Chapitre 3
Un système de management

1. Introduction

Ce chapitre décrit un système opérationnel de management des données à caractère personnel dont le but est de permettre à toute entreprise, quels que soient sa taille, son secteur, de respecter dans le temps les exigences du RGPD et de pouvoir le démontrer.

Au préalable, il nous semble utile de définir les termes suivants :

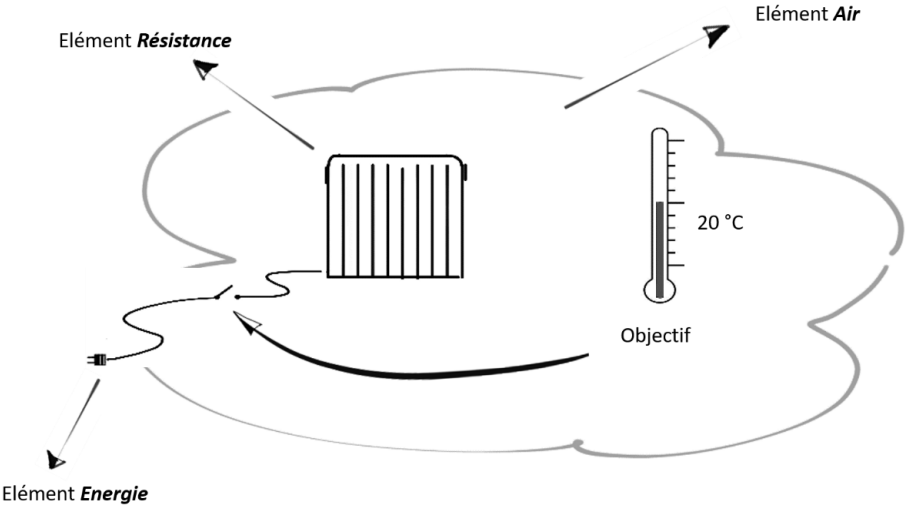
– Mesurer, c'est obtenir expérimentalement une ou plusieurs valeurs que l'on peut raisonnablement attribuer à une grandeur de même nature.
– Évaluer, c'est porter un jugement sur les valeurs mesurées.
– Contrôler, c'est vérifier le respect des procédures pour rechercher la conformité ou la régularité de celles-ci. Lorsqu'un écart est constaté, des actions correctives sont à mener.
– Piloter, c'est conduire vers un objectif.

2. Le système de management

2.1 Qu'est-ce qu'un système ?

Un système est un ensemble d'éléments interagissant entre eux de manière dynamique et en fonction d'un objectif. Pour assurer sa régulation, il dispose d'une boucle de rétroaction, appelée aussi feedback, qui permet de mesurer l'atteinte de l'objectif et d'agir en retour.

Exemple : votre système de chauffage comprend plusieurs éléments, à savoir l'énergie électrique, la résistance électrique du radiateur et l'air, qui interagissent. Dans ce système, si l'objectif est de maintenir une température ambiante de 20°, la fonction feedback est assurée par un thermostat d'ambiance qui actionne un interrupteur pour laisser passer le courant dans la résistance lorsque la température mesurée est au-dessous des 20° ou bien pour le couper lorsque celle-ci est au-dessus.



Système de chauffage

2.2 Qu'est-ce qu'un système de management ?

Les modalités de gestion d'une entreprise par sa direction constituent « l'art de manager ». Ces modalités font souvent partie de la culture et de la tradition orale de l'entreprise. Cela est particulièrement vrai pour les petites et moyennes entreprises, dans lesquelles les employés savent tous comment faire leur travail bien que peu de choses soient documentées. Disposer de politiques et procédures correctement documentées permet de s'assurer que chacun a bien connaissance des opérations qu'il doit réaliser pour contribuer à l'atteinte des objectifs de l'entreprise. Cette approche qui vise à objectiver, à structurer, à documenter et à communiquer les modalités de gestion d'une activité ou de plusieurs activités constitue un système de management.

