Cabinet Infhotep

Data Protection Officer

Quel schéma organisationnel de gouvernance Informatique et Libertés ?

Edition 2017

Cabinet Infhotep
6 rue d'Antin
75002 Paris
France
Tél : +33 (0) 155 353 636
Fax : +33 (0) 155 353 640
Mail : contact@infhotep.com
www.infhotep.com
demain.infhotep.com

Remerciements

Pour commencer, nous tenons à remercier les acteurs en charge de la protection des données des groupes SANOFI, ACXIOM, AG2R LA MONDIALE, CNP ASSURANCES et de la Commission Nationale des Allocations Familiales qui ont acceptés de répondre à nos questions lors des entretiens que nous avons menés et plus particulièrement Pierre-Yves LASTIC, Sarah WANQUET, Michel BAZET, Philippe SALAUN et Bruno RASLE.

Nous adressons nos sincères remerciements à Albine Vincent, Cheffe du service des Correspondants Informatique et Libertés au sein de la CNIL.

Nous tenons également à remercier les membres de l'AFCDP qui ont répondu au questionnaire en ligne sur les différentes actions déjà menées dans le cadre de la mise en conformité au Règlement Général de Protection des Données de leur organisation.

Sans oublier l'ensemble des participants au questionnaire en ligne qui ont répondu via les réseaux sociaux.

Préambule

Le règlement général sur la protection des données du 27 avril 2016, adopté par le Conseil et le Parlement européen sera applicable à partir du 25 mai 2018 dans tous les pays membres de l'Union européenne, abrogeant la Directive 95/46/CE.

Cette présente étude est publiée le 18 mai 2017. Une année est déjà passée depuis la publication du règlement. Il reste 372 jours pour se mettre en conformité, sans oublier que cette période ne représente que 266 jours ouvrés.

Certains initient des réflexions, d'autres ont déjà formalisé un plan d'action et les plus proactifs optimisent déjà les processus métiers prenant en compte les impacts organisationnels auxquels ils sont confrontés.

Et vous, où en êtes-vous ?

Le règlement général sur la protection des données est aujourd'hui au cœur des préoccupations des entreprises. Les sanctions prévues par le règlement sont, pour un grand nombre d'entreprises, vues comme une véritable épée de Damoclès.

Au cours de nos missions, tant dans le secteur privé que dans le secteur public, deux questions nous sont posées de façon récurrente : comment doit-on organiser la gouvernance liées à la protection des données à caractère personnel ? Et par quoi devons-nous commencer ?

Ce sont ces deux questions qui ont été l'élément déclencheur à la rédaction de cette étude. Nous avons effectué plusieurs entretiens auprès de Data Protection Officers de grands groupes confrontés à ces deux questions.

Ces entretiens se décomposaient en deux parties. Une première traduite par une série de questions ouvertes concernant l'organisation du groupe, le ou les modèles organisationnels liés à protection des données mis en place, les modes de gouvernance adoptés, les différents choix d'animation du réseau interne, les impacts organisationnels qu'implique le règlement ainsi que les avantages et les inconvénients pour chacun de ces facteurs.

Par ailleurs, nous avons sollicités des organisations par le biais d'un questionnaire anonyme en ligne composé uniquement de questions fermées relatives aux actions effectuées ou pas dans le cadre de la mise en conformité au règlement.

Ce qu'il faut retenir c'est qu'il n'y a pas de schéma organisationnel de gouvernance bon ou mauvais. Quelle que soit l'organisation envisagée, elle devra tenir compte et répondre à des spécificités structurelles de l'organisme. Certains modèles pourront se cumuler pour répondre au mieux aux besoins d'un groupe avec un historique existant, alors que d'autres permettront a contrario d'initier une transformation nécessaire utilisant le Règlement Général de Protection des Données comme une opportunité d'optimiser l'organisation en place.

Sommaire

«Ce règlement ne souffre pas de retard. En mai 2018, la Cnil, les acteurs publics et privés devront être prêts pour le mettre en œuvre opérationnellement.

Pour les entreprises, la marche à monter est réelle, a reconnu la responsable qui présentait son rapport 2016, citant une étude récente selon laquelle moins de 10% d'entre elles pensent être prêtes à temps.

Le message numéro un que nous souhaitons passer aux entreprises, mais aussi aux acteurs publics, c'est qu'il faut absolument qu'ils se mettent en marche pour être prêts sur le règlement européen. »

Isabelle Falque-Pierrotin

Présidente du G29 (le groupe des Commissions nationales de l'information et des libertés européennes)
Présidente de la Commission Nationale Informatique et Libertés (CNIL)
et Conseiller d'État

LA VOIE DU NORD, publié le 27 mars 2017

Introduction

Par Jérôme Deroulez

Avocat au Barreau de Paris (ancien membre de la représentation française auprès de l'UE à Bruxelles).

Alors que le règlement européen sur la protection des données personnelles (RGPD) doit entrer en vigueur le 25 mai 2018, de nombreuses questions se posent toujours sur ses conséquences et les mutations engendrées par ce texte de grande ampleur.

Un des signes de la complexité du texte adopté le 27 avril 2016 est le délai de plus d'un an laissé par le législateur européen aux autorités de contrôle, aux opérateurs et aux entreprises pour s'adapter à cette nouvelle législation européenne. Délai d'un an marqué depuis par de nombreux rapports et contributions des opérateurs concernés comme par des avis du G29[1], le groupe rassemblant les autorités de contrôle européennes dont la CNIL. Marqué également par une jurisprudence offensive de la Cour de Justice de l'Union européenne pour faire respecter le droit à la protection des données personnelles, droit fondamental en Europe et qui doit faire l'objet de mécanismes de protection adéquats.

Ce nouveau règlement européen donne des outils et fixe des objectifs précis en matière de protection des données personnelles. Si la ligne d'horizon est sans équivoque et constituée des grands principes du règlement (traitement licite, loyal et transparent, durée de conservation encadrée, consentement, etc.), le texte n'en appelle pas moins à une refonte de la façon dont les entreprises collectent, stockent et conservent des données personnelles, dans une logique de conformité à ces nouveaux dispositifs.

Pour les entreprises concernées, le changement d'optique opéré par le règlement par rapport à la directive 95/46 doit interpeller. À une logique de déclarations et de formalités administratives est substituée une logique de responsabilisation, d'*accountability* et de sanctions renforcées.

Cette nouvelle philosophie n'est pas neutre et induit des conséquences redoutables puisque le niveau des sanctions peut être modulé en fonctions des mesures éventuellement prises ou non par une entreprise pour éviter ou anticiper un risque de violation de données ou coopérer en amont avec une autorité de contrôle. En l'absence de telles mesures, le montant des sanctions prononcées pourra être revu à la hausse.

Une entreprise ou un opérateur peuvent-ils cependant se passer d'une politique spécifique de « protection des données personnelles » ou d'une réflexion sur la façon dont ils traitent, stockent ou analysent de telles données ?

La question peut être posée : plutôt que de mettre en place une politique dédiée, coûteuse en temps et en ressources internes, pourquoi ne pas attendre encore et évoluer en fonction des positions qui seront prises ultérieurement par les autorités de contrôle ? Pourquoi ne pas provisionner de tels risques ou d'éventuelles sanctions et en tenir compte en fonction d'une logique qui serait avant tout comptable ?

Cette approche nous semble dangereuse et à plus d'un titre. En effet, comme indiqué plus haut, le droit à la protection des données personnelles est aujourd'hui un droit fondamental au sein de l'Union européenne et la Cour de Luxembourg se montre particulièrement soucieuse d'en assurer l'effectivité. On supposera facilement qu'elle se montrera tout aussi attentive dans la mise en œuvre du règlement à l'échelle du marché intérieur.

Par ailleurs les conséquences d'un constat de violations de données pour une entreprise ne seront pas seulement liées aux sanctions infligées par une autorité telle que la CNIL et en l'espèce financières.

Au-delà de la charge financière causée par ces sanctions, l'effet sur la réputation pourra être tout aussi dommageable et ce d'autant plus pour des entreprises qui collecteraient des volumes importants de données. Et que dire, dans des circonstances où le défaut de vigilance ou d'anticipation serait relevé ?

