

PRESENTATION

Le Délégué à la protection des données (DPD) ou *Data Protection Officer* en anglais (DPO) est une évolution du Correspondant à la protection des données à caractère personnel défini dans le titre III (articles 42 à 55) du décret abrogé n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, plus connu sous l'appellation de Correspondant Informatique et Libertés (CIL).

Cette fonction de DPD est définie dans le Règlement général sur la protection des données (RGPD), 2016/679 du 27 avril 2016, principalement par le considérant 97 et par sa section 4. L'article 37 traite de la désignation du délégué à la protection des données, l'article 38 décrit ses fonctions et l'article 39 liste ses missions.

Depuis le 25 mai 2018, les Délégués à la protection des données sont formellement désignés par les responsables de traitement de données auprès des autorités de contrôle (la CNIL en France), soit obligatoirement, soit volontairement.

Les laboratoires font partie des entreprises qui vont devoir désigner un DPD. Dans ce cadre, Biocom Ouest propose un DPO en temps partagé qui aura pour mission principale d'aider la structure qui l'a désigné à être en conformité avec le cadre légal relatif aux données personnelles.

MISSION

Cet objectif est atteint au travers des missions suivantes :

a) Informer et sensibiliser, diffuser une culture « Informatique et Libertés »

Le Délégué à la protection des données :

- pilote, de façon maîtrisée, des actions visant à sensibiliser la direction, les collaborateurs - dont le personnel participant aux opérations de traitement - aux règles à respecter en matière de protection des données à caractère personnel ;
- fait en sorte de présenter les efforts de mise en conformité comme productifs et positifs, et non comme seulement des contraintes ;
- s'assure que les personnes concernées sont informées des traitements opérés impliquant leurs données personnelles, ainsi que de leurs droits.

b) Veiller au respect du cadre légal

Le Délégué à la protection des données veille en toute indépendance au respect du Règlement européen (RGPD), d'autres dispositions du droit de l'Union européenne ou du droit des États membres et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités. Ses analyses et conseils s'étendent à la gestion de la relation avec les sous-traitants et prestataires prenant part aux traitements décidés par le Responsable de traitement.

Le DPD porte conseil auprès du Responsable de traitement, et émet des avis et recommandations motivés et documentés. Pour mener à bien ses tâches, le Délégué à la protection des données se fait communiquer par le Responsable de traitement l'ensemble des informations nécessaires et dispose des moyens adéquats.



Le Délégué à la protection des données :

- pilote l'Analyse d'impact sur la protection des données (AIPD/PIA) ;
- est étroitement associé dans le « Privacy by Design » et le « Privacy by Default » (protection des données dès la conception du traitement de données et par défaut) ;
- pilote la notification à la CNIL et la communication aux personnes concernées relatives aux violations de données.

Il est **obligatoirement consulté avant la mise en œuvre d'un nouveau traitement ou la modification substantielle d'un traitement en cours** et peut faire toute recommandation au Responsable de traitement.

c) Informer et responsabiliser, alerter si besoin, son responsable de traitement

Le Délégué à la protection des données informe sans délai le Responsable de traitement de tout risque que les initiatives des opérationnels ou le non-respect de ses recommandations feraient courir à l'organisme et à ses dirigeants. À cette fin, il peut faire toute recommandation au Responsable des traitements et présenter des demandes d'arbitrage (il appartient au Responsable de traitement de prendre la responsabilité de mettre en œuvre un traitement malgré les recommandations du DPD). Le professionnel veille à formaliser une procédure pour informer directement le Responsable de traitement d'une non-conformité majeure.

d) Analyser, investiguer, auditer, contrôler

Le Délégué à la protection des données pilote, de façon maîtrisée et indépendante, toute action permettant de juger du degré de conformité de l'organisme, de mettre en évidence les éventuelles non-conformités (gravité, impacts possibles pour les personnes concernées, origine, responsabilité, etc.), de vérifier le respect du cadre légal ou la bonne application de procédures, méthodes ou consignes relatives à la protection des données personnelles. Ce pilotage nécessite dans un premier temps un audit externe de maturité sur la sécurité informatique et la conformité au RGPD, suivi d'audits réguliers en fonction de la vitesse d'avancement vers la mise en conformité.

e) Établir et maintenir une documentation au titre de « l'Accountability »

