Denis VIROLE
Directeur des services d'Ageris Group
Gérant de Virole Conseil Formation

Le Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données définit dans la section 4, articles 37, 38 et 39 la désignation du Délégué à la Protection des Données, ses fonctions et ses missions. Le G29 a adopté le 13 décembre 2016 un « Guidelines on Data Protection Officers » afin d'aider les organismes à se mettre en conformité dans la désignation du DPO.

Pourtant un grand nombre d'organismes au sein de l'union se pose un grand nombre de questions dans l'interprétation de ces différents textes. Le DPO est-il simplement le nouveau nom du Correspondant à la Protection des données (CIL) pour la France ou s'agit-il d'une nouvelle fonction ?

Comment intégrer la répartition des fonctions dans la gouvernance pour la sécurité des données à caractère personnel et la protection de la vie privée ?

L'évolution de la fonction CIL vers la fonction DPO

1. Introduction

Nous nous intéresserons tout d'abord aux missions du Correspondant à la Protection des Données, (Correspondant Informatique et Libertés, pour la France) et aux évolutions vers la fonction de DPO (Data Protection Officer) présentée dans le GDPR (Règlement 2019/ : 679 du Parlement Européen et du Conseil relatif à la protection et à la libre circulation de ces données, et abrogeant la directive 95/46/CE).

L'objectif étant de non seulement structurer l'organisation pour la protection de la vie privée et la sécurité des Données à Caractère Personnel mais aussi et surtout de concevoir une gouvernance efficace, notamment avec les directions métiers et les services chargés de la mise en œuvre opérationnelle des traitements, harmonieuse, en fonction de la culture professionnelle de l'entité et conforme aux exigences du règlement.

2. La désignation et les missions du CIL

Nous allons analyser les types de désignation, les missions et les qualifications du CIL présentées dans la loi et comment les organismes ont intégré la fonction dans leur système de gouvernance. L'objectif est de modéliser trois types de maturité (naissante, moyenne et forte).

L'Article 22 III de la loi du 6 janvier 1978 modifiée suite à la Directive Européenne du 24 octobre 1995 définit que : *« Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24 sauf, lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé. La désignation du correspondant est notifiée à la CNIL. Elle est portée à la connaissance des instances représentatives du personnel. Le correspondant est une personne bénéficiant des qualifications requises pour exercer ces missions. Il tient une liste des traitements effectués immédiatement accessible à tout personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions … Il peut saisir la CNIL des difficultés qu'il rencontre dans l'exercice de ses missions ».*

2.1. Les trois types de désignation

Trois types de désignation sont alors possibles de la part du Responsable du Traitement.

- La désignation partielle : La désignation est faite seulement pour certains des traitements relevant des régimes de la dispense de déclaration, de la déclaration normale et de la déclaration simplifiée ;
- La désignation générale : La désignation est faite pour l'ensemble des traitements relevant des régimes de la dispense de déclaration, de la déclaration normale et de la déclaration simplifiée ;
- La désignation étendue : La désignation étendue est faite pour la totalité des traitements relevant de la responsabilité de celui qui désigne : les missions du CIL concernent également les traitements soumis au régime de la demande d'autorisation ou d'avis préalable.

Dans les trois cas, les traitements pour lesquels le responsable a désigné un CIL, chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 (déclaration) et 24 (déclaration simplifiée).

La désignation d'un CIL permet donc d'alléger les formalités. Elle a pour effet d'exonérer les responsables de traitements de l'accomplissement de tout ou partie des formalités préalables leur incombant. L'idée directrice est donc d'assurer une meilleure application de la loi. La désignation du correspondant permet au responsable de traitements de mieux assurer les obligations qui lui incombent en application de la loi.

La désignation du CIL offre un vecteur de sécurité juridique, elle doit permettre de garantir la conformité de l'organisme à la LIL. Elle est bien sûr un facteur de simplification des formalités administratives (exonération de l'obligation de déclaration préalable des traitements ordinaires et courants), elle offre un accès personnalisé aux services de la CNIL (extranet, formations, suivi personnalisé…), elle donne la preuve d'un engagement éthique et citoyen.