Crise de réputation, effet sur l'image de l'entreprise, conséquences sur ses relations avec ses clients ou ses utilisateurs, effets sur son utilisation des réseaux sociaux, les répliques d'une telle sanction pourront s'étendre bien au-delà de

[1] *Le G29 est un groupe de travail réunissant l'ensemble des CNIL européennes. Il a pour objectif de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays hors UE et de conseiller la Commission européenne sur tout projet ayant une incidence la protection des données et des libertés des personnes.*

la seule logique financière et surtout être particulièrement dommageables sur le long terme. En témoignent aujourd'hui le buzz crée par la simple modification des conditions d'utilisation de certains réseaux sociaux : quid en cas de sanction et de mise en évidence de violations répétées ou non anticipées ? Que faire aussi lorsqu'il s'agit de données sensibles ou que l'entreprise n'a pas su réagir à temps, faute de circuits de décisions adaptés, à rebours de toutes les exigences du règlement ?

Au vu de ces éléments, il importe de plaider une nouvelle fois pour la mise en place réfléchie et anticipée de ce règlement, dans une approche ouverte et constructive vis-à-vis d'un environnement de plus en plus sensible à ces enjeux. Mise en place qui est sans nul doute un atout à terme et un avantage compétitif.

Plus qu'un catalogue d'obligations nouvelles, ce règlement incite également les entreprises à mettre en place une gouvernance dans la gestion de leurs données personnelles et à entrer dans un cercle vertueux, tant en interne que vis-à-vis de leurs clients ou de leurs utilisateurs.

Ce règlement incite les entreprises à mettre en place une gouvernance dans la gestion de leurs données personnelles et à entrer dans un cercle vertueux.

De plus, les politiques menées en matière de protection des données n'ont pas non plus vocation à être circonscrites à cette seule matière mais plutôt à être incluses dans des chapitres plus généraux de la vie des entreprises et notamment en matière de *compliance* ou de sécurité (PSSI). A ce titre, la protection des données constitue un des volets illustrant le respect ou non par une entreprise ou une entité de ses obligations et engagements.

Répondre à ces engagements implique la mise en place de modes de gouvernance spécifiques et adaptés à chaque entreprise, en fonction de leur activité, de leur structuration ou leurs logiques intra-groupes.

Comme l'indique la présente étude, **quatre grands schémas d'organisation peuvent être proposés** (modèle hiérarchique, modèle en réseau, modèle avec autorité centrale ou modèle avec un DPO mutualisé).

Si chaque modèle possède ses propres avantages et inconvénients et doit être adapté en fonction des spécificités propres à chaque organisation. Certaines questions transverses doivent aussi être prises en compte.

À ce titre, l'identification des schémas de responsabilité dans le cadre des grands groupes doit faire l'objet d'un suivi attentif.

Le règlement n'évoque pas directement cette question sinon à travers celles de la responsabilité du responsable de traitement (article 24), des responsables conjoints de traitement, de leurs représentants et de leurs relations avec des sous-traitants.

Le règlement insiste ainsi sur la responsabilité du responsable de traitement (considérant 74) et sur la nécessité d'une répartition claire des responsabilités (cons. 79), notamment entre responsable et sous-traitant. Le règlement n'a pas vocation à se pencher sur les éventuelles règles nationales en matière de responsabilité (civile voire pénale) mais appelle à des clarifications et à une identification sans équivoque.

Par ailleurs, le rôle central qui doit être joué par le (ou les) Data Protection Officer (DPO) conformément aux articles 37 et suivants du règlement, doit aussi inciter les entreprises à repenser leur organisation pour garantir son indépendance.

Cette question de la responsabilité doit faire l'objet d'un examen précis au regard de l'organisation de chaque entreprise et de leurs relations avec leur environnement.

Ainsi de l'examen des clauses particulières dans les contrats avec les sous-traitants, de l'attention spécifique à apporter aux contrats internationaux voire des limitations apportées par le règlement à la liberté de sous-traiter. De la même façon, pour les clauses en matière de responsabilité ou des délégations de pouvoir accordées dans le cas des filiales : là encore, les chaînes de responsabilité doivent pouvoir être clairement identifiées.

Les enjeux de protection des données personnelles impliquent donc des questions en termes de gouvernance et de responsabilité, pour mettre en place des chaînes de décision efficaces et réactives, à même de garantir la sécurité des données et de susciter un environnement protecteur des usagers et des clients.

Devez vous nommer un DPO ?

Dans le cadre du RGPD, il est obligatoire pour certains organismes de désigner un DPO.

Article 37 du RDPD « Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 »

Le RGPD ne donne pas de définition précise des entreprises concernées, mais le groupe de travail européen G29 précise les points suivants :

- Toutes les organisations publiques sont concernées par le règlement, ainsi que tous les organismes privés exerçant des fonctions sous le contrôle de l'autorité publique ou des fonctions de service public (transport, etc.).
- Sont concernés également les organismes dont les données personnelles sont utilisées pour la réalisation de leur cœur d'activité. Cela inclus les fonctions supports nécessaires au fonctionnement de l'activité (données RH par exemple).
- La désignation d'un DPO est obligatoire pour les organismes qui effectuent le traitement des données à caractère personnel à grande échelle. Cette notion de grande échelle reste à évaluer en fonction du nombre de personnes concernées, du volume de données, de la durée ou de la permanence des traitements et de l'étendue géographique de l'activité de traitement.
- Les entreprises qui exercent de la surveillance régulière et systématique. Cela comprend notamment toutes formes de suivi et de profilage sur Internet et le suivi régulier des activités d'une personne (services de télécommunication, profilage clients à des fins d'évaluation des risques, suivi de localisation, suivi des données de bien être, etc.).

Ne sont pas concernés par le RGPD, les données personnelles de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat.

Quoi qu'il en soit – à moins qu'il soit évident que l'organisme n'est pas tenu de désigner un DPO – le G29 recommande que **le responsable de traitement réalise une analyse interne afin de déterminer si un DPO doit ou non être nommé. Cette analyse doit faire partie de la documentation en vertu du principe de la responsabilité.**

Rappel du rôle et de la fonction du DPO selon la réglementation

Le Data Protection Officer (DPO), traduit par la CNIL comme le délégué à la protection des données, n'est ni un « Chief Compliance Officer », ni un auditeur. Il a un rôle bien précis dans le processus de la compliance d'un organisme :

- Un rôle de conseil et d'information (article 39) vis-à-vis du responsable de traitement, des employés sur leurs droits et obligations.
- Un rôle d'interlocuteur privilégié des personnes concernées par les traitements à caractère personnel. Ses coordonnées doivent être fournies aux personnes quand leurs données sont collectées (articles 13 et 14).
- Un rôle de contrôle du respect du RGPD et du cadre légal applicable (article 39). Il doit collecter les informations sur les traitements. Il doit analyser et contrôler le respect des dispositions en matière de protection des données pour tous ces traitements. Ce contrôle ne fait pas de lui la personne responsable des manquements. C'est toujours le responsable de traitement (à savoir le responsable de l'organisme) qui est légalement responsable en cas d'infraction.
- Un rôle de sensibilisation et de formation des collaborateurs sur les bonnes pratiques en termes de protection des données personnelles.
- Un rôle de conseil lors des analyses d'impact. Il est en charge d'identifier la nécessité ou non d'effectuer une analyse d'impact. Il est le garant de la méthodologie utilisée. Il s'assure de leur réalisation et des conclusions. Enfin, il doit s'assurer que les mesures définies sont bien appliquées.
- Un rôle d'interface avec les autorités de contrôle. Il les consulte en cas de traitement présentant un risque élevé pour les personnes concernées. Il notifie ces mêmes autorités en cas de violation des données à caractère personnel. Il est l'interlocuteur privilégié en cas de contrôle ou de sollicitation de l'autorité de contrôle.

Le délégué à la protection des données hérite entra autres des missions historiquement assumées par le Correspondant Informatique et Libertés depuis sa création en 2004. Il devra reporter directement au responsable de traitement mais ce dernier ne doit en aucun cas donner des instructions en ce qui concerne l'exercice des missions (Article 38-3).

Il ne devra pas être dans une position où il pourrait déterminer les finalités / les moyens d'un traitement ou être en charge de la réalisation des mesures de sécurité. Il va donc s'appuyer sur un réseau de partenaires au sein de son organisme : la DSI, le RSSI, le juridique, les équipes de risques ou d'audit interne. Ces interlocuteurs doivent apporter leur support, leur expertise, leur analyse et leurs informations pour assurer la compliance au nouveau règlement.

De tous les freins ralentissant la mise en œuvre du RGPD, le choix du mode d'organisation doit être levé en premier

Pour mesurer le niveau d'avancement des organisations en matière d'application du RGPD, nous avons mené une enquête par le biais d'un questionnaire en ligne.

Plus de 40 entreprises hexagonales ont répondu de manière anonyme, de secteurs et de tailles variées.