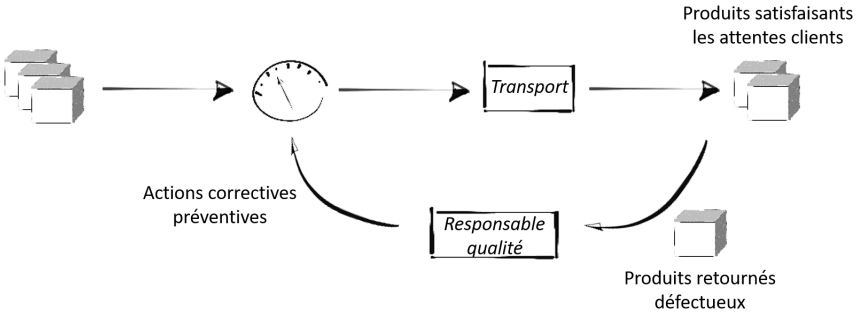
Selon l'ISO (Organisation internationale de normalisation), les systèmes de management permettent aux organismes de mettre en œuvre une démarche structurée dans leurs activités afin d'atteindre leurs objectifs.

Voici quelques exemples de systèmes de management :

Norme	Domaine	But
ISO 50001	Énergie	Pour faire un meilleur usage de l'énergie.
ISO 9001	Qualité	Pour que les produits et services soient constamment en phase avec les attentes des clients.
ISO 14000	Environnement	Pour maîtriser la responsabilité environnementale de l'entreprise.
ISO 27001	Sécurité de l'information	Pour assurer la sécurité des informations de l'entreprise.
ISO 27701	Protection de la vie privée	Extension d'ISO 27001 au management de la protection de la vie privée.

Il est probable que vous ayez déjà été concerné par un système de management de la qualité. C'est sans doute le système de management le plus répandu au monde. À partir d'objectifs de qualité ou de satisfaction client, il permet à l'entreprise de s'organiser pour que le niveau de qualité d'un produit ou d'un service soit conforme aux attentes des clients.

Exemple : une entreprise définit son taux de retour de produits défectueux. Celui-ci ne doit pas excéder 5 % du volume des ventes. Pour piloter cet objectif, l'entreprise effectue régulièrement des mesures. Au-dessous de 5 %, il n'y a pas d'actions spécifiques à mener. Au-dessus de 5 %, un contrôle est effectué pour identifier les causes de dépassement et des actions correctives et préventives sont à mener.



Contrôle qualité sur la chaîne logistique

2.3 Caractéristiques d'un système de management

Pour mieux comprendre ce qu'est un système de management, il nous paraît utile d'en donner ses caractéristiques. C'est à partir de ces caractéristiques que nous allons concevoir le système de management des données à caractère personnel (SMDCP).

Un système de management se caractérise principalement par :

– sa finalité
– son interaction avec l'environnement
– les objectifs pour arriver à la finalité

– les éléments qui le composent
– la fonction de contrôle ou de feedback
– sa politique
– le référentiel auquel il appartient
– ses propriétés, c'est-à-dire les qualités qui lui sont propres

3. Conception du SMDCP

Pour concevoir le SMDCP, nous avons considéré chacune des caractéristiques énoncées précédemment et nous les avons déclinées sur le domaine concerné.

3.1 Finalité du système

Il s'agit d'exprimer son but : pour quoi le système de management est conçu.

Dans notre cas, le système est conçu pour : permettre à l'entreprise de respecter dans le temps les exigences du RGPD et de pouvoir le démontrer.

