Berdugo Metoudi

Le point sur…

Comment se préparer au règlement européen sur la protection des données ?

Le nouveau règlement européen sur la protection des données personnelles entrera en application le 25 mai 2018. L'adoption de ce texte doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique.

Une méthodologie en 6 étapes pour se préparer et anticiper les changements liés à l'entrée en application de ce règlement européen.

Alors que les obligations des organismes au regard de la loi informatique et libertés reposent en grande partie sur les formalités préalables (déclaration, autorisation), le règlement européen sur la protection des données repose sur une logique de responsabilisation (principe « *d'accountability* ») et de transparence.

Ainsi, tout responsable de traitement de données à caractère personnel devront, dorénavant, être en mesure de démontrer leur conformité aux nouvelles dispositions.

ÉTAPE 1 – DÉSIGNER UN RESPONSABLE DES QUESTIONS PERSONNELLES

La mise en œuvre de ces outils implique, au préalable, la désignation d'un « pilote » interne : le délégué à la protection des données, véritable « chef d'orchestre » de la protection des données personnelles au sein de l'organisme.

La désignation d'un délégué est obligatoire en 2018 si :

- Vous êtes un organisme public,
- Vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Même si votre organisme n'est pas formellement dans l'obligation de désigner un PDPD, il est fortement recommandé de désigner une personne disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen.

ÉTAPE 2 – IDENTIFIER L'ENSEMBLE DES TRAITEMENTS DE DONNÉES PERSONNELLES

Dans le cadre du futur règlement, les organismes doivent tenir une documentation interne complète sur leurs traitements de données personnelles et s'assurer que ces traitements respectent bien les nouvelles obligations légales.

Ainsi, vous devez recenser :

- Les différents traitements de données personnelles,
- Les catégories de données personnelles traitées,
- Les objectifs poursuivis par les opérations de traitements de données,
- Les acteurs (internes ou externes) qui traitent ces données. Vous devrez notamment clairement identifier les prestataires sous-traitants afin d'actualiser les clauses de confidentialité,
- Les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.

Pour chaque traitement de données personnelles, posez-vous les questions suivantes :

Qui ?

- Inscrivez dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données,

Le point sur…

Comment se préparer au règlement européen sur la protection des données ?

- Identifiez les responsables des services opérationnels traitant les données au sein de votre organisme,
- Etablissez la liste des sous-traitants.

Quoi ?

- Identifiez les catégories de données traitées,
- Identifiez les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple, les données relatives à la santé ou les infractions).

Pourquoi ?

- Indiquez la ou les finalités pour lesquelles vous collectez ou traitez ces données (exemple : gestion de la relation commerciale, gestion RH…).

Où ?

- Déterminez le lieu où les données sont hébergées,
- Indiquez vers quels pays les données sont éventuellement transférées.

Jusqu'à quand ?

- Indiquez, pour chaque catégorie de données, combien de temps vous les conservez.

Comment ?

- Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées ?

ÉTAPE 3 - HIÉRARCHISER LES ACTIONS À MENER

Identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir.

Points d'attention quels que soient vos traitements :

1. Assurez-vous que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées.
2. Identifiez la base juridique sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale).
3. Révisez vos mentions d'information afin qu'elles soient conformes aux exigences du règlement.
4. Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
5. Prévoyez les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement…).
6. Vérifiez les mesures de sécurité mises en place.

ÉTAPE 4 – GESTION DES RISQUES

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées,vous devrez mener, pour chacun de ces traitements, une étude d'impact sur la protection des données (en anglais, « *Privacy Impact Assessment* » ou PIA).

Le point sur…

Comment se préparer au règlement européen sur la protection des données ?

ÉTAPE 5 – ORGANISER LES PROCESSUS INTERNES

Mettez en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demandes de rectifications ou d'accès, modification des données collectées, changement de prestataire). Notamment :

- 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). Pour cela, appuyez-vous sur les conseils du délégué à la protection des données,
- Sensibiliser et organiser la remontée d'information en construisant notamment un plan de formation et de communication auprès de vos collaborateurs,
- Traiter les réclamations et les 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) en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen),
- Anticiper les violations de données en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

ÉTAPE 6 – DOCUMENTER LA CONFORMITÉ

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire.

Cette documentation devra notamment comporter les éléments suivants :

- Le registre des traitements (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants),
- Les analyses d'impact sur la protection des données (PIA) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes,
- L'encadrement des transferts de données hors de l'Union européenne (notamment, les clauses contractuelles types, les BCR et certifications).

L'information des personnes :

- Les mentions d'information,
- Les modèles de recueil du consentement des personnes concernées,
- Les procédures mises en place pour l'exercice des droits.

Les contrats qui définissent les rôles et les responsabilités des acteurs :

- Les contrats avec les sous-traitants,
- Les procédures internes en cas de violations de données,
- Les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

Pour être à jour de vos obligations, contactez dès à présent votre expert-comptable !