Etude RGPD

Le RGPD : Règlement adopté en avril 2016 par l'Union Européenne renforçant et unifiant les droits des citoyens européens sur l'utilisation de leurs données personnelles, applicable sans transposition dans le droit national à compter du 25/05/2018 dans tous les pays de l'Union Européenne.

Définition des données personnelles : *toute information se rapportant à une personne physique identifiée ou identifiable; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*.

Définition des traitements de données personnelles : *L'article 4 du règlement définit un traitement comme " toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;"*.

6 Axes dans le RGPD :

1. Les données communiquées à une plate-forme peuvent être récupérées par le citoyen et être transmise à une autre plate-forme.
2. Les droits d'accès et de rectification sont plus faciles à exercer et le citoyen bénéficie de plus de lisibilité sur l'utilisation de ses données.
3. La protection des mineurs de moins de 16 ans est renforcée par l'obligation de consentement des parents avant inscription sur un service en ligne.
4. Si un citoyen français rencontre un problème particulier avec le traitement de ses données par une entreprise, il s'adresse à la CNIL et ce même si l'entreprise concernée est implantée à l'étranger.
5. Les sanctions sont augmentées en cas de violation des droits pouvant aller jusqu'à 4% du CA mondial de l'entreprise ou 20 M € pour une entité publique.
6. Le droit à l'oubli est renforcé, un lien sur un moteur de recherches ou des informations personnelles doivent être supprimées si le citoyen estime qu'ils portent atteinte à sa vie privée.

La mise en œuvre de ces axes s'appuie sur une logique de responsabilisation des acteurs traitant des données personnelles.

- Pour les traitements n'induisant pas de risque pour la vie privée des personnes, la déclaration administrative préalable à la CNIL avant la mise en œuvre d'un traitement disparaîtra.
- Pour ceux pour lesquels des risques existent, le régime d'autorisation perdurera ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.
- Pour tous les traitements, l'adoption de mesures techniques et organisationnelles par l'entreprise ou la collectivité devra permettre de s'assurer et de démontrer à tout instant que l'entreprise ou la collectivité offre un niveau optimal de protection des données traitées.
- Si des sous-traitants ont été choisis pour certaines applications (hébergement ou traitement direct de données par exemple), ils devront également participer à la démarche de mise en conformité sous peine de sanctions.

Les collectivités sont extrêmement concernées par le RGPD car elles traitent et détiennent de nombreuses données à caractère personnel liées à leurs fonctions régaliennes ou non : registres d'état-civil, listes électorales, coordonnées des usagers d'un service à fins de facturation, …

La CNIL propose une démarche en 6 étapes :

1. Désigner le délégué à la protection des données (DPD ou DPO)
2. Recenser les traitements de données personnelles
3. Prioriser les actions à mener
4. Gérer les risques
5. Organiser les processus internes
6. Documenter la conformité en continu

ETAPE 1 : Désigner le délégué à la protection des données

- Le 25 mai 2018 au plus tard, la collectivité doit désigner le DPD qui remplace le Correspondant Informatiques et Libertés (CIL).
- Si la collectivité a désigné un CIL, celui-ci a vocation naturelle à devenir le DPD. Les fonctions assumées sont toutefois un peu différentes, le DPD est chargé :
    - D'informer et de conseiller le responsable de traitement, le sous-traitant et les utilisateurs ;
    - De contrôler le respect du RGPD et droit national en matière de protection des données ;
    - De conseiller la collectivité sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
    - De coopérer avec la CNIL et d'être le point de contact de celle-ci.
- Pour cela le DPD doit :
    - Se tenir informé sur le contenu des nouvelles obligations ;
    - Sensibiliser la hiérarchie sur l'impact des nouvelles règles ;
    - Réaliser l'inventaire des traitements des données de la collectivité ;
    - Concevoir des actions de sensibilisation ;
    - Piloter la conformité en continu,
    - Etre désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données ;
    - Etre associé à l'ensemble des questions Informatique et Libertés (en amont de la mise en œuvre d'un traitement par exemple) ;
    - Bénéficier des ressources et formations nécessaires pour mener à bien ses missions.
- De plus, il devra être à l'abri des conflits d'intérêts, rendre compte au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté certaine dans les actions qu'il décidera d'entreprendre.
- Focus sur les conflits d'intérêts : le DPD ne peut occuper des fonctions le conduisant à déterminer les finalités et les moyens d'un traitement (DGS, DGA, Responsable informatique,…) :
    - Les finalités d'un traitement sont souvent réglementaires et ne dépendent alors pas d'un agent de la collectivité ;
    - Par contre, les moyens d'un traitement sont eux, souvent influencés ou même choisis par les agents utilisateurs.
- La CNIL encourage, pour les collectivités qui n'en ont pas, la nomination rapide d'un CIL qui pourra ainsi, suivre les formations adéquates et être naturellement nommé DPD.
- La mutualisation du DPD est encouragée pour les collectivités de petite taille.