Le CIL exerce sa mission directement auprès du Responsable des Traitements. Sa désignation n'entraine aucun transfert de responsabilité. Le responsable des traitements demeure responsable de tous les manquements à la loi.

Le CIL ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de sa mission.

La responsabilité pénale d'un CIL doit toutefois pouvoir être retenue s'il enfreint intentionnellement la législation Informatique et Libertés ou s'il aide le Responsable des Traitements à violer la loi.

2.2. CIL interne ou externe

Le CIL interne est un employé du Responsable du Traitement connaissant bien l'activité et le fonctionnement interne de l'organisme.

Il est toutefois possible de désigner un CIL extérieur à l'organisme. Les possibilités de choix d'un CIL externe ne sont pas les mêmes pour toutes les structures :

- Le CIL interne : Le CIL est un employé du RT, de préférence connaissant bien l'activité et le fonctionnement interne de son entreprise ou administration ;
- CIL externe : Il est toutefois possible de désigner un CIL extérieur à l'organisme. Les possibilités de choix d'un CIL externe ne sont pas les mêmes pour toutes les structures :
    - Pour les entreprises ayant moins de 50 personnes qui sont chargées de la mise en œuvre des traitements et qui y ont directement accès, c'est-à-dire les structures de petite, moyenne importance : le choix du CIL est ici entièrement libre, c'est-à-dire qu'il peut être un employé, un employé d'une autre entité ou un professionnel indépendant ;

    - Pour les entreprises ayant plus de 50 salariés qui sont chargées de la mise en œuvre des traitements ou qui y ont directement accès : le choix du CIL externe est limité et seul peut être désigné comme CIL un employé de l'organisme ou un salarié d'une des entités du groupe de sociétés auquel appartient l'organisme, un salarié du groupement économique dont est membre l'organisme, une personne mandatée à cet effet par un organisme professionnel, une personne mandatée à cet effet par un organisme regroupant des responsables de traitements d'un même secteur d'activité.
- Le CIL mutualisé : La fonction de CIL peut être mutualisée entre différents organismes publics et privés, dès lors que ceux-ci sont liés par des intérêts économiques communs ou appartiennent à un même secteur d'activité.

3. Les missions

Le correspondant ne reçoit aucune instruction pour l'exercice de sa mission (le Responsable des Traitements ou son représentant légal ne peut être désigné comme CIL).

Les fonctions ou activités exercées concurremment par le CIL ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission (article 46 du décret d'application de 2005) :

- Diffuser une culture Informatique & Libertés ;
- Veiller en toute indépendance à l'application de la loi ;
- Tenir à jour la liste des traitements et assurer son accessibilité ;
- Définir une politique de protection de la vie privée ;
- Conseiller les acteurs concernés par le traitement des Données à Caractère Personnel ;
- Fournir des recommandations à ces différents acteurs ;
- Réaliser la médiation entre les personnes concernées et le Responsable du Traitement ou le Responsable du Traitement et l'autorité de contrôle (la CNIL) ;
- Exercer un droit d'alerte auprès de l'autorité de contrôle en cas de manquements constatés de la part du Responsable du Traitement.

4. Les qualifications

La Loi prévoit que le CIL est une personne bénéficiant des qualifications requises pour exercer ses missions. Ces compétences doivent porter tant sur l'informatique et les nouvelles technologies que sur la réglementation relative à la protection des données à caractère personnel. Elles doivent également avoir trait au domaine d'activité dans lequel il exerce ses fonctions.

Lorsque le CIL est une personne morale, cette condition de qualification doit être remplie par le préposé désigné par celle-ci pour mettre en œuvre les activités du correspondant.

Attention, la Loi ne prévoit pas d'agrément et aucune exigence de diplôme. Toutefois, le CIL doit disposer de compétences variées et adaptées à la taille comme à l'activité du Responsable du Traitement.

Lorsque le CIL ne dispose pas de l'ensemble des qualifications requises à la date de sa désignation, il devra les acquérir, notamment, en participant aux ateliers du CIL organisés par la CNIL.

