Les étapes de mise en conformité RGPD

La démarche de mise en conformité au RGPD se déroule en **plusieurs étapes** :

Désignation du Délégué à la Protection des Données

Afin d'orchestrer la mise en conformité au RGPD, il est désormais **obligatoire** de **désigner un Délégué à la Protection des Données (DPD ou DPO en anglais)**.

Il sera le **point d'appui** pour mener à bien les différents points exigés par le RGPD.

Le CDG14, s'étant doté d'un service de Protection des Données, est en capacité d'ouvrir ce service à l'extérieur pour proposer une **solution mutualisée** aux collectivités du Département.

Vous trouverez plus de détails concernant la prestation sur notre document « **Notre Offre de Service RGPD** »

Cartographie

La **première étape** à effectuer dans la démarche de conformité est de **recenser toutes les données personnelles** que l'on trouve et **tous les traitements** s'y rapportant.

Cela permettra d'établir le **registre de traitements**, document **obligatoire**.

Cette étape permet également de **faire le tri** sur les données personnelles en possession de l'entité mais n'étant pas rattachées à un traitement. Elles doivent alors être supprimées ou archivées.

Identifier les risques

À partir du registre de traitements, les **données sensibles** seront **identifiées**.

Une analyse d'impact (**AIPD**) sera à réaliser et des **mesures de sécurité supplémentaires** seront à mettre en place.

Sécurité des données

Il est important de **garantir l'intégrité** de votre patrimoine de **données** en **minimisant les risques** de pertes de données ou de piratage. Les **mesures** à prendre, **informatiques ou physiques**, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas d'incident.

Différentes actions doivent être mises en place :

- Mises à jour de vos antivirus et logiciels
- Changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement de vos données dans certaines situations.

En cas de perte ou vol d'un outil informatique, il sera plus difficile pour un tiers d'y accéder.

Les failles de sécurité ont également des **conséquences** pour ceux qui vous ont confié des données personnelles.

Ayez à l'esprit les conséquences, pour les personnes, de la perte, la divulgation, la modification non souhaitée de leurs données, et prenez les **mesures nécessaires** pour **minimiser ces risques**.

Pour **évaluer le niveau de sécurité** des données personnelles dans votre organisme, voici quelques questions à se poser :

- Les **comptes utilisateurs** internes et externes sont-ils **protégés** par des **mots de passe** d'une complexité suffisante ?
- Les **accès aux locaux** sont-ils **sécurisés** ?
- Des **profils distincts** sont-ils créés selon les **besoins** des utilisateurs pour accéder aux données ?
- Avez-vous mis en place une **procédure de sauvegarde** et de récupération des données en cas d'incident ?

Les Sous-traitants

Les **sous-traitants** et **prestataires** doivent également être **conformes au RGPD**.

Ils doivent prendre en compte l'**objectif de protection des données personnelles** et de la vie privée **dès la conception** de leur service (principe du « **privacy by design** ») ou de leur produit, et ils doivent mettre en place des mesures permettant de **garantir une protection optimale des données**.

Pour déterminer les **obligations respectives** des responsables de traitements et de leurs sous-traitants, il est nécessaire de rédiger un **contrat** prévoyant une **clause spécifique sur la protection des données personnelles.**

Droits des personnes

Il faut s'assurer que les **mentions d'informations** sont bien présentes, de manière **explicite** et **claire**, aux différents niveaux de communication et de collectes des données personnelles tels que les **formulaires d'inscriptions**.

On pourra utiliser une formule du type :

*« * Les informations recueillies par … ont pour **finalité** ……. Elles sont uniquement **destinées** aux agents en charge de leur traitement et ne seront pas cédées ou transmises à des tiers. Conformément à la loi « Informatique et Libertés » de 1978 modifiée et à la réglementation européenne en vigueur, vous disposez du **droit d'accès, de rectification, d'effacement et de limitation des données**. Pour exercer ces droits ou pour toute question, veuillez contacter le **délégué à la protection des données** : ……@…… »*

Archivage

Il faut s'assurer que les **durées de conservation** indiquées dans le registre de traitement soient effectivement **respectées**. Les **procédures** de destructions physique et numérique des données doivent être détaillées et faire l'objet d'un **suivi** régulier.

Les données à caractère personnel **ne doivent pas être conservées** sous une forme permettant **l'identification des personnes** concernées **au-delà de la période nécessaire** au regard des finalités pour lesquelles elles sont traitées.

Il existe des **exceptions** de limitation déterminant des durées plus longues si les données à caractère personnel sont traitées exclusivement :

- À des fins archivistiques dans l'**intérêt public**
- À des fins de **recherche scientifique ou historique**
- À des fins **statistiques**
- Suite à l'adoption des **mesures techniques et organisationnelles appropriées**