

ELEMENTS ESSENTIELS MINIMUMS QU'UNE FORMATION DPD DOIT CONTENIR

I. OBJECTIF

L'objectif du présent document est d'établir une liste générale des éléments essentiels que doit contenir une formation qui a vocation à former et le cas échéant, au terme de celle-ci, de certifier des délégués à la protection des données au sens du règlement 2016/679 général sur la protection des données.

Le responsable du traitement ou le sous-traitant devront s'assurer, lors de la désignation (qu'elle soit obligatoire ou volontaire) d'un délégué à la protection des données, que ce dernier dispose des qualités professionnelles requises, en ce compris de connaissances spécialisées du droit et des pratiques en matière de protection des données ainsi que de sa capacité à exercer les missions qui lui sont attribuées par l'article 39 du règlement 2016/679.

Afin d'aider les responsables du traitement et les sous-traitants, la Commission vie privée a élaboré une liste des éléments essentiels minimums qu'une formation de délégués à la protection des données doit contenir.

Le présent texte a pour objectif de guider le responsable de traitement et les sous-traitants dans leur analyse et leur choix d'un délégué à la protection des données dans le respect du RGPD.

II. COMPETENCES REQUISES

Le délégué à la protection des données doit avoir une excellente connaissance des lois de protections des données et, idéalement des législations (sectorielles) autres qui complètent l'encadrement de la protection des données (en matière de santé, de gouvernance électronique par exemple), ainsi que des pratiques en la matière.

La fonction de délégué à la protection des données exige d'être capable, entre autre, de :

- ⇒ **S'assurer de la conformité avec les principes de base du traitement des données**, comme le principe de finalité déterminée, de minimisation des données, d'exactitude, de limitation de la conservation, et de l'intégrité et la confidentialité des données.
- ⇒ **Identifier avec précision la base de légitimité** des traitements de données.
- ⇒ **Analyser la compatibilité des finalités** autres que celles pour lesquelles les données ont été collectées.
- ⇒ **Déterminer s'il existe une réglementation sectorielle ou nationale** qui pourrait déterminer des conditions spécifiques autres que celles qui sont prévues par le RGPD.
- ⇒ **S'assurer de la bonne information** des personnes concernées via l'implémentation de procédures claires et bien définies.
- ⇒ **Gérer les demandes** des personnes concernées lorsqu'elles exercent leurs droits et mettre en place des procédures accessibles et simples pour l'exercice de ces droits.

- ⇒ **Gérer les demandes d'information** des personnes concernées par rapport au traitement de leurs données.
- ⇒ **Vérifier les contrats signés ou envisagés** avec des sous-traitants afin de s'assurer du respect des dispositions de l'article 28 du RGPD.
- ⇒ **Identifier les situations de transferts de données personnelles** en dehors de l'UE.
- ⇒ **Identifier les mécanismes les plus adéquats** pour encadrer au mieux les transferts de données personnelles.
- ⇒ **Veiller à la rédaction et exercer un contrôle** sur le contenu des « privacy policies » en conformité avec le RGPD.
- ⇒ **Participer à la création et à la gestion du registre des activités de traitement.**
- ⇒ **Participer à l'analyse de risque** des activités de traitement envisagées et en cours ainsi que **participer à l'analyse d'impact relative à la protection des données.**
- ⇒ **Veiller à la mise en place de mesures de sécurité adéquates** aux risques présentés et à la nature des opérations de traitement.
- ⇒ **Veiller à la mise en place de procédures pour gérer les brèches de sécurité** en conformité avec les prescrits du RGPD, en ce compris la notification à l'autorité de contrôle et la communication au public.
- ⇒ **Etre le point de contact pour les autorités de protection des données** et s'assurer d'une bonne collaboration avec elles.
- ⇒ **Mettre en place des programmes de formations** pour le personnel au sujet de la protection des données.

III. ÉLÉMENTS ESSENTIELS

Pour pouvoir effectuer toutes ces tâches, le/la candidat(e) au poste de délégué à la protection des données doit pouvoir démontrer qu'il/elle possède les compétences adéquates c'est-à-dire la connaissance théorique, la capacité professionnelle et les compétences personnelles pour s'acquitter des tâches liées à ce poste.

Les formations qui ont vocation à former/certifier des délégués à la protection des données au sens du RGPD doivent au minimum permettre au candidat :

- De **connaître la législation applicable en matière de protection des données**, en particulier le RGPD mais aussi les mesures nationales qui viennent le compléter (via les ouvertures laissées aux Etats membres).

- ☑ De **savoir quand celle-ci s'applique et à quelles situations** (champ d'application matériel et territorial).
- ☑ De **reconnaitre une données à caractère personnel** au sens du RGPD ainsi que de **reconnaitre les catégories spéciales** de données personnelles et d'avoir une connaissance fonctionnelle de toute autre définition du RGPD.
- ☑ De **connaître les principes de base de tout traitement de données**, en ce compris l'aptitude d'identifier les finalités de traitements des données personnelles.
- ☑ D'être en mesure de **rédiger des « privacy policies » ou « privacy statement » en toute transparence** vis-à-vis des personnes concernées.
- ☑ De **connaître en profondeur les droits des personnes concernées** ainsi que les **recours** possibles et les **sanctions** en cas de non-conformité à la législation.
- ☑ D'être capable de **faire une analyse de risque** des traitements de données personnelles en général.
- ☑ D'être capable **d'identifier quand une analyse d'impact relative à la protection des données** est nécessaire et veiller à ce qu'elle soit effectuée.
- ☑ D'avoir les **bases en sécurité de l'information** pour pouvoir conseiller efficacement lors de la définition des mesures de sécurité en fonction des risques.
- ☑ D'être capable **d'avoir une vue globale sur la gestion des données personnelles** au sein d'une entreprise ou autre organe via la tenue du registre des traitements.
- ☑ D'être en mesure **d'identifier le rôle d'un responsable de traitement et d'un sous-traitant** ainsi que d'être en mesure de **contrôler le contenu d'un contrat** conclu avec des sous-traitants pour la gestion des données personnelles.
- ☑ D'être en mesure **d'agir lors de la survenance d'une brèche de sécurité** via la mise en place de procédure efficaces.
- ☑ D'avoir une **connaissance fonctionnelle des autorités de protection des données**, de leurs tâches, de leurs pouvoirs et du mode de coopération en cas de mise en œuvre du mécanisme de guichet unique et de la cohérence.
- ☑ D'être en mesure **d'identifier les situations de transferts de données à caractère personnel** en dehors de l'EU et d'identifier le moyen adéquat pour encadrer ces transferts.