5. La fonction CIL et les types de maturité face à la protection des Données à Caractère Personnel

5.1. Les organismes en maturité naissante :

Un très grand nombre d'organismes privés ou publics n'ont retenu que le gain de l'allégement des formalités dans la nomination d'un CIL. La nomination du Correspondant devient donc un véritable « alibi » de mise en conformité avec la loi.

Les autres missions sont sous estimées voire oubliées, notamment ;

- La mise en conformité opérationnelle et technique avec les Normes simplifiées, les Autorisations Uniques, les actes Réglementaires Uniques par exemples sur les devoirs de durée de conservation / destruction ;
- La formalisation des politiques et recommandations pour la protection de la vie privée ;
- La mise en œuvre effective de ces politiques ;
- La garantie de respect des droits de la personne concernée.
- …

De plus il est très courant que la fonction CIL soit partagée avec la mission de Directeur des systèmes d'information ou de Responsable sécurité système d'information. Si ce type de fusion de responsabilités sur le même poste semble faciliter les échanges culturels et d'expérience, il est contradictoire avec les principes de séparation des pouvoirs et des responsabilités liés aux fonctions de gouvernance et contrôle de conformité. Ce type d'organisation entraine classiquement des situations de conflit d'intérêt ou a minima de divergences de vue dans la réalisation effective des traitements de Données à caractère personnel.

Il est intéressant que certaines autorités de contrôle dans l'Union, telle que la Commission Nationale pour la Protection des Données du Luxembourg refuse ce type de désignation.

Le point marqueur de ce type d'organisation en faible maturité est la mauvaise compréhension et donc la sous-utilisation de la voie fonctionnelle qui relie le CIL à la CNIL. En effet, comme évoqué plus haut le CIL, ne reçoit aucune instruction de la part du Responsable du Traitement et en cas de difficulté, le CIL doit pouvoir solliciter et alerter la CNIL en cas de manquement.

Pour synthétiser, les caractéristiques de ce type d'organisme sont la faible culture Informatique et Libertés (la mission du CIL est donc réduite à la tenue d'un Registre et la constitution d'un bilan annuel rappelant les actions de sensibilisation effectuées dans l'organisme), le faible engagement opérationnel pour le respect des droits de la personne concernée, l'absence de prise en compte des risques juridiques et techniques.

5.2. Les organismes en maturité moyenne :

Les CIL de ces organismes ont su profiter non seulement de la voie fonctionnelle qui les relie à l'autorité de contrôle (la CNIL pour la France) mais aussi de la relation « privilégiée » qui les relie au Responsable des traitements. A force de sensibilisation, en mettant plus en avant le dommage de déficit d'image et la perte de confiance dans l'organisme que la peur de la sanction éventuelle, ils ont su récupérer des moyens et l'autorisation de déclencher des campagnes de sensibilisation, responsabilisation auprès de non seulement les directions métiers et les utilisateurs mais aussi auprès des directions techniques chargées de la mise en œuvre opérationnelle des traitements.

Ils entretiennent la diffusion de la culture protection de la vie privée grâce à des outils de communication (posters, goodies, plaquettes de synthèse, …). Ils mettent en œuvre un réseau de RILS, (Relais Informatique et Libertés) dans les métiers afin de relayer les messages essentiels.

Ils ont su aller plus loin que la simple sensibilisation. Ils écrivent ou se font assister pour la formalisation des procédures de traitement des demandes des personnes concernées, ce qui a sans conteste augmenté la mise en conformité de leur organisme avec la loi.

Pourtant la situation n'est pas totalement satisfaisante. Les CIL de ce type d'organisme sont suivis et appuyés par le Responsable du Traitement essentiellement pour les actions non structurantes. L'organisation de campagnes de sensibilisation, la constitution d'un registre des traitements et la définition des procédures pour mieux traiter les demandes des personnes concernées, n'est que peu structurante pour l'organisme et notamment pour le système d'information qui les traite. L'organisme n'a que peu intégré la dimension sécurité des traitements. La sécurité est encore vue comme une affaire d'expert technique.