3.2 Interaction du système avec son environnement

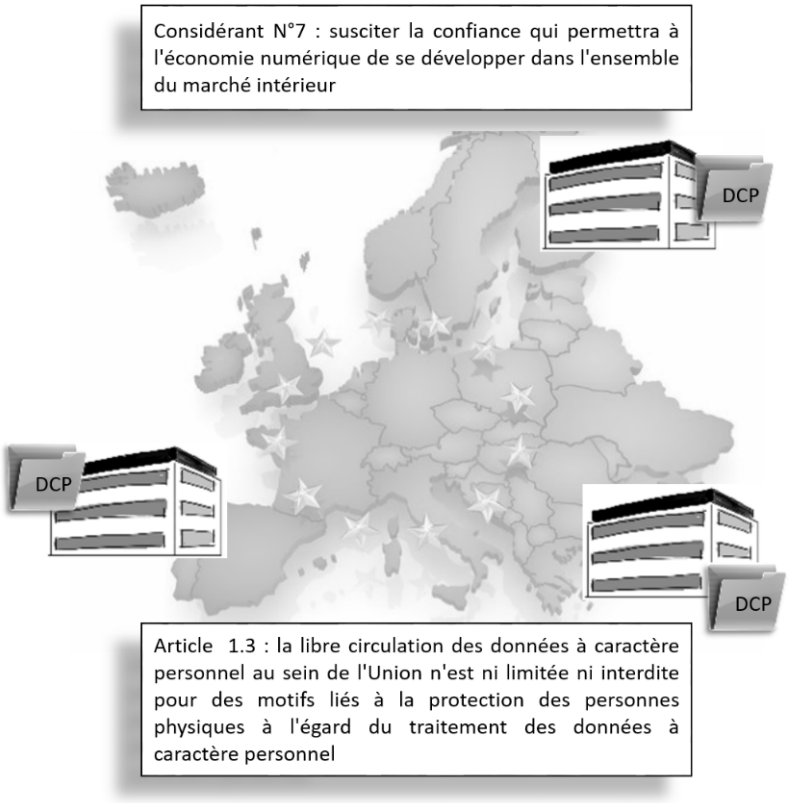
L'environnement considéré est celui du marché intérieur de l'Europe dans un contexte d'économie mondiale qui trouve principalement sa croissance dans le numérique. La libre circulation des données à caractère personnel est un des fondamentaux de cette nouvelle économie.

Cet environnement est pour partie résumé dans les considérants 6 et 7 ainsi que dans l'article 1.3 :

– L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. Ces évolutions requièrent un cadre de protection des données solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, car il importe de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur.

– La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Ce système doit accompagner la transformation numérique de l'entreprise pour lui permettre d'opérer légalement dans cette nouvelle économie.



Environnement

3.3 Objectifs du système

Une finalité du SMDCP qui se décline en objectifs.

Respecter dans le temps les exigences du RGPD et pouvoir le démontrer oblige l'entreprise à définir, à formuler et à combiner de multiples objectifs.

Pour définir et formuler les objectifs du SMDCP, nous avons analysé le contenu des exigences réglementaires. Nous en avons fait ressortir une trentaine. Nous les détaillerons un peu plus loin, mais à titre d'exemple en voici trois :

– Garantir que la gestion des droits de la personne concernée et les obligations réglementaires sont prises en compte dès la phase de conception d'un projet et durant son cycle de vie.
– S'assurer que tout le personnel traitant des données à caractère personnel a conscience de la pertinence et de l'importance de ses activités de traitement.
– Être organisé pour réagir en cas de violation de données.