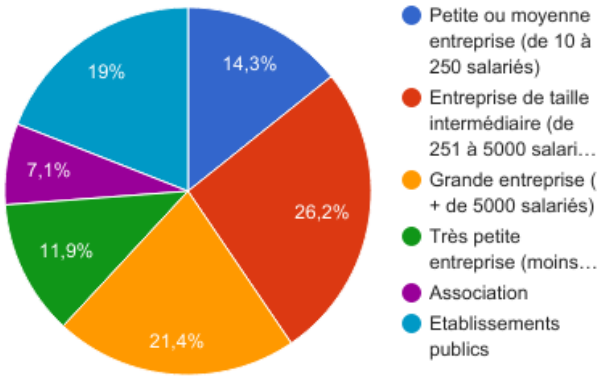


Figure 1 : Répartition du panel de l'enquête en ligne

Les entreprises sont désormais sensibilisées à l'importance du RGPD et à la nouvelle fonction de DPO

Une grande majorité d'entreprises, tous secteurs et tailles confondus, confirment que la conformité au RGPD est perçue comme un chantier majeur compris par leur direction générale. On le comprend aisément au regard des nouveaux enjeux financiers qui découlent des sanctions possibles.

Parmi notre panel, la majorité de nos interlocuteurs (83%) ont déjà réalisé les démarches de sensibilisation auprès de leurs dirigeants.

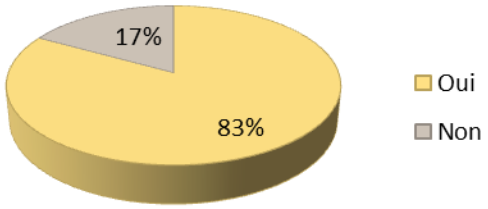


Figure 2 : Avez-vous informé les décideurs sur les changements à venir ?

Depuis deux ans nous évangélisons régulièrement nos clients, sur les problématiques de RGPD que ce soit au cours de nos séminaires ou au cours de nos missions. Nous avons vu une évolution dans les prises de conscience. Cette prise de conscience est particulièrement forte dans les organismes dotés d'un CIL ou d'un RSSI, dont le travail de veille a permis d'alerter leurs équipes dirigeantes. Pour les autres – à quasiment un an de l'application du RGPD – la prise de conscience de l'ampleur du chantier progresse significativement. L'étape de la prise de conscience nous semble désormais franchie.

La fonction de DPO est perçue comme une des mesures incontournables pour se mettre en conformité. 86% des entreprises envisagent la mise en place de cette fonction. Ce constat n'est pas une surprise. À l'inverse de l'actuel chargé de protection des données (CIL) dont la nomination est facultative, la réglementation rend obligatoire sa nomination dans trois cas, comme évoqué précédemment. Le texte vise expressément l'obligation de création d'un poste pour toutes les autorités ou organismes publics, les « activités consistant en des opérations de traitement qui […] exigent un suivi régulier et systématique à grande échelle des personnes concernées » et enfin les activités manipulant des catégories particulières de données. Pour ces dernières, le texte donne des exemples non exhaustifs comme les données de santé, raciales ou religieuses, d'autres pourraient venir se rajouter au travers des actes délégués au niveau national.

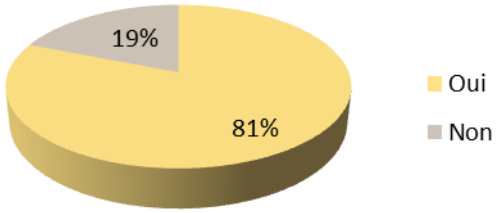


Figure 3 : Nommerez-vous un "Data Protection Officer" ou une personne en charge ?

Par ailleurs, selon le baromètre de l'AFCDP[2], le rôle et la fonction du DPO sont relativement bien maitrisés par les organismes (68% des cas), même si 23% de leur panel déclarent n'avoir qu'une connaissance partielle de ses missions et que beaucoup de zones d'ombres subsistent pour 7%.

Malgré cette prise de conscience, le degré d'avancement de la mise en œuvre de la conformité est encore réduit

Dans une démarche de mise en conformité au RGPD, de nombreuses thématiques sont à étudier, notamment :

- La cartographie des données et des traitements gérés au sein de l'organisme ;
- La politique de confidentialité ;
- L'information aux personnes concernées au moment de la collecte des consentements ;
- Les modalités d'exercice des droits des personnes et plus spécifiquement la demande d'accès aux données personnelles ;
- La gestion des consentements et la gestion des spécificités relatives aux mineurs ;
- La gestion des contrats vis-à-vis des sous-traitants.

Le panel de notre enquête a conscience que, si des réflexions ont été initiées, les mises en œuvre restent encore loin d'être l'actualité pour les équipes projet en charge du RGPD. En effet 73% des organismes déclarent que les différents points abordés dans l'étude ne sont pas opérationnels.

Les équipes semblent majoritairement au stade du travail de cartographie des données personnelles et des traitements au sein de l'organisme.

Cette phase consiste à Identifier clairement les données personnelles gérées, d'où elles proviennent, avec qui elles ont été partagées et d'identifier les traitements de données associés. Cette cartographie indispensable pour comprendre les enjeux propres à son organisme est réalisée selon notre panel à **73% en termes de données**. En revanche **au niveau des traitements**, la démarche est nettement moins avancée puisque seulement **47%** de notre panel a effectué ce travail de documentation. Ces résultats encourageant peuvent s'expliquer en France par les démarches déclaratives auprès de la CNIL et les démarches des directions informatiques en termes d'urbanisme.

[2] *Association Française des Correspondants à la protection des Données à caractère Personnel*

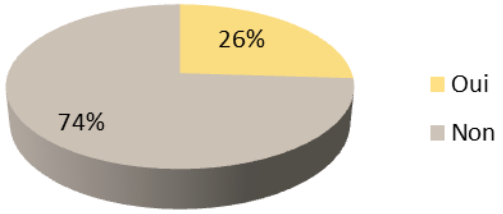


Figure 4 : Avez-vous déjà mis en place les changements nécessaires pour être en conformité RGPD ?

Selon le résultat de notre enquête, il est clair que la plupart des sujets restent encore à défricher :

	Oui	Non
Avez-vous évalué votre **politique de confidentialité** existante et planifiez les changements nécessaires en vue du RGPD ?	**57,10%**	42,90%
Envisagez-vous d'organiser une vérification des **processus d'information** liée aux traitements ?	**81%**	19%
Avez-vous documenté vos **traitements** ?	47%	53%
Avez-vous vérifié si les procédures en cours dans votre organisation, fournissent tous les **droits accordés** par le RGPD à la personne concernée ?	47,60%	**52,40%**
Avez-vous mis à jour vos procédures d'accès existantes et réfléchi à la façon dont vous allez traiter les **demandes d'accès** ultérieures en vertu des nouvelles conditions RGPD ?	35,70%	**64,30%**
Avez-vous évalué votre façon de recueillir et d'enregistrer le **consentement** ?	50%	**50%**
Pour les entités (23,8% des sondés) concernées par le recueil de **consentement de mineur**, avez-vous développé des systèmes pour vérifier l'âge de la personne concernée et demandé le consentement des parents ou des tuteurs lors du traitement des données personnelles des mineurs ?	25,9%	**74,1%**
Avez-vous évalué vos **contrats** existants - principalement avec les **fournisseurs** et **sous-traitants** ?	31%	**69%**
Avez-vous déterminé qui est votre **autorité** de protection des données de surveillance si votre organisation est active dans plusieurs juridictions ?	50%	**50%**
Avez-vous prévu des procédures adéquates pour détecter, signaler et enquêter sur les **violations de données** personnelles ?	50%	**50%**

Figure 5 : Degré d'avancement dans la prise en compte du RGPD

Les organismes n'ayant pas fini les travaux préparatoires d'état des lieux, il est difficile de tirer des conclusions sur leur capacité à être conforme au RGPD à la date d'échéance du 25 mai 2018. Selon le baromètre de l'AFCDP, seulement 19% des organismes estiment qu'ils seront conformes le 25 mai, 44% sont plutôt d'avis qu'elles ne seront pas totalement conformes et 33% estiment qu'elles ne seront pas en conformité du tout. Ces métriques montrent en soi un faible niveau dans la préparation du RGPD.

Les freins se situent essentiellement au niveau de l'organisation

Une difficulté importante se situe dans l'organisation même de la mise en place de la fonction de DPO. Selon notre panel, seulement 47% arrive à se projeter dans l'organisation à mettre en place, son rattachement, comment la fonction interagira avec les autres acteurs de la protection des données.