Dans ce type de cas le Responsable des Traitements a donné son vert pour les actions citées, mais seule une partie du chemin est réalisée pour se mettre en conformité.

En effet quelle est la nature de la relation du CIL avec le DSI, le directeur de la sécurité physique et le RSSI ? Les engagements de responsabilité du Responsable du Traitement vont-ils plus loin que la simple communication ? Les engagements annoncés pour la protection de la vie privée sont-ils corrélés avec :

- Des règles de sécurité physique pour le cloisonnement, et l'accueil, l'accès, la circulation des personnes externes ou internes dans l'organisme ;
- Des règles de protection pour limiter les risques divers de la protection physique, (environnement, services essentiels, …) ;
- Des exigences fonctionnelles et opérationnelles de sécurité logique et physiques ;
- Des validations formelles des risques résiduels lors des projets manipulant des volumes importants de Données à Caractère Personnel ou de données sensibles ;
- De sensibilisations aux règles d'utilisation des supports d'informations sensibles ;
- D'audits de sécurité.

Le point marqueur de ce type de d'organisation en maturité moyenne est l'engagement relatif du Responsable du Traitement qui réduit la fonction du CIL à la communication interne et externe.

La réalisation d'actions effectives et opérationnelles de protection physique et logique en concertation avec les directions techniques est clairement sous-estimée ou retardée. En bref les actions sont concentrées sur la communication et peu dans les actions opérationnelles. Sans doute les actions effectives et concrètes corrélées à la protection de la vie privée font peur au Responsable du Traitement qui voit les principes de la protection plus comme des contraintes que comme des exigences. Il pressent ces contraintes comme allant à l'encontre des objectifs d'efficacité et performance.

La relation entre le CIL et le RSSI, s'il existe, est rarement fluide, surtout si le CIL a un profil technique faible ou une connaissance peu approfondie de la maitrise des risques Ils ont du mal à se comprendre, aussi dans ce cas le CIL se concentre essentiellement sur les actions de communication et de constitution du Registre et du bilan.

5.3. Les organismes en maturité effective :

Les CIL de ces organismes ont su alerter et surtout convaincre les Responsable de Traitement de mettre en place une gouvernance où chacun a un rôle déterminant à jouer, entre le Responsable du Traitement, les directions métiers, les utilisateurs, la Direction des systèmes d'information, le Responsable sécurité d'information et le CIL.

La ligne conductrice n'est plus la communication interne ou externe et la constitution d'un registre ou du bilan mais dans la protection effective de la vie privée par la sécurité des traitements des Données à Caractère Personnel.

L'approche est donc beaucoup plus structurante pour l'organisme. Il s'agit donc de définir :

- Des textes de référence montrant l'engagement de la direction pour la protection de la vie privée, une politique de protection des données à caractère personnel plus particulièrement destinée aux directions métiers, une politique de sécurité système d'information destinée à la DSI ou sa transcription contextuelle dans un Plan d'Assurance Sécurité destinée à un sous-traitant ;
- Les processus et les acteurs permettant aux directions métiers de définir par les directions les exigences juridiques et fonctionnelles liées à la sensibilité des traitements de Données à Caractère Personnel et aux menaces et risques associés ;
- Les règles opérationnelles structurées par la DSI ou le sous-traitant pour la mise en application des règles fonctionnelles définies par le RSSI ;
- Les principes du contrôle réalisé par le RSSI pour audit de la mise en conformité opérationnelle du SI avec le Référentiel.

Il est important de noter l'absence de contrôle direct du CIL et donc de la difficulté fournir une preuve de la mise en œuvre opérationnelle et effective de mesures concrètes pour la protection de la vie privée.

Les contrôles réalisés dans ces types de structure sont essentiellement des contrôles techniques réalisés par le RSSI sur le SI pour vérifier la bonne intégration des règles fonctionnelles du référentiel SSI, aussi les contrôles « informatique et libertés » de conformité juridique ou d'adéquation techniques au regard des évènements redoutés sont clairement sous-estimés.