Remarque

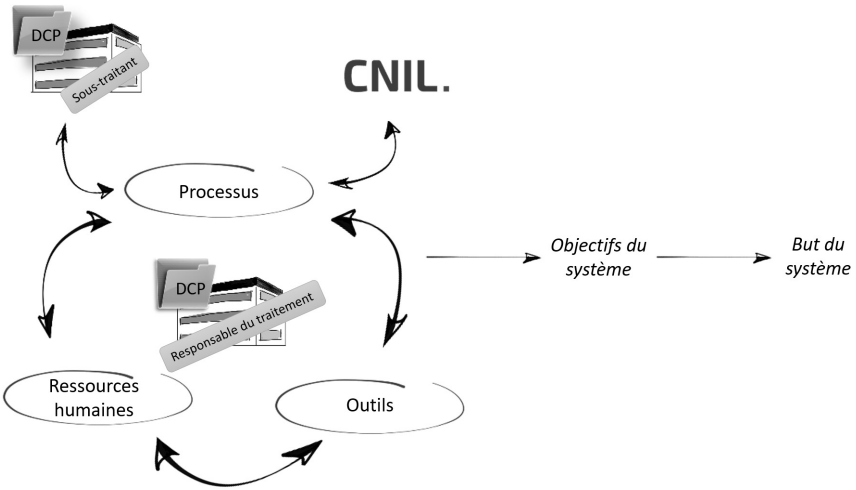
Le nombre et la formulation des objectifs sont à la libre appréciation du responsable du traitement.

3.4 Éléments qui le composent

Une fois les objectifs définis, nous pouvons déterminer les éléments qui composent le système, sa fonction de régulation, ses propriétés et ses règles de fonctionnement. Si les objectifs sont mal définis, le système sera mal conçu et il ne pourra atteindre son but.

Nos différentes expériences en matière de système de management organisationnel mettent en évidence trois types d'éléments qui interagissent entre eux :

– Des processus
– Des outils matériels ou immatériels
– Des ressources humaines



Trois éléments qui permettent de contribuer à l'atteinte des objectifs

3.5 Autres caractéristiques

Nous reviendrons plus loin sur les autres caractéristiques énoncées, car il nous semble important d'aborder dès à présent les éléments du système.

4. Processus du SMDCP

4.1 Définition

Un processus est un ensemble ou une succession d'activités réalisées à l'aide de moyens (personnel, informations, outils) pour atteindre un objectif.

Un processus peut se décomposer en plusieurs activités, qui elles-mêmes se décomposent en tâches.

La procédure est, quant à elle, une manière spécifiée d'effectuer les tâches d'un processus.

Chapitre 3
Le métier et son environnement

1. Le métier et son environnement

Depuis mai 2018, le rôle et les responsabilités du DPO ont évolué en raison de l'accent mis sur la protection des données à l'échelle mondiale.

Le RGPD a permis une harmonisation des règles au sein de l'Europe et le rôle du DPO est devenu central dans la conformité à cette réglementation.

Même si le RGPD est une réglementation de l'Union européenne, ses principes et exigences ont influencé les pratiques de protection des données à l'échelle mondiale. De nombreuses organisations en dehors de l'UE ont également choisi de désigner un DPO pour garantir la conformité aux normes internationales de protection des données.

Le RGPD a renforcé l'indépendance du DPO en exigeant qu'il exerce ses fonctions de manière indépendante et ne soit pas soumis à des instructions hiérarchiques. Cela garantit que le DPO peut accomplir ses tâches sans ingérence et jouer un rôle de contrôle et de conseil impartial au sein de l'organisation.

Les DPO sont devenus des acteurs clés, ils jouent un rôle de liaison avec les personnes concernées (les individus dont les données sont traitées) et doivent faciliter l'exercice de leurs droits en matière de protection des données.

2. Le positionnement du DPO dans l'organisation

Comme vu précédemment, le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données à caractère personnel pour l'ensemble des traitements réalisés par l'organisme pour lequel il travaille.

Pour mener à bien cette mission, qu'il soit interne ou externe à l'organisme, le DPO doit disposer de qualités et connaissances spécifiques au métier mais également de moyens matériels et organisationnels. Il doit avoir un positionnement adéquat au sein de l'organisation et a besoin des ressources nécessaires pour mener à bien sa mission.

Le DPO est un acteur clé de la mise en conformité aux lois et règlements en matière de protection des données, il est la pierre angulaire du principe de responsabilité, renforcé depuis la mise en application du RGPD.

Même s'il n'est pas personnellement responsable en cas de non-respect, il établit clairement les responsabilités portées par le responsable de traitement et ses potentiels sous-traitants.