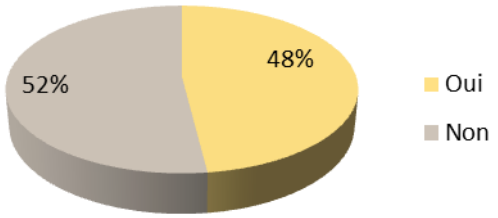


Figure 6 : Avez-vous déjà défini comment cette personne fonctionnera ?

Si pour identifier les impacts et établir la feuille de route il est préférable de travailler dans un mode collégial au sein de l'organisme, la coopération, pour ne pas dire parfois la compétition, entre des directions de différents types, engendre une certaine confusion sur la manière d'organiser la fonction de DPO. En effet, celle-ci empiète sur plusieurs domaines fonctionnels qui avaient jusque-là l'habitude de fonctionner en silos.

Le projet de conformité suscite un intérêt naturel auprès des CIL, RSSI, des directions juridiques, des directions informatiques et des directions des risques qui sont souvent en première ligne sur ces sujets. Mais l'on voit aussi des directions plus opérationnelles en charge de traitements de données à caractère personnel comme les équipes digitales, marketing ou RH s'en préoccuper fortement.

Dans ces conditions, mettre en place une organisation pour cadrer la coopération et les responsabilités de ces différents acteurs n'est pas simple. Il est nécessaire qu'un porteur du projet de mise en conformité au RGPD soit nommé pour être en mesure d'orchestrer tous les chantiers de la conformité. Et celui-ci n'est pas obligatoirement ou nécessairement votre futur DPO.

Ceci n'est naturellement pas le seul frein. Le texte du RGPD doit encore être précisé. Les membres du G29 travaillent à la publication de démarches sur des sujets majeurs. Nous sommes encore en attente des avis des autorités de contrôle sur des points importants. Par ailleurs, les principes de protection des données dès la conception (privacy by design) et les dispositifs techniques renforçant la vie privée (Privacy Enhancing Technologies) ne sont pas simples à cerner. Ces sujets nécessitent des réflexions collectives. En revanche, la réponse à la question « quelle organisation mettre en place ? » ne pourra être résolue qu'à l'échelle de chaque entité. C'est pourquoi nous avons choisi de traiter en priorité le sujet de l'organisation de la fonction de DPO dans cette étude.

Que devez-vous avoir à l'esprit pour construire votre organisation ?

Avant de construire son organisation liée à la fonction DPO, il est nécessaire de prendre du recul sur votre organisme, notamment en termes de culture, d'existant et de gestion du risque. Vous pouvez notamment, vous inspirer des recommandations des autorités de contrôle et des groupes de travail européens, tel que le G29.

Un modèle organisationnel impacte les acteurs en charge de la problématique I&L. Les postures et les compétences des profils évoluent avec le RGPD et il est nécessaire de bien comprendre les acteurs en jeu et leurs rôles.

Enfin, quel que soit le modèle, nous avons pu faire certains constats qu'il faut bien avoir à l'esprit au moment de la construction de votre organisation.

La position de la Commission Nationale de l'Informatique et des Libertés

Selon Albine Vincent, Cheffe du service des CIL au sein de la CNIL interviewée par le site internet cyberrisques.com le 9 janvier 2017.

« A chaque organisation correspond une histoire et une culture. Le positionnement de la fonction de DPO doit en tenir compte pour être efficace.

Il est donc difficile de livrer le positionnement d'un DPO de façon générale. Il faut qu'il soit reconnu et légitime dans la culture de l'entreprise. Un rattachement à un secrétariat général peut être une piste.

Les CIL sont actuellement issus des formations techniques mais dans les entreprises anglo-saxonnes à dimension internationale, ces mêmes postes sont positionnés au niveau du juridique par exemple.

La fonction de DPO nécessite d'être aussi un bon communicant qui sait aussi convaincre. Il faut savoir oser pousser des portes. Il doit aussi montrer les bénéfices d'une gestion intelligente des traitements et des données pour l'entreprise.

Pour ce qui concerne l' « accountability » ce pilotage des données à termes peut être bénéfique pour l'image des entreprises. En outre, la sensibilisation de l'ensemble des utilisateurs aux bénéfices d'une mise en conformité peut et doit déclencher de nouveaux réflexes. »

Le 15 mars 2017, la CNIL a publié une méthodologie en 6 étapes pour se préparer et anticiper les changements liés à l'entrée en application du règlement européen. La démarche proposée par la CNIL a vocation à accompagner les professionnels et à leur apporter une sécurité juridique à la hauteur des attentes du nouveau cadre règlementaire.

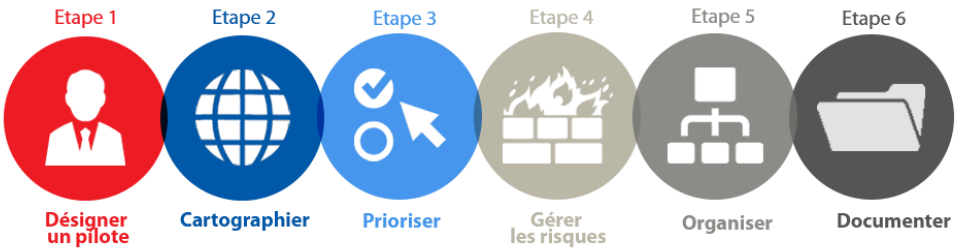


Figure 7 : La démarche de conformité RGPD en 6 étapes

Comme nous pouvons le constater la première étape présente la désignation d'un pilote comme un prérequis. Pour les entreprises, les grands groupes ou les organismes publics n'ayant pas opté pour la fonction de Correspondant Informatique et Libertés dans les années passées, le choix du bon profil pour endosser la fonction de Data Protection Officer peut être difficile. En effet, cela nécessite d'avoir une vision claire sur le schéma organisationnel de gouvernance qui sera mis en place.

Les acteurs de la gouvernance Informatique et Libertés

Nous vous présentons dans un premier temps les différents acteurs qui pourront être présents dans les différentes structures de gouvernance.

Le Chief Privacy Officer (CPO)

Véritable chef d'orchestre du groupe, il est en charge de définir et d'assurer la cohérence des directives ou de la politique du groupe. Il peut également accompagner les DPO dans la mise en œuvre de la politique. Il est responsable des Privacy Officers dans le cas où il dirige un service.

Ce type de profil a généralement des compétences juridiques, organisationnelles, en management et techniques. Il endosse un vrai rôle politique au niveau Groupe et participe aux comités exécutifs et aux comités de direction.

Le Data Protection Officer (DPO)

Chef d'orchestre au sein de son entité, il assure la conformité des organismes ou des pays dont il a la charge au regard de la politique du groupe.

Ce type de profil a également des compétences juridiques, organisationnelles, en management et techniques. Il endosse un rôle politique au sein de son entité et participe également aux comités exécutifs et aux comités de direction de son entité.

Le Privacy Officer (PO)

Il assiste le CPO dans au sein du Privacy Office pour définir et assurer les directives ou la politique du groupe. Il est également en mesure d'assister un DPO sur des sujets précis dans lesquels il aurait une expertise spécifique.

Ce type de profil a généralement des compétences juridiques et/ou techniques ou dans un domaine métier spécifique (santé, sécurité, marketing, etc.).

Le Référent Informatique et Libertés (RIL)

Sa mission consiste dans un premier temps à identifier les nouveaux traitements au sein des projets métiers afin qu'ils puissent être qualifiés par le DPO puis à remonter les informations permettant d'effectuer le suivi des traitements.

Il est également un relais entre son entité / direction et le DPO :

- Relais descendant : il diffuse dans son entité / direction les bonnes pratiques I&L et les procédures à respecter.
- Relais ascendant : il remonte au DPO les questions, les difficultés rencontrées ou les spécificités locales (exemple : réglementation spécifique à un métier ou à un pays, contraintes métier en conflit avec les exigences I&L, etc.).

Le RIL exerce sa mission sur le long terme mais il s'agit d'actions ponctuelles. Cette fonction – contrairement aux différents profils présentés précédemment – ne nécessite pas un poste à temps plein.

Pour qu'un RIL apporte une réelle valeur ajoutée, il doit avoir une appétence pour les sujets de protection des données et maitriser les procédures et les dispositifs métiers impactés par la protection des données au sein de son entité et ou de son groupe.

Les invariants ou les contraintes inhérentes au schéma organisationnel que vous mettrez en place

Lors de l'analyse des différents schémas organisationnels de gouvernance Informatique et Libertés, nous avons constaté que plusieurs éléments étaient indépendants du modèle d'organisation choisi. En effet, quel que soit le schéma observé, un grand nombre de facteurs que nous pourrions considérer comme fondamentaux ne changent pas.