Il est probable que le G29 a bien pris conscience cette situation et va bien insister notamment dans le document Guidelines on Data Protection Officer du 13 décembre 2016 sur l'objectif de contrôle afin d'être en mesure de démontrer la sécurité effective des données à Caractère Personnel, la protection de la vie privée, le respect des droits de la personne concernée et la communication et la coopération avec l'autorité de contrôle, (la CNIL pour la France) notamment en ce qui concerne la violation éventuelle de données à caractère personnel.

6. La désignation et les missions du DPO

La nouvelle réglementation européenne prévoit différents cas pour lesquels la désignation d'un DPO est obligatoire, article 37 :

- Le Traitement est effectué par une autorité publique ou un organisme public ;
- Les activités de base du Responsable du Traitement ou du Sous-Traitant consistent en des opérations de Traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- Il s'agit de Traitement de catégories particulières (condamnations pénales et infractions et données de santé, convictions religieuses, vie ou orientation sexuelle, données biométriques, données génétiques, origine raciale ethnique etc.).

A la différence du décret de 2005, le Règlement Européen ne prévoit pas de conditions particulières quant à la désignation d'un DPO externe. En d'autres termes, une entreprise chargée de la mise en œuvre d'un traitement peut choisir de désigner un DPO externe.

Le Règlement précise que le Responsable du Traitement ou le sous-traitant (aucune mention dans le Décret) publient les coordonnées du DPO à l'autorité de contrôle.

La réglementation européenne prévoit que le DPO soit désigné sur la base de ses qualités professionnelles et en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

Elle détaille la fonction du délégué à la protection des Données à Caractère Personnel. Outre les points déjà abordés par le Décret de 2005 :

- Informer et conseiller le Responsable du Traitement ou le sous-traitant ;
- Contrôler le respect du Règlement Européen ;
- Dispenser sur demande des conseils relatifs à l'Etude d'impact sur la Vie Privée, (EIVP) ;
- Coopérer avec l'autorité de contrôle ;
- Faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement.

Ainsi Il nous semble important de mettre en avant les points suivants :

- La dispense de conseil en ce qui concerne l'EIVP ;
- La coopération avec l'autorité de contrôle ;
- Faire office de point de contact aussi bien pour les personnes concernées, l'autorité de contrôle ou les sous-traitants ;
- Le contrôle du respect du Règlement européen ;
- La capacité de démontrer la conformité au Règlement.

La différence fondamentale avec la mission du CIL réside dans la fonction de contrôle afin de pouvoir démontrer la conformité.

Il est donc clair que pour les organismes à maturité naissante ou moyenne, cette fonction n'est que très rarement mise en œuvre.

Les CIL étaient à l'aise pour réaliser des opérations de sensibilisation et de communication. Ces profils de CIL assurent partiellement les fonctions de conseil auprès des directions métiers, rencontrent beaucoup de difficultés pour participer aux EIVP et se sentent très rarement capables techniquement et humainement parlant de réaliser les fonctions de contrôle.

Par contre pour les organismes à forte maturité sécurité, le CIL devient une maitrise d'ouvrage de sécurité :

- Exprimant des exigences juridiques de protection, des besoins fonctionnels de protection, des évènements redoutés ;
- Identifiant des sources de menaces et de risques ;
- Sous-traitant la fonction de contrôle des mesures techniques de sécurité par le RSSI.

Il faut souligner dans ce cas la nécessité de séparer la fonction CIL de celles du RSSI et du DSI afin d'éviter la confusion entre les fonctions de spécification, de mise en œuvre et de contrôle

7. Les deux interprétations possibles de la mission du DPO

7.1. La reconduction du CIL dans la fonction de DPO

C'est clairement la lecture la plus classique, courante et facile. Elle est rassurante, mais trompeuse, nous alertons le lecteur, que cette interprétation de la fonction de DPO ne peut être réduite qu'à un changement d'acronyme.