La CNIL précise dans son *Guide du DPO* : "*Le DPO a avant tout une mission d'information de conseil et de contrôle. Il n'est pas responsable de la conformité de l'organisme, de la tenue du registre, de la réalisation des analyses d'impacts ou des notifications de violations de données. Il est cependant en position d'en être un acteur clé dont les compétences seront très utiles au responsable de l'organisme pour l'aider à se conformer à ses obligations.*"

Ceci démontre bien que le DPO doit disposer d'une parfaite autonomie au sein de l'organisme qui l'emploie, au regard de la ligne managériale puisqu'il accompagne les responsables de traitements, dans leurs tâches pour assurer et être en mesure de démontrer que leurs traitements sont effectués conformément aux dispositions légales (article 24, paragraphe 1).

Comme il doit être en capacité de les conseiller et de contrôler la mise en œuvre effective des mesures techniques et organisationnelles, il ne doit pas être lui-même dépendant d'une entité pour laquelle il aurait des responsabilités opérationnelles dans la définition et la mise en œuvre de ces mesures, au risque sinon de devenir "juge et partie".

Nous le voyons, l'absence de **conflit d'intérêts** est étroitement liée à l'obligation d'agir en toute indépendance. Cela ne signifie pas pour autant qu'un DPO ne peut pas être rattaché à une Direction, et être obligatoirement un "satellite", bras droit de la Direction au niveau d'un organigramme, mais surtout que le DPO ne peut pas se voir confier d'autres missions et tâches opérationnelles s'il assure sa mission de DPO à temps partiel.

Le DPO, pour des facilités administratives, est souvent rattaché à une entité dont le responsable devrait jouer un rôle de « superviseur » uniquement afin de laisser son autonomie au DPO et ne pas conditionner une relation de subordination. Or, ce rôle de superviseur est très souvent mal compris, car il ne correspond pas à la relation classique d'un manager vis-à-vis d'un membre de son équipe. Cela sous-entend qu'il ne faut pas donner d'instructions, mais accompagner le DPO afin qu'il puisse remplir sa mission au sein de l'organisme. Il y a donc, au vu des remontées terrain, des difficultés aussi bien au niveau du « superviseur » pour trouver sa place que des difficultés pour le DPO au regard de ses missions pour trouver également sa place.

Le DPO, par exemple, ne peut pas exercer au sein de l'organisme une fonction avec un pouvoir décisionnel qui l'amène à déterminer, lui-même, les finalités et les moyens des traitements de données à caractère personnel de son entité et devenir ainsi responsable de traitement, donc être "juge et partie".

Autre exemple donné par la CNIL en termes de conflit d'intérêts : "*un conflit d'intérêts peut également exister si un Délégué, nommé sur la base d'un contrat de service, représente l'organisme devant les tribunaux dans des dossiers impliquant des sujets en matière de données à caractère personnel.*"

En ce qui concerne le cas particulier du DPO souhaitant assurer un rôle de **représentant du personnel**, il est à noter qu'un délégué du personnel peut être amené, dans le cadre d'un vote, à prendre position sur certains sujets ou projets en lien avec le traitement de données à caractère personnel, notamment la gestion du personnel. Dans cette hypothèse, il peut exister un risque de conflit d'intérêts avec la fonction de DPO.

En ce qui concerne les aspects "comité éthique" et "déontologie", un DPO peut figurer dans ce type de comité si tant est que cela ne crée pas de risques de conflits d'intérêts.

Vis-à-vis du rattachement du DPO à une direction particulière, le RGPD ne précise pas le niveau de « rattachement » du délégué qui dépend le plus souvent de la direction des systèmes d'information (DSI), de la direction des risques, de la conformité, de la direction juridique ou encore du secrétariat général de l'organisme. Quelle que soit la direction à laquelle il est rattaché, il importe que le DPO soit en mesure de faire directement un rapport au niveau le plus élevé de la direction de l'organisme afin que ses conseils soient connus et pris en compte.