Responsabilité et autonomie

Quel que soit le modèle organisationnel, les DPO ne sont pas personnellement responsables en cas de non-respect du RGPD. Le RGPD indique clairement que cette responsabilité revient au responsable de traitement. Ce dernier confie cette mission au DPO mais en conserve la responsabilité. Il est donc tenu de s'assurer que le DPO dispose des moyens nécessaires pour réaliser cette mission, à savoir une autonomie dans l'organisme et des ressources suffisantes pour mener à bien cette tâche.

Il s'agit donc d'une délégation de responsabilité qu'il faut bien distinguer du transfert de responsabilité. Nommer un DPO n'offre pas une sécurité juridique incontestable mais permet de pallier le risque.

Néanmoins, en cas de contrôle ou de litige, le DPO est en première ligne et doit démontrer que les actions qu'il a menées sont en conformité avec le RGPD. Il est donc garant de la protection des données personnelles du pays ou des entités dont il a la charge. Cela implique qu'il a le devoir de faire valoir son opinion dissidente lorsque les décisions du responsable de traitement sont incompatibles avec le RGPD.

Une ambition proportionnelle à la responsabilité endossée.

Pour un responsable de traitement, endosser la responsabilité lui permet d'imposer ses ambitions, une politique de protection des données et de rassurer les différentes filiales lors de projets « data ».

En fonction de l'importance de la responsabilité (et donc des risques), l'organisme s'orientera vers un modèle organisationnel plutôt qu'un autre. En cas de risques forts, il peut par exemple vouloir conserver le leadership de la holding sur ses filiales ou au contraire maitriser le risque par le biais d'un DPO dans chaque filiale, pour assurer une proximité de terrain.

Responsabilité du Groupe ou des entités ?

Aucune décision de justice ne permet actuellement d'appréhender avec certitude de quelle manière la responsabilité d'une holding pourrait être mise en cause en cas de non-conformité d'une de ses filiales.

Un des éléments auquel il faut s'attacher est le contrôle financier d'une holding sur ses filiales. **E**n effet, en cas de contrôle financier de la holding sur les filiales, la responsabilité sera indéniablement remontée en cas de manquement d'une des filiales.

Soutien de la direction et implication dans les instances de pilotage

Ce que nous pouvons également noter c'est que l'ensemble des politiques de protection des données des entreprises bénéficient toujours du soutien de la direction générale.

De plus, nous pouvons observer que le Data Protection Officer est impliqué dans l'ensemble des instances de pilotage, comité de projet, comité de pilotage, comité de direction ou comité exécutif à l'exception du DPO mutualisé qui se limite aux deux dernières instances citées.

Niveaux d'acteurs fonctionnels ou hiérarchiques

Nous avons constaté qu'il y a toujours au moins deux niveaux d'acteurs permettant l'identification, la qualification ou le suivi d'un traitement. Lorsque la conformité est assurée par un service dédié ou par DPO mutualisé, un réseau de Référent Informatique et Libertés est toujours présent et organisé.

L'audit et le contrôle de la conformité dans le temps sont présents dans tous les modèles

Quel que soit le modèle de gouvernance mis en place la conformité Informatique et Libertés fait également toujours l'objet d'audits internes.

Quel rattachement et quel profil ?

Concernant le rattachement des personnes en charge du sujet, il n'y a pas de règle ou constat permettant de déduire une pratique répandue. Certains sont rattachés à la direction juridique, à la direction des risques, au secrétariat général ou encore à la direction générale.

De même, les profils des Data Protection Officers rencontrés sont hétérogènes. Nous retrouvons des juristes, des responsables de la sécurité des systèmes d'information, des responsables du risque, des informaticiens et des chefs de projet.

Retenons les leçons de la fonction RSSI

Par Marc-Eric Trioullier

Directeur de la pratique système d'information au sein du Cabinet Infhotep

Comment organiser la fonction RSSI au sein de mon organisme ? À qui doit-il être rattaché ? Ces questions sont inusables depuis plus de dix ans. Force est de constater qu'il n'existe pas de réponse unique dans les pratiques des organismes qu'ils soient publics ou privés. Et nous faisons le pari que la création de la fonction du DPO suscitera le même genre de débat dans les dix ans à venir. D'ailleurs, la fonction CIL qui en principe devait être rattachée au responsable de traitement, tout comme le DPO, est très souvent rattachée à un département/service informatique ou juridique. Alors examinons ce qui s'est fait au niveau des RSSI pour réfléchir à la position du DPO dans nos organismes demain…

Selon l'étude du Clusif « Menaces informatiques et pratiques de sécurité en France » de 2016, la fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI) est identifiée et attribuée dans 67% des entreprises françaises. On retrouve là un ratio similaire d'intention de création du poste de DPO.

Les freins

Au cours de cette enquête les principaux **freins** à la mission du RSSI sont « le manque de budget » (42%) et les « contraintes organisationnelles ». En sera-t-il de même pour la fonction de DPO ?

Les risques financiers dues aux sanctions (20 millions d'euros ou 4 % du chiffre d'affaire mondial annuel de l'organisme si cette seconde valeur est supérieure) sont nettement plus mesurables et visibles. Les entreprises alloueront peut-être des budgets en conséquence.

Le problème organisationnel peut être posé de la manière suivante : certains RSSI n'ont aucun pouvoir ou levier sur les équipes et les pratiques qu'ils auditent. Ils sont dans une posture de conseil, qualité avec un faible sponsoring managérial, rendant très faible la probabilité de voir aboutir un de leurs projets. Le problème se posera à l'identique pour notre Délégué à la protection des données personnelles.

Le rattachement

La problématique du **rattachement** du DPO au juridique, à la DSI, au département des risques et conformité, à la direction générale, se posent au sein de tous les organismes. Les réponses seront multiples comme pour le RSSI. En 2016, la fonction RSSI est soit rattachée à la direction des systèmes d'information (42% contre 46% en 2014), soit à la direction générale (30% contre 27% en 2014) ou en troisième position à la direction administrative et financière (DAF) (7%), à la direction des risques (2%), à la direction de l'audit et contrôle interne (1%). Elle est donc le plus souvent perdue quelque part dans les organigrammes. Ceci s'explique, selon nous, par un niveau de maturité à la sécurité relativement moyen voir faible au sein des organismes. De plus, une proportion importante du panel est constituée d'organismes entre 200 ou 500 salariés (66% équivalent à la répartition des entreprises en France) où le nombre d'acteurs pouvant prendre en charge les aspects sécurité est plus réduit. Ce rattachement majoritaire à la DSI, pose une réelle question en termes d'indépendance et en termes de capacité d'arbitrage. Le RSSI se trouve dans une posture de juge et parti. Il doit appliquer les consignes de son management alors même qu'il est censé les contrôler. Par ce biais, la fonction RSSI en est souvent tronquée la cantonnant dans une posture de maitre d'œuvre plus que comme la maitrise d'ouvrage de la sécurité d'un organisme.

Cet indicateur statistique ne permet pas de mettre en lumière l'inventivité des entreprises pour pallier cela. En effet, dans certains grands groupes ou administrations, la fonction RSSI est rattachée administrativement à la DSI sans en dépendre fonctionnellement. Et dans ce cas, le rattachement peut être porté par la direction du risque ou le directeur qui dirige la DSI, un DGA, un directeur des fonctions supports, en évitant le lien hiérarchique.

La taille de l'équipe

L'autre interrogation que nous abordons implicitement dans cette étude est la taille de l'équipe en charge de la protection de données personnelles. Le Clusif dans son étude de 2016 indique que la fonction de RSSI est pris en charge à temps plein dans 76% des organismes. Dans 46% des cas c'est une personne seule ou un binôme qui porte la fonction. Dans 21 % des cas cette fonction est prise en charge par 3 ou 5 personnes. Seulement 20% des RSSI exercent d'autres

fonctions au sein de leur organisme. On retrouve majoritairement une approche centralisée de la fonction s'appuyant sur un réseau de partenaire. Pour les organisations comportant des filiales, on retrouve des interlocuteurs comme référent sécurité voir des RSSI locaux (en fonction de la taille de l'organisme).

Selon nous, la question des organisations de ces fonctions transversales est un faux débat. Le positionnement de ces fonctions transversales reste et restera dépendant de la culture même de l'entreprise et de l'importance que l'on porte à cet enjeu. Il faut miser sur la personnalité, les compétences, le professionnalisme et la capacité de ces acteurs (DPO, RSSI) à créer leur réseau de partenaires et de soutiens dans l'entreprise pour faire aboutir les projets.