Effectivement, la nomination d'un DPO ne pourra être restreinte qu'aux actions de communications ou de gestion des demandes des personnes concernées mais devra a minima permettre des actions structurantes de sécurité des traitements associés aux données à caractère personnel afin de limiter les risques redoutés et de protéger la vie privée des personnes concernées.

La lecture du point 74 de l'introduction du Règlement insiste clairement sur la nécessité de **démontrer** la sécurité : *« il y a lieu d'instaurer la responsabilité du Responsable du Traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte. Il importe en particulier, que le responsable du traitement soit tenu de mettre en œuvre des mesures appropriées et effectives et soit à même de* ***démontrer*** *la conformité des activités de traitement avec, le présent règlement, y compris l'efficacité des mesures. Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et les libertés des personnes physiques ».*

La capacité de démontrer que les actions de protection sont en adéquation avec le contexte, les enjeux et les risques entraine une nouvelle compréhension de la fonction de DPO.

Elle nécessite bien entendu la mise en place d'une gouvernance optimale entre les métiers et les maitres d'œuvre de la protection.

La mise en place de cette gouvernance nécessitera avant tout une nouvelle communication sensibilisation auprès du Responsable du Traitement.

L'exigence « de démontrer la sécurité » devient certes un levier extrêmement fort pour le RSSI pour récupérer des appuis et des ressources du Responsable du Traitement mais restera un peu floue pour un grand nombre de DPO qui auraient compris le Règlement uniquement comme un changement d'acronyme de la fonction CIL.

L'organisation à mettre nécessitera une réponse à l'interrogation majeure : comment contrôler la protection effective et comment fournir la preuve de cette sécurité pour les personnes concernées, la vie privée et les autorités de contrôle afin d'assumer les responsabilités du Responsable du Traitement ou du sous-traitant ?

7.2. Le DPO, contrôleur de la mise en conformité

Comme évoqué plus haut, le G29 a formalisé dans le document « Guidelines on Data Protection Officer le 13/122016 les exigences du contrôle afin de démontrer la conformité et c'est bien face à l'obligation de contrôle que cette deuxième lecture de la fonction de DPO, se caractérise.

Le DPO doit être bien plus qu'un CIL. Tout contrôle de conformité s'appuie sur le principe de séparation des devoirs et responsabilités. Il n'est pas possible de s'autocontrôler.

Les organismes matures en sécurité ont bien compris cette exigence dans le lien qui lie le RSSI et le maitre d'œuvre, classiquement le DSI. Le RSSI formalise les règles fonctionnelles, le DSI ou le sous-traitant les intègre, ce qui permet au RSSI de contrôler puisque ce n'est pas lui qui les a intégrées. Il est intéressant de noter que ces organismes matures ont été contraint d'atteindre ces exigences de séparation des devoirs (expression de besoins, déclinaisons opérationnelles du besoin et contrôle de conformité) ont été réalisées suite à la formalisation de réglementations telles que Bâle 3, le Sarbanes Oaxley Act ou Solvency 2.

Or dans le contexte de la protection de la vie privée, la fonction de CIL était réduite pour l'essentiel à signer les demandes internes d'autorisation de traitement, alerter les directions métiers, à participer (dans le meilleur des cas) avec le fort appui du RSSI, conformément aux recommandations de la CIL, la méthode EIVP, à formaliser les mesures juridiques liées aux traitements à mettre en œuvre lors des EIVP.

Or, si les organismes matures en SSI ont su gérer la séparation des fonctions dans le SI :

- Les Chefs de projet utilisateur (CPU) représentent les métiers, responsables de l'expression des besoins de sécurité et de l'identification des évènements redoutés ;
- Les Chefs de projet informatique (CPI) coresponsables avec les Chefs de projet utilisateur de l'identification des risques ;
- Les CPI sont responsables de la mise en œuvre des solutions techniques pour les réduire ;

- Le RSSI contrôlant la conformité de la solution avec la politique de sécurité système d'information de l'organisme ;
- Le Responsable du Traitement valide, voire homologue le SI, après avoir pris connaissance et acceptation des risques résiduels.

Le problème se pose de manière équivalente pour la protection de la vie privée dans le Règlement.