Le Délégué à la protection des données pilote la mise en œuvre de la documentation relative aux traitements de données à caractère personnel dont le registre des traitements, les différentes politiques, procédures et règles de contrôle, au titre de la Responsabilité du Responsable de traitement (« Accountability ») et assure son accessibilité à l'autorité de contrôle.

f) Assurer la médiation avec les personnes concernées et veiller à la bonne gestion des demandes d'exercice de droits

Le Délégué à la protection des données reçoit les réclamations des personnes concernées par les traitements pour lesquels il a été désigné et veille au respect du droit des personnes. Il traite ces réclamations et plaintes avec impartialité, ou met en œuvre les procédures propres à assurer leur bon traitement.

g) Présenter un rapport annuel à son Responsable de traitement

Le Délégué à la protection des données rend compte de son action en présentant chaque année un rapport à son Responsable de traitement. Ce rapport est le reflet fidèle de son action au cours de l'année écoulée et fait état des éventuelles difficultés rencontrées.

h) Interagir avec l'autorité de contrôle

Le Délégué à la protection des données est le point de contact privilégié de l'autorité de contrôle, avec laquelle il communique en toute indépendance sur les questions relatives aux traitements mis en œuvre par l'organisme qui l'a désigné, y compris la consultation préalable visée à l'article 36 du RGPD, et pour mener des consultations, le cas échéant, sur tout autre sujet.

Le DPD n'endosse pas la responsabilité juridique qui pèse sur le Responsable de traitement concernant la conformité.

ENGAGEMENTS DU LBM

Pour permettre de mener à bien ces différentes missions, le laboratoire s'engage à :

- Fournir l'accès aux données et aux opérations de traitement
- Fournir les ressources et les moyens nécessaires à la mise en conformité. A ce titre, le laboratoire à minima doit :
 - désigner un référent protection des données personnelles interne à l'entreprise qui sera le relai du DPO. Ce référent devra être associé à toutes les questions relatives à la protection des données, informé et consulté avant la mise en œuvre d'un nouveau traitement ou la modification substantielle d'un traitement en cours afin de transmettre de manière efficace l'information au DPO.
 - réaliser un audit externe de maturité informatique et de conformité au RGPD
 - réaliser à minima un audit externe de suivi tous les trois ans.

TARIFS

L'accompagnement à la mise en conformité proposé par Biocom Ouest se décline suivant les modalités suivantes, au choix (frais de mission sont en sus) :

1. Accompagnement forfaitaire sur une année

LBM : nb de salariés	Durée de la mission	Tarif TTC par an
De 1 à 20 salariés	1 jour in situ tous les 2 mois	4 800 € TTC (4 000 € HT)
De 21 à 50 salariés	1 jour in situ tous les 2 mois +0.5 jour / mois en back office	7 800 € TTC (6 500 € HT)
De 51 à 200 salariés	1 jour in situ tous les 2 mois +1 jour / mois en back office	10 800 € TTC (9 000 € HT)
+ de 200 salariés	8 jours in situ + 1 jour / mois en back office	15 600 € TTC (13 000 € HT)

2. Mission ponctuelle au tarif de 1 200 € TTC la journée, afin d'accompagner le LBM sur des thèmes précis, par exemple :

- Aide à la rédaction du registre de traitement de données
- Accompagnement à la conduite de l'analyse d'impact sur la protection des données (AIPD/PIA)
- Établir une politique de protection des données ou de sécurité
- Mettre en place les procédures de notification d'incidents, de gestion des droits des patients et des autres personnes concernées
- Sensibilisation des salariés et de la direction
- Cartographie des traitements (entre 2 et 4 jours en fonction du nombre de sites)

BULLETIN REPONSE

A faxer au 02 23 45 04 08 ou christine.provost@armoris.bzh

Je suis intéressé par :

L'accompagnement forfaitaire sur une année

Nb de salariés :

Nb de sites :

Mission ponctuelle

- Aide à la rédaction du registre de traitement de données
- Accompagnement à la conduite de l'analyse d'impact sur la protection des données (AIPD/PIA)
- Établir une politique de protection des données ou de sécurité
- Mettre en place les procédures de notification d'incidents, de gestion des droits des patients et des autres personnes concernées
- Sensibilisation des salariés et de la direction
- Cartographie des traitements

Cachet du LBM

Nom du biologiste :