L'important se situe aussi dans la lettre de mission et l'implication de la direction générale. En effet, ces postes nécessitent une prise de responsabilité, de l'autonomie, des moyens et un fort sponsoring ou un pouvoir reconnu pour imposer des mesures, des pratiques dans les équipes. Idéalement, il faut répartir les responsabilités, inciter chaque acteur à s'impliquer dans la réussite de ses projets (création d'indicateur de pilotage, critères de management, etc.) et favoriser la diffusion, le partage du savoir et des bonnes pratiques.

Les modèles d'organisation possibles

L'objectif de cette étude est d'analyser les différents schémas organisationnels en se posant les questions suivantes :

- Quels sont les rôles des différents acteurs et les profils les plus adaptés ?
- Quel est le périmètre couvert par ces différents acteurs ?
- Quel positionnement du DPO dans l'organisation ? Doit-il exercer ses fonctions au sein du siège, dans chaque filiale ou dans chaque pays ?

Issu de nos interviews, quatre schémas organisationnels se profilent. Dans un premier temps nous les analyserons en étudiant les avantages et les inconvénients qu'ils impliquent. Ces différents schémas ne présupposent pas du rattachement hiérarchique des différents acteurs à une direction particulière. Ils n'ont pas non plus vocation à être appliqués tel quel ; votre organisation cible peut être une combinaison de plusieurs schémas en fonction de la structure de votre Groupe.

Hierarchical Model

Un « Chief Privacy Officer » pour coordonner plusieurs « Data Protection Officer ».

L'un des premiers schémas possibles est celui d'une organisation avec un « Data Protection Officer » par filiale, dirigée par un « Chief Privacy Officer » dont le rôle consiste à définir et assurer la cohérence des directives ou de la politique du groupe. Ce type d'organisation implique un lien hiérarchique entre le CPO et les différents DPO. L'externalisation totale de la fonction DPO n'est pas identifiée comme modèle organisationnel pour les grands groupes qui conservent toujours la gouvernance de la PDP. Néanmoins, elle peut avoir lieu au niveau d'une ou plusieurs filiales.

Rôle du CPO

Le rôle du CPO est avant tout un rôle politique et hiérarchique

- Porter la politique PDP au niveau des instances dirigeantes
- Coopérer avec l'autorité de surveillance
- Définir la politique PDP Groupe et les directives associées
- Harmoniser les pratiques et les outils
- Auditer les entités du Groupe sur leur conformité RGPD et sur les règles du Groupe
- Manager l'équipe DPO
- Consolider les indicateurs PDP des différentes filiales et réaliser le rapport annuel PDP
- Apporter les moyens aux DPO pour réaliser leurs missions
- Conseiller, assister et apporter son expertise.

Rôle du DPO

Le DPO a un rôle fonctionnel dans l'entité à laquelle il est rattaché.

- Surveiller la conformité RGPD au niveau de son entité
- Identifier les spécificités locales (réglementation, gouvernance de la filiale, etc.)
- Appliquer et décliner les règles et les procédures du Groupe au niveau local
- Remonter les indicateurs PDP au CPO
- Réaliser les études d'impacts sur la vie privée (PIA)
- Tenir le registre de son entité
- Communiquer et former les personnels de son entité
- Conseiller et assister au niveau de son entité
- Participer aux comités décisionnels de son entité.

Les DPO sont rattachés à la holding et détachés à une filiale. En cas de cession ou d'acquisition d'une filiale, la gestion RH du DPO reviendra à la holding.

Les DPO ont un rôle fonctionnel vis-à-vis de l'entité à laquelle ils sont détachés. Cela présente l'avantage de préserver leur autonomie et leur indépendance vis-à-vis de la filiale mais peut être considéré par l'entité comme une contrainte et une surveillance de la part de la holding.

Pourquoi choisir ce modèle ?

Ce modèle convient aux organisations hiérarchiques qui souhaitent garder le contrôle sur les pratiques en matière de protection des données personnelles. Il peut également convenir aux organisations qui gèrent des données très sensibles et dont les risques en cas de non-conformité sont élevés.

Par ailleurs, cette organisation permet d'harmoniser les différentes pratiques du Groupe et garantit la cohérence des mesures organisationnelles et des dispositifs de protection des données.

Il permet également d'avancer sur un sujet simultanément dans les différentes filiales, de profiter des retours d'expérience de chacun et de mutualiser les pratiques et les analyses de risques.

Ce type d'organisation prend en compte les spécificités locales des entités par le détachement du Data Protection Officer qui reste autonome au sein de l'entité tout en respectant la politique du Groupe. Certains pourront couvrir une filiale, un pays ou encore se mutualiser sur un périmètre plus vaste. Dans le cas d'un Groupe international, chaque Data Protection Officer apportera son expertise sur la législation locale et sur les spécificités métiers.

Le lien hiérarchique garantit le bon fonctionnement de la gouvernance et permet de contrôler un avancement homogène des filiales et de leur assurer les moyens nécessaires à la réalisation de leurs missions.

Quels sont les points de vigilance ?

La principale difficulté de ce modèle réside dans le recrutement des DPO qui doivent avoir un niveau de compétence conforme aux exigences du RGDP. Les entreprises et les organismes publics ont souvent une organisation déjà en place avec des personnes en charge de la protection des données personnelles, parfois en plus de leur activité principale. Il s'agit donc d'identifier les profils susceptibles d'évoluer en DPO et de les faire monter en compétence, tant sur des aspects juridiques que techniques.

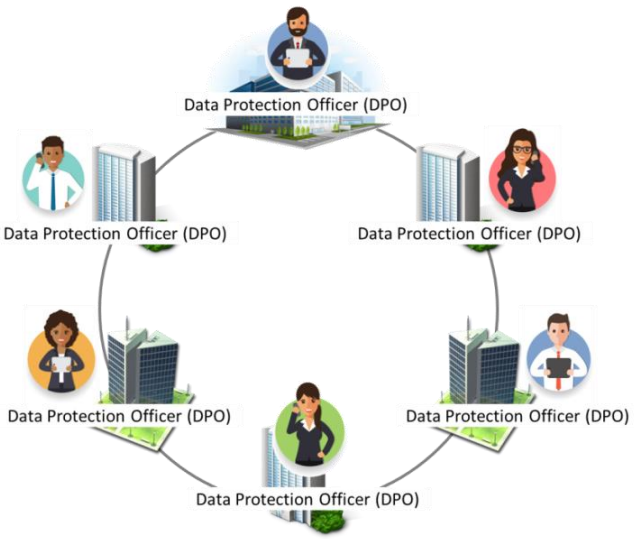
De même, dans ce modèle, les DPO doivent partager :

- une compréhension commune du RGPD et de la politique du Groupe.
- des outils mutualisés
- des méthodes et des pratiques

Si le DPO est autonome pour décliner les principes du Groupe au niveau de sa filiale, il n'a pas le pouvoir d'adapter le règlement ou les règles du Groupe.

Network Model

Un « Data Protection Officer » par entité du groupe



Le second schéma possible est celui d'une organisation avec un Data Protection Officer par entité, dont la holding.

Ils sont tous indépendants et travaillent collégialement à la sécurisation du groupe. Dans ce type d'organisation, il n'existe pas de lien hiérarchique. Chaque DPO est au même niveau.

La cohérence du Groupe sur la problématique I&L est basée sur la coopération et le partage entre les DPO.

Dans ce modèle, chaque DPO peut mettre en place sa propre organisation, en s'appuyant sur des référents informatiques et libertés (RIL) ou des experts métiers (RSSI, responsables métiers, etc.). Il possède ses propres moyens qu'il défend auprès de la direction générale de son entité.

Rôle de chacun des DPO

Le rôle du DPO est politique et opérationnel.

- Porter la politique PDP au niveau des instances dirigeantes
- Participer aux comités décisionnels de son entité.
- Coopérer avec l'autorité de surveillance
- Conseiller, assister et apporter son expertise auprès de son entité
- Surveiller la conformité RGPD au niveau de son entité
- Réaliser des études d'impacts sur la vie privée (PIA)
- Tenir le registre de son entité
- Communiquer et former les personnels de son entité
- Coopérer avec les autres DPO

Pourquoi choisir ce modèle ?

Ce modèle est privilégié pour les organisations où chaque entité est indépendante et autonome. Il peut s'agir des unions, des syndicats, des communautés d'agglomération, des opérateurs de l'état rattaché à un ministère, etc.

Ce modèle peut également être envisagé lorsque les entités d'un Groupe concernent des activités distinctes et spécifiques (exemple : groupes possédant plusieurs marques qui parfois peuvent être concurrentes sur un plan commercial).

