandes d'exercice des droits des personnes ;
- Amendes administratives : pouvant s'élever, selon l'infraction, de 10 à 20 millions d'euros (ou 2 à 4 % du CA annuel (mondial), le montant le plus haut étant retenu)[6]

Pour conclure, la CNIL conseille dès à présent aux organismes de se préparer à l'entrée en vigueur du règlement européen en 6 étapes :

- **Désigner un pilote** : nomination d'un CIL/futur DPD en interne ou en organisant une mutualisation

- **Cartographier les traitements** de données personnelles : recensement de tous les traitements opérés et évaluation de l'impact du règlement européen

- **Prioriser les actions à mener** : identifier les actions à mener pour se conformer au règlement européen et les prioriser au regard des risques pesant sur les droits et libertés des personnes concernées par les traitements.

- **Gérer les risques** : mener les études d'impacts sur la vie privée pour les traitements qui le nécessite

- **Organiser les processus internes** : mise en place des procédures de notification des failles de sécurité, de demande de rectification ou d'accès…

- **Documenter la conformité** : constituer une bibliothèque avec la documentation démontrant la conformité de la structure au droit national et européen.

[6] Aujourd'hui le montant maximum de l'amende administrative est de 150 000 € ou 300 000 € en cas de récidive.