Ainsi, nous pouvons dire que le positionnement, ou les missions annexes du DPO dans le cadre par exemple d'un temps partiel, est à étudier au cas par cas par l'organisme.

Retour d'expérience « autonomie et conflit d'intérêts » : sur le terrain, de nombreux DPO mettent en avant que leur « autonomie » est plutôt synonyme de « solitude ». Le DPO est régulièrement rattaché à une entité et rend des comptes au quotidien, non pas au plus haut niveau de la hiérarchie mais à un responsable qui, même involontairement, induit une orientation à la démarche : plus juridique ou sécurité informatique selon le service de rattachement. Pour se sentir moins seul, le DPO entretient des relations privilégiées avec ses pairs.

On pourra noter également le cas de l'avocat du barreau inscrit au COD (Conseil de l'ordre départemental) de son département et qui devient le DPO de son Ordre départemental. La proposition de poste est intéressante car il a toutes les compétences requises, mais son statut initial le met dans la position d'être juge et partie et il a fait le choix de décliner l'offre.

En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts avec la fonction DPO au sein de l'organisme peuvent figurer :

– les fonctions d'encadrement supérieur : directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable département marketing, responsable des ressources humaines, responsable du service informatique ;
– les fonctions d'un niveau inférieur à l'encadrement supérieur (management de proximité par exemple) : ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement, comme évoqué précédemment.

Souvent par le passé, le responsable de la sécurité des systèmes d'information était également désigné DPO. Si celui-ci ne dispose pas, en qualité de RSSI (Responsable de la sécurité des systèmes d'information) d'un pouvoir décisionnel dans la détermination des finalités et des moyens des traitements de données à caractère personnel de son entité, cela ne pose pas de problème; mais ce cas de figure s'est avéré de moins en moins vrai, et des problématiques de conflits d'intérêts se sont posés, c'est pourquoi ce cumul des fonctions est de moins en moins répandu à ce jour.

La notion d'**autonomie** est primordiale pour l'efficacité de la mission du DPO. Ainsi, l'article 38 du RGPD, paragraphe 3 prévoit certaines garanties de base destinées à maintenir un degré suffisant d'autonomie au sein de l'organisme. Par exemple, il est précisé que les responsables du traitement/sous-traitants doivent veiller à ce que le DPO « ne reçoive aucune instruction en ce qui concerne l'exercice des missions».

Arrêt de la CJUE du 09/02/23 sur l'indépendance du DPO : s'agissant de la question de **l'existence de conflits d'intérêts**, la CJUE a rappelé que le RGPD prévoyait que le DPO peut exécuter d'autres missions et tâches, sous réserve que ces dernières n'entraînent pas de conflit d'intérêts, pour préserver l'indépendance fonctionnelle de ce dernier. Logiquement, la Cour a souligné que le DPO ne "*saurait se voir confier des missions ou des tâches qui le conduiraient à déterminer les finalités et les moyens du traitement de données à caractère personnel auprès du responsable de traitement ou de son sous-traitant [...] le contrôle de ces finalités et moyens doit être effectué de manière indépendante par le DPO*". Elle a d'ailleurs rappelé que la détermination de l'existence d'un conflit d'intérêts dans le cadre de l'application de l'article 38 du RGPD devait être effectuée au cas par cas, en prenant en compte l'ensemble des circonstances pertinentes et notamment la "*structure organisationnelle*" du responsable de traitement ou du sous-traitant.

Il est intéressant de noter que cet arrêt s'inscrit aussi dans le contexte des futurs travaux du *Coordinated Enforcement Framework* (CEF) de l'EDPB en 2023, ceux-ci ayant pour objectif de se pencher sur le rôle et les modalités de désignation des DPO.