L'avantage de cette organisation est l'agilité de chaque entité dans l'application des principes I&L en fonction de sa taille, de son organisation, de son activité, de ses spécificités légales, des données qu'elle traite, etc.

Quels sont les points de vigilance ?

Ce modèle pose inévitablement la question de la structure juridique du Groupe et des responsabilités entre les entités. Pour rappel, le RGPD prévoit des sanctions pouvant aller jusqu'à 4% du chiffre d'affaire mondial. Il est donc nécessaire d'étudier quels sont les risques pour le Groupe en cas de défaillance d'une entité.

Un autre risque majeur de ce modèle est l'hétérogénéité des pratiques, des outils et des niveaux de conformité en fonction des niveaux de compétence des DPO, de leur approche sur la protection des données personnelles, des moyens que lui alloue son entité et de l'écoute de ses dirigeants.

Chaque entité étant autonome, il n'y a pas de visibilité globale au niveau du Groupe qui permettrait de connaître le niveau de conformité global ou d'identifier les défaillances éventuelles d'une des entités.

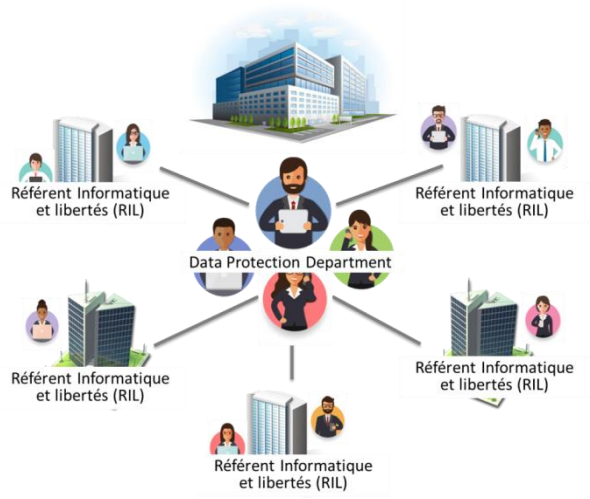
C’est pourquoi il est conseillé, autant que possible, que le contrôle interne effectue ou fasse effectuer des audits réguliers pour assurer un niveau d’exigence et de conformité homogène au sein du groupe.

De même, il est important qu’une collaboration étroite entre les DPO soit mise en place (à travers des instances par exemple, des outils de collaboration, etc.) afin de partager les pratiques, les retours d’expérience, les expertises spécifiques, les outils, voire définir des lignes de conduites communes.

Chaque DPO coopère avec l'autorité de surveillance et agit en tant que point de contact. Il y a autant de point de contact que de DPO.

Central Office Model

Un « Data Protection Department » pour l'ensemble du groupe.



Compte tenu de la taille et de la structure de l'organisation, il peut être nécessaire de mettre en place une équipe « Privacy ». Dans un tel cas, la structure interne de l'équipe, les tâches et les responsabilités de chacun des membres doivent être clairement définis.

Ce « Data Protection Department » accompagne la conformité de l'ensemble du Groupe, couvrant ainsi à la fois la gouvernance de la protection des données personnelles et l'application au niveau local.

Rôle du Chief Privacy Officer (CPO)

- Porter la politique PDP au niveau des instances dirigeantes
- Coopérer avec l'autorité de surveillance
- Définir la politique PDP Groupe et les directives associées
- Manager l'équipe DPD
- Consolider les indicateurs PDP des différentes filiales et réaliser le rapport annuel PDP
- Surveiller la conformité RGPD globale du groupe

Rôle du Privacy Officer (PO)

- Déployer la politique et les directives au niveau des filiales, notamment à travers le relais des RIL.
- Apporter une expertise technique, juridique et/ou métier
- Etudier les spécificités locales (culture, organisation, réglementation, etc.)
- Déployer les outils
- Communiquer et former
- Apporter conseil, assistance et expertise auprès des entités.
- Auditer les entités du Groupe
- Assister les RIL à la réalisation des études d'impacts et à la tenue du registre.
- Etc.

Rôle du Référent Informatique et liberté (RIL)

- Identifier les traitements
- Communiquer au sein de son entité
- Remonter les informations au Data Protection Department
- Réaliser les études d'impacts

Le CPO a un rôle hiérarchique sur les PO qui eux-mêmes ont un rôle fonctionnel sur les RIL.

Pourquoi choisir ce modèle ?

Ce modèle peut être utilisé pour des organisations de taille moyenne, par les sociétés faisant de la délégation de DPO (externalisation de la fonction) ou des organisations présentes sur le territoire européen exclusivement.

Ce type de schéma organisationnel n'est pas forcément le plus adapté pour un groupe international car il impliquera une importante veille juridique pour assurer la conformité des différentes législations. Néanmoins, il peut être déployé au niveau de certaines filiales, sur un territoire juridique cohérent.

Tout comme le modèle hiérarchique, ce modèle permet de poser une gouvernance globale et d'harmoniser les pratiques et les outils. Il permet également – à travers une équipe – de couvrir un champ de compétences élargi et prenant en compte les spécificités métiers de l'organisme (sauf si le Data Protection Department est externalisé).

Quels sont les points de vigilance ?

Le principal risque de ce modèle est le phénomène « tour d'ivoire » où les experts, concentrés au siège, manquent de pragmatisme et d'opérationnalité. Les spécificités locales en termes de culture, d'organisation, de contraintes métiers, de réglementations ne sont pas toujours facilement appréhendables lorsqu'on n'est pas sur le terrain.

Un des prérequis à ce modèle est de bien dimensionner l'équipe et d'identifier les ressources comprenant des compétences complémentaires au regard de la sensibilité et de la complexité des données traitées. En général, plus les opérations de traitement sont complexes et/ou sensibles, plus les ressources doivent être données au CPO.

Pour rappel, l'article 38 du RGPD exige que l'organisation prenne en charge cette fonction en « fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées ».

Enfin, l'animation du réseau de RIL est particulièrement sensible dans ce modèle car il permet d'accéder aux enjeux et aux contraintes locales pour un département qui en est éloigné. L'animation de ce réseau peut être chronophage et complexe. En effet, il s'agit de personnes ayant une activité principale autre avec des enjeux et des priorités différentes.

Shared DPO Model

Un « Data Protection Officer » mutualisé pour accompagner et assurer la conformité de plusieurs entités.

Le quatrième schéma que nous avons pu rencontrer est celui d'un unique « Data Protection Officer » pour l'ensemble de l'organisme ou mutualisé pour différentes filiales / entités / entreprises.

Il endosse l'ensemble des missions et représente le seul garant de la conformité de(s) organisation(s).

Rôle du DPO mutualisé

- Informer et conseiller le responsable du traitement, les salariés et les sous-traitants
- Contrôler le respect du règlement européen de protection des données personnelles
- Sensibiliser et former les différents acteurs concernés et impliqués
- Préparer aux audits
- Assister les responsables de traitement à la réalisation des PIA
- Coopérer avec l'autorité de contrôle
- Analyser le risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Pourquoi choisir ce modèle ?

Ce modèle convient à des organismes de taille moyenne ou des entreprises dont les données gérées sont peu sensibles. Il peut s'agir également d'un DPO mutualisé pour plusieurs organisations. On trouve le cas par exemple, dans certains grands groupes où plusieurs filiales mutualisent la fonction DPO au niveau d'un pays. Pour le secteur public, il peut s'agir d'une mutualisation de la fonction entre collectivités territoriales par exemple.

Quels sont les points de vigilance ?

Le nombre d'entités ou d'organismes pris en charge par le DPO doit être raisonnable afin qu'il puisse exercer correctement sa fonction. Pour rappel, le DPO n'est pas personnellement responsable en cas de non-respect du RGPD. C'est le responsable de traitement qui est tenu de démontrer que le traitement est effectué conformément à ses dispositions. De plus, le responsable de traitement a pour obligation de donner les moyens au DPO d'exercer sa fonction. Il est donc de sa responsabilité de vérifier que le DPO est en capacité d'assurer sa fonction.

Par ailleurs, ce modèle implique que le DPO ait toutes les compétences requises pour exercer ces fonctions, qu'elles soient techniques ou juridiques.

Conclusion

Connaitre son organisme, sa culture, son histoire, les femmes et les hommes qu'il regroupe est un prérequis à la définition de son organisation. La gouvernance liée au poste de DPO en termes de protection des données ou plus généralement en termes de gouvernance de l'information doit répondre aux enjeux stratégiques de son organisme et doit être accompagné de mesures à la hauteur des ambitions.

