

TARIFS

L'accompagnement à la mise en conformité proposé par Biocom Ouest se décline suivant les modalités suivantes, au choix (les frais de déplacements, restauration et hébergement 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
De 21 à 50 salariés	1 jour in situ tous les 2 mois + 0.5 jour / mois en back office	7 800 € TTC
De 51 à 200 salariés	1 jour in situ tous les 2 mois + 1 jour / mois en back office	10 800 € TTC
+ de 200 salariés	8 jours in situ + 1 jour / mois en back office	15 600 € TTC

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



VOTRE CONTACT :

sandrine.molgatini@armoris.bzh

armoris

Fédération des biologistes scolaires

ARMORIS

LE DPO EN TEMPS PARTAGE : ACCOMPAGNEMENT DES LBM

PRESENTATION

La fonction de Délégué à la protection des données (DPD) ou Data Protection Officer en anglais (DPO) est définie dans le Règlement européen sur la protection des données (RGPD) du 27 avril 2016, principalement par le considérant 97 et les articles 37 à 39. Depuis le 25 mai 2018, les Délégués à la protection des données sont formellement désignés par les responsables de traitement de données auprès de la CNIL.

Les laboratoires font partie des entreprises qui doivent obligatoirement désigner un DPO. 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 DPO :

- pilote, de façon maîtrisée, des actions visant à sensibiliser la direction et les collaborateurs aux règles à respecter en matière de protection des données ;
- s'assure que les personnes concernées sont informées des traitements de données opérés impliquant leurs données personnelles, ainsi que de leurs droits.

b) Veiller au respect du cadre légal

Le DPO veille en toute indépendance au respect du RGPD, d'autres dispositions du droit de l'Union européenne ou du droit des États membres, ainsi que des règles internes du Responsable du traitement ou du sous-traitant en matière de protection des données, 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 DPO porte conseil auprès du Responsable de traitement et émet des avis et recommandations motivés et documentés. Pour mener à bien ses tâches, il se fait communiquer par le Responsable de traitement l'ensemble des informations nécessaires et dispose des moyens adéquats.

Le DPO :

- pilote l'Analyse d'impact relative à la protection des données (AIPD/PIA) ;
- est étroitement associé à la protection des données dès la conception du traitement 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 DPO 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.

d) Analyser, investiguer, auditer, contrôler

Le DPO 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, de vérifier le respect du cadre légal ou la bonne application de procédures, méthodes ou consignes relatives à la protection des données. 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 DPO pilote la mise en œuvre de la documentation relative aux traitements de données dont le registre des traitements, les différentes politiques, procédures et règles de contrôle, au titre de la Responsabilité (Accountability) du Responsable de traitement, et il assure son accessibilité à la CNIL.

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

Le DPO peut recevoir 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 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 DPO 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 DPO est le point de contact privilégié de la CNIL, 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 (AIPD), et pour mener des consultations, le cas échéant, sur tout autre sujet.

Le DPO 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 doit a minima :

- désigner un référent protection des données 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 a minima un audit externe de suivi tous les trois ans.