Précisons que si le responsable de traitement ou un sous-traitant prend des décisions qui sont incompatibles avec le RGPD et à l'encontre de l'avis du DPO, ce dernier devrait avoir la possibilité d'indiquer clairement son avis divergent auprès de la Direction. Ce point est précisé dans l'article 38, paragraphe 3 du RGPD de la façon suivante : le DPO "fait directement rapport au niveau le plus élevé de la Direction du responsable du traitement ou du sous-traitant". Ainsi, le rapport annuel rédigé sur les activités du DPO remis à la Direction constitue un des moyens les plus efficaces pour permettre cette communication directe au plus haut niveau de la hiérarchie de l'organisme.

Par ailleurs, le DPO agit comme intermédiaire entre les différents acteurs concernés par la protection des données à caractère personnel, tels que les responsables de traitement de l'organisme, les sous-traitants de l'organisme, mais également en externe vis-à-vis des personnes concernées et les autorités de contrôle.

Retour d'expérience « Intermédiaire et chef d'orchestre » : dans la pratique en tant que DPO, nous sommes nombreux à tenir le registre, à rédiger les analyses d'impacts et à être en quelque sorte le conseiller mais également «la petite main» du responsable de traitement. Il nous faut donc, non seulement connaître parfaitement le règlement pour conseiller le responsable de traitement sur le plan réglementaire et procédural, mais également maîtriser les outils pour rédiger et tenir la documentation participant à assurer la conformité au règlement.

Ceci nous amène à la situation cocasse où nous donnons régulièrement un avis sur une analyse de risque (PIA) que nous avons-nous même rédigé ! Le DPO est chef d'orchestre et homme-orchestre.

Retour d'expérience « Intermédiaire et chef d'orchestre » : il arrive très souvent qu'en matière de gestion des contrats, le DPO soit amené à auditer la conformité de tous les contrats passés par l'organisation en direction de ses partenaires et fournisseurs. En ce sens, il sert d'intermédiaire entre plusieurs entités qui commercent ensemble et devient dès lors pour le groupe entier, une précieuse ressource pour le groupe entier.

En ce qui concerne la localisation du DPO, le RGPD ne fixe pas d'exigence, cependant, celui-ci doit être facilement joignable par les personnes concernées et les autorités de contrôle compétentes.

Il est ainsi recommandé que le DPO soit localisé au sein de l'Union européenne dans la mesure du possible. Et ceci, que le responsable du traitement ou le sous-traitant soit ou non établi dans l'Union européenne. Si l'organisme ne possède pas d'établissement dans l'Union européenne, le délégué peut être établi hors Union européenne sous réserve qu'il puisse efficacement mener ses activités.

Retour d'expérience « UE » : le RGPD est un règlement qui a été pensé pour sécuriser tous les échanges de données dans et en dehors de la zone Europe. Ainsi, nul n'est censé ignorer l'esprit du texte car il représente une réelle garantie pour l'entreprise qui évolue sur des marchés internationaux. Ainsi, dans le cas de la filiale d'une entreprise américaine sur le sol italien, cette dernière a recruté un DPO qui réside dans le pays et qui en connaît les usages autant qu'il connaît l'entreprise de l'intérieur. Elle a fait le choix d'un collaborateur en interne car elle estime que c'est plus adapté à ses enjeux. Ce sont des choix qui engagent toute la ligne hiérarchique.

3. Le positionnement du DPO selon les études récentes

Afin de mieux comprendre ce qui se passe sur le terrain, différents organismes ont réalisé un certain nombre d'études. Celles-ci permettent également de mieux comprendre les évolutions au fil des années du métier du DPO.

3.1 L'étude de la DGEFP en 2022

L'AFCDP (Association française des correspondants à la protection des données à caractère personnel) s'est engagée aux côtés de la Délégation générale à l'emploi et à la formation professionnelle (Ministère du Travail) et de l'Agence nationale pour la formation professionnelle (AFPA) afin d'identifier au mieux les dynamiques et les enjeux en termes d'emploi et de formation liées au RGPD.