- Le DPD n'est pas responsable en cas de non-respect du RGPD. Il ne peut l'être que s'il enfreint intentionnellement les dispositions de la Loi Informatique et Libertés et/ou du RGPD ou s'il aide le responsable du traitement ou le sous-traitant à enfreindre ces dispositions.
- Le DPD doit agir d'une manière indépendante et bénéficier d'une protection suffisante dans l'exercice de ses missions.

ETAPE 2 : RECENSER LES TRAITEMENTS DE DONNEES PERSONNELLES

- La cartographie des traitements de données personnelles est un élément majeur de la mise en conformité et va déterminer les actions à mener.
- La tenue d'un registre est obligatoire, il doit recenser précisément :
    - Les traitements de données personnelles ;
    - Les catégories de données personnelles et leur durée de conservation (si possible) ;
    - Les objectifs poursuivis par les opérations de traitements de données ;
    - Les mesures de sécurité techniques et organisationnelles ;
    - Les acteurs (internes ou externes) qui traitent ces données ;
    - Les flux en indiquant l'origine et la destination des données.
- Un modèle de registre (sous excel) est mis à disposition sur le site de la CNIL.

ETAPE 3 : PRIORISER LES ACTIONS A MENER

- La priorisation des actions à mener peut se faire en fonction des risques pesant sur les libertés des personnes concernées par les traitements de données.
- Les points à étudier systématiquement sont les suivants :
    1. Les données détenues doivent être strictement nécessaires à la finalité des traitements ;
    2. La base juridique du traitement doit être identifiée (consentement de la personne, intérêt légitime, contrat, obligation légale) ;
    3. Les mentions d'information des personnes concernées par le traitement doivent être conformes au RGPD ;
    4. Les sous-traitants doivent connaître leurs obligations, les contrats conclus avec eux doivent inclure des clauses rappelant ces obligations ;
    5. Les personnes concernées doivent pouvoir exercer leur droit d'accès, de rectification, portabilité, retrait du consentement, …) ;
    6. Les mesures de sécurité en place doivent être suffisantes.
- Si des données sensibles sont traitées et/ou si les traitements ont certains objets (surveillance systématique à grande échelle d'une zone accessible au public ; évaluation systématique et approfondie d'aspects personnels devenant la base de décisions juridiques ou affectant de manière significative une personne physique) et/ou si les données sont transférées hors de l'Union Européenne, des mesures particulières doivent s'appliquer en accord avec la loi Informatique et Libertés.

ETAPE 4 : GERER LES RISQUES

- Si des traitements opérés par la collectivité engendrent des risques élevés pour les droits et libertés des personnes concernées, une étude d'impact sur la protection des données doit être menée.
- Cette étude contient :
    - Une description du traitement et de ses finalités ;
    - Une évaluation de la nécessité et de la proportionnalité du traitement ;

- Une appréciation des risques sur les droits et libertés des personnes concernées ;
- Les mesures envisagées pour traiter ces risques et se conformer au règlement.

ETAPE 5 : ORGANISER LES PROCESSUS INTERNES

- Il convient
  - De prendre en compte la protection des données personnelles dès la conception d'une application ou d'un traitement (minimisation de la collecte de données au regard de la finalité, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données, s'assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données).
  - De sensibiliser et d'organiser la remontée d'information (plan de formation des utilisateurs).
  - De traiter les réclamations et demandes des personnes concernées quant à l'exercice de leurs droits (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement).
  - D'anticiper les violations de données et de prévoir dans certains cas, la notification à la CNIL dans les 72 heures et aux personnes concernées dans les meilleurs délais.

ETAPE 6 : DOCUMENTER LA CONFORMITE

- Un dossier devra être établi pour prouver la conformité au RGPD.
- Il comprendra :
  - Les registres des traitements ;
  - Les éventuelles analyses d'impact sur la protection des données ;
  - Les mentions d'informations aux personnes concernées par les traitements ;
  - Les modèles de recueil du consentement ;
  - Les procédures mises en place pour l'exercice des droits des personnes concernées ;
  - Les éventuels contrats avec les sous-traitants ;
  - Les procédures internes en cas de violation de données ;
  - Les preuves que les personnes ont donné leur consentement lorsqu'il est nécessaire.