Beaucoup se posent la question de la responsabilité. Pour un grand groupe qui endosse la responsabilité globale des traitements de ses filiales, il est important de formaliser et d'imposer une politique de protection des données personnelles. Si le terme de patrimoine informationnel fait écho à vos actifs d'entreprise, c'est qu'il représente une richesse, un capital pour vous. Vous vous devez alors de le maitriser, de le protéger et de le sécuriser. Les données à caractère personnel en font partie. Elles doivent donc être gérées à la mesure de leur importance pour vous, vos clients, vos usagers, vos collaborateurs, etc.

Quel que soit le modèle d'organisation, il conviendra d'être en mesure de prouver que des mesures ont été mises en œuvre pour assurer la protection des données à tous les niveaux de l'organisme. Provisionner le risque et effectuer le minimum vital pour garantir une situation de conformité ne permettra pas de répondre à la logique d'auto régulation et d'accountability introduite par le Règlement Général de Protection des Données.

Ce dernier a justement été élaboré et réfléchi pour que de telles stratégies ne puissent plus exister. La reconnaissance juridique du Privacy by Design, la protection des données dès la conception en est un exemple probant. La protection des données personnelles doit être anticipée en amont ; les entreprises se devront d'être proactives et non plus réactives. Les études d'impact de la vie privée participent à la mise en œuvre de cette proactivité.

De notre enquête, nous confirmons que les entreprises et les organismes publics sont en train de se mettre en ordre de marche et de s'organiser pour se mettre en conformité. La volonté de créer une fonction DPO en est un signe annonciateur fort.

Il est important d'avoir conscience que le travail à venir sera long et ne se fera pas d'un simple claquement de doigt ou par la signature d'un contrat avec une société de DPO externe. Si l'on se réfère à l'expérience des conformités au Référentiel Général de Sécurité (RGS) et à la Politique de sécurité du système d'information de l'Etat (PSSIE) dans les organismes publics, la conformité s'obtient par un savant mélange de formalisme, de sensibilisation et d'actions opérationnelles. Ce travail n'a de sens que s'il s'inscrit dans la durée et se fond dans les pratiques opérationnelles de l'entreprise.

Pour les organismes, il est important selon nous d'être en mesure de démontrer en mai 2018 **que la feuille de route a été clairement définie** et que **des équipes sont en charge** de la problématique au sein de l'organisme. Des mesures « à minima » devront avoir été réalisées, telles que :

- Les traitements actuels sont en conformité avec les attentes de la CNIL ;
- Une démarche de gouvernance a été mise en place ;
- Le référencement des traitements doit être réalisé avec les mécaniques de maintien en condition opérationnelle définies voir en place (révision des démarches projet) ;
- La démarche d'analyse des risques sur la protection de la vie privée (PIA) a été formalisée ;
- Une sensibilisation des équipes a été effectuée.

Il faut voir dans cette obligation réglementaire une réelle opportunité et une chance pour les responsables de la protection des données personnelles de faire avancer la culture Informatique et Libertés au sein de leur organisation et d'avoir une meilleure écoute des instances dirigeantes.

À propos du cabinet Infhotep

Depuis plus de 10 ans, les consultants du cabinet Infhotep accompagnent les entreprises privées et publiques dans leur transformation technologique, organisationnelle et culturelle. Nos domaines d'expertise sont le système d'information, le management du capital humain et la gouvernance de l'information. En 2017, nous créons Infhotep R&D, filiale entièrement dédiée à la recherche et à l'innovation dans le cadre de la transformation de notre métier de conseil qui s'oriente vers le consultant augmenté.

CHIFFRES CLES

Créé en 2005
20 salariés
2,7 M€ de CA en 2016

Notre démarche

« Des hommes, des process, des outils », c'est le slogan que le cabinet Infhotep met en avant dans ses missions quotidiennes de transformation numériques auprès de ses grands clients.

Le cabinet apporte à ses clients une vision et une assistance globale qui se déclinent dans l'élaboration, le pilotage et la déclinaison opérationnelle de la stratégie avec en sous-jacent le « *change* » qui impacte le capital humain de l'entreprise.

Doté de consultants expérimentés issus du monde de l'entreprise et du conseil, le cabinet Infhotep a pour objectif de permettre à ses clients d'atteindre leurs résultats dans une approche efficace, rationnelle et pragmatique. Le travail des consultants est renforcé par des boites à outils et des *best practices* qui renforcent l'efficacité du consultant Infhotep dans ses missions.

Le positionnement et la force de frappe du cabinet Infhotep reposent sur des valeurs fortes telles que l'excellence, l'indépendance, la pédagogie, l'humanisme et le pragmatisme. Avec cette volonté affichée de proposer une équipe unie par une forte culture d'entreprise et des valeurs partagées, le cabinet Infhotep garantit à ses clients un travail réalisé avec déontologie, confiance, confidentialité et engagement. Ce travail en commun avec ses clients permet un atterrissage concret des projets.

Conseil

L'objectif de nos prestations de conseil est de rendre nos clients autonomes dans la gestion de leur projet. Elles visent à rapprocher les enjeux métiers et organisationnels du système d'information et à rendre opérationnelles les ambitions de ses clients.

Outils

Au cours des missions de conseil, le cabinet conçoit des outils au bénéfice de ses clients :

- Logiciels
- Modèles de données
- Modèles de connaissances
- Documents types

Formations

Infhotep est un organisme de formation agréé. Nous réalisons des formations en intra et en inter sur tous nos métiers.

Nos références

Au-delà des compétences et de l'expérience de ses consultants, le savoir-faire et la force du cabinet reposent sur les missions effectuées pour des clients, tels que :

À propos des auteurs

Alessandro FIORENTINO est consultant au sein de la pratique Système d'information du cabinet, en charge de l'activité Informatique et Libertés. Il commencé sa carrière en tant qu'analyste-programmeur. Il a par la suite assumé la fonction d'architecte des systèmes d'information au sein d'un grand groupe de courtiers en gestion de patrimoine. Titulaire d'un Mastère spécialisé en Management et Protection des données à caractère personnel de l'Institut Supérieur d'Electronique de Paris (ISEP), il a soutenu une thèse professionnelle relative à la mise en œuvre du Privacy by Design. Ambassadeur du Privacy by Design depuis mai 2013, il accompagne les entreprises dans le développement de projets intégrant les principes de protection de la vie privée dès la conception.

Jérome DEROULEZ est avocat au Barreau de Paris. Ancien magistrat, il a exercé les fonctions de juge d'instruction. Il a ensuite été en charge de négociations européennes et internationales pour le ministère de la Justice. Conseiller au sein de la Représentation permanente de la France à Bruxelles de 2009 à 2013, Jérôme Deroulez a participé aux négociations de textes européens et d'accords internationaux dans le domaine de la protection des données personnelles, du droit international privé et de la coopération judiciaire pénale. Il a également acquis une connaissance précise de l'administration publique française. Jérôme Deroulez est membre de l'Association des Avocats Lobbyistes et de l'incubateur du Barreau de Paris.

Marc-Eric TRIOULIER conseille depuis dix-sept ans les grands comptes du secteur privé et public dans l'évolution de leur système d'information sur les aspects techniques, fonctionnels et organisationnels. Responsable de la pratique Systèmes d'Information au sein du Cabinet Infhotep, il coordonne également l'ensemble de l'offre sécurité au sein du cabinet et anime le séminaire du cabinet sur le plan de continuité d'activité. Marc-Eric est co-auteur de l'ouvrage : « Sécurité des architectures Web » paru chez Dunod (ISBN : 2100073540). Marc-Eric Trioullier est titulaire d'un Master de Méthodes Informatiques Appliquées à la Gestion des Entreprises et d'un DESS Ingénierie Réseau et Système.

Aude DE MONTGOLFIER travaille depuis quinze ans dans le domaine du management des informations, des stratégies d'organisation et de fonctionnement documentaires. Elle possède une réelle expertise tant dans le domaine privé que dans le domaine public, à travers des missions précédemment réalisées ou en cours de réalisation. Au sein du cabinet Infhotep, elle porte la practice sur la gouvernance de l'information.

Pour échanger sur des points qui sont détaillés dans notre étude :
« Data Protection Officer
Quel schéma organisationnel de gouvernance
Informatique et Libertés? »
N'hésitez pas à nous contacter :
contact@infhotep.com

Nous tenons à remercier l'ensemble des consultants du cabinet Infhotep pour leurs retours d'expériences aussi divers qu'enrichissants. Plus particulièrement, nous remercions Claude Guéant pour ses remarques et ses relectures avisées.

www.infhotep.com
demain.infhotep.com