Le contrôle est fondamental afin de pouvoir fournir la preuve du principe de sécurité. Les organismes soucieux de cette problématique, donc matures en protection des Données à Caractère Personnel, devront désigner un DPO dans une structure d'audit et de contrôle de conformité, interne ou externe.

On peut ainsi imaginer un CIL au sens classique qui met en œuvre avec le RSSI et le DSI ou le sous-traitant la protection de la vie privée et la sécurité des données personnelles et un DPO qui contrôle voire « certifie » afin d'être capable de fournir la preuve de la protection.

Encore une fois la fonction de DPO ne pourra être cumulée avec la fonction de DSI.

Il est important de souligner que les avocats ou les juristes qui se positionnent commercialement en futurs DPO externes sont particulièrement crédibles pour la mise en conformité et le contrôle des exigences juridiques (profondément réduites en termes de déclarations auprès de l'autorité de contrôle), notamment auprès des personnes concernées devront faire un effort réel pour fournir la même crédibilité pour les aspects fonctionnels et techniques de la sécurité notamment pour les EIVP.

Ainsi conformément aux points 2 et 3 de l'article 37 *:*

« 2 Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

3 Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille »

Il est particulièrement probable que les cabinets de conseil juridique se positionnent pour réaliser des missions de DPO orientés contrôle plus que mise en œuvre. Ils devront aussi acquérir la même crédibilité pour les contrôles techniques.

Il devient logique de se poser la question alors de la fusion de la fonction CIL historique classique avec la fusion de RSSI.

Le CIL « évangélisateur » de la protection de la vie privée et les CPU expriment des besoins, les CPI avec la DSI implémentent et intègrent les mesures et les solutions techniques. Le RSSI contrôle l'implémentation des solutions et le respect des politiques de sécurité. Le DPO contrôle l'efficacité de l'ensemble pour la protection de la vie privée et s'assure de la capacité de fournir des preuves de la conformité des mesures et de l'efficacité des solutions pour la protection de la vie privée.

Conclusion

Comme le Règlement Européen le rappelle « *afin de respecter tous les droits fondamentaux et d'observer les libertés et les principes reconnus par la* ***Charte des droits fondamentaux de l'Union Européenne****, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des DCP, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et accéder à un tribunal impartial, et la diversité culturelle et religieuse*, » il est important d'insister sur les connaissances nécessaires spécialisées du droit et des pratiques en matière de protection des données, du DPO.

L'objectif, après la protection des droits de la personne concernée et la mise en conformité juridique est d'être en capacité de fournir la preuve de la protection des données à caractère personnel et des traitements associés.

Il est important de noter que le respect des Codes de conduite (aujourd'hui packs de conformité ou Binding Corporate Rules), la labellisation par exemple pour la gouvernance, puis la certification, sont des outils importants pour démontrer le respect des exigences juridiques.

La CNIL va certainement diffuser dans les 12 à 18 mois qui viennent de nouveaux Codes de conduite et de nouvelles directives pour appliquer le règlement.

La mise en place d'un système de management ISO 27001 pour le périmètre des traitements de données à caractère personnel ou l'utilisation de produits certifiés ANSSI ou CNIL constituent d'autres outils pour être en mesure de démontrer une sécurité coordonnée, contrôlée puis optimisée.

La bonne réalisation de la mission de DPO devra nécessiter un plan d'action de sensibilisations juridiques et techniques auprès du Responsable du Traitement et de tout l'encadrement. Le message essentiel étant de gérer la séparation des fonctions de l'expression de besoins, de la déclinaison technique et du contrôle du respect des exigences afin de fournir la preuve de la conformité et de l'adéquation de la solution au contexte. Ce message étant compris (la fourniture des ressources au DPO par le Responsable du Traitement en dépend) » la mission de DPO (interne ou externe) véritable certificateur au service du Responsable du Traitement pourra s'effectuer en harmonie avec les autres acteurs.

Denis VIROLE

Directeur des services Ageris Group

Gérant de VIROLE CONSEIL FORMATION