MÉTIERS D'AVENIR

DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

Octobre 2018
Le Forem - Veille, analyse et prospective du marché de l'emploi

DÉLÉGUÉ À LA PROTECTION DES DONNÉES, UN MÉTIER D'AVENIR ?

Pour beaucoup, aujourd'hui, engager un *délégué à la protection des données*, ou DPO, consiste avant tout à se conformer au Règlement Général sur la Protection des Données à caractère personnel (RGPD). Or, à y regarder de plus près, recruter un DPO c'est l'occasion de rentrer pleinement dans l'économie digitalisée et de développer une véritable gouvernance des données dans son organisation. Loin de l'image d'un « contrôleur pinailleur », le DPO devient un influenceur inspirant, définitivement orienté vers l'avenir.

Au regard de l'importance que prennent les données comme actifs dans l'économie, le *délégué à la protection des données*, plus connu sous son acronyme anglais DPO[1], joue un rôle central dans la gouvernance des données de l'entreprise, en assurant de manière spécifique la protection des données à caractère personnel. À cet égard, les quelque 2.400 DPO enregistrés en Belgique[2] exercent un métier d'avenir, même si d'aucuns y voient plutôt une fonction ou un rôle dans l'entreprise plutôt qu'un métier.

Les missions du DPO requièrent de celui qui les remplit de développer de multiples compétences dans le domaine informatique, celui du droit ou encore de la communication et de la gestion. L'objectif du présent rapport réside dans l'identification de ces compétences après avoir exploré les grandes évolutions auxquelles devra faire face le DPO endéans les trois à cinq ans.

Conformément à l'esprit de la prospective stratégique dans lequel le futur n'est pas déterminé mais reste à construire, les experts réunis lors de ces ateliers ont adopté une posture délibérément volontariste plaçant le DPO au cœur de la montée en maturité des entreprises dans le traitement de leurs données tout en restant dans le périmètre de la protection des données personnelles. Il en résulte un profil de DPO complexe, veillant tout autant à assurer la conformité des traitements à la législation en vigueur, et développant une « culture de la donnée » dans son organisation, voire au-delà.

Anticiper les évolutions, l'émergence ou la transformation de métiers constitue un axe majeur de la mission d'analyse et d'information sur le marché du travail du Forem. Une première étude exploratoire réalisée en 2013[3] a permis de dégager les grandes tendances d'évolution des secteurs. En 2016, Le Forem poursuit sa démarche en publiant des rapports sur les effets de la transition numérique sur les secteurs en

TABLE DES MATIÈRES

[1] DPO = Data Protection Officer.
[2] Les entreprises doivent enregistrer leur DPO auprès de l'Autorité de Protection des Données. En juin 2018, ils étaient au nombre de 2.377.
[3] Le Forem, Métiers d'avenir pour la Wallonie, septembre 2013, téléchargeable sur https://www.leforem.be/chiffres-et-analyses/prospectives.html.

termes d'activités, métiers et compétences[4]. Des métiers d'avenir sont ainsi identifiés. Ils peuvent être de natures différentes. Il peut s'agir de :

- nouveaux métiers ;
- métiers actuels dont les contenus évoluent ;
- métiers avec un potentiel de croissance en effectifs.

Partant de cette base, une analyse en profondeur, « métier par métier » est mise en œuvre. Elle permet de mieux en cerner les évolutions et d'adapter, après l'analyse de grands domaines de transformation attendus, l'offre de prestation. C'est dans ce cadre que s'inscrit le présent rapport.

Cette analyse prospective se fonde sur la méthode *Abilitic2Perform.* Il s'agit d'une méthode d'anticipation des compétences basée sur l'animation de groupes d'experts lors d'ateliers successifs. Elle s'inspire des études relatives à la prospective stratégique[5], dont certains outils sont mobilisés comme l'analyse structurelle ou morphologique. D'abord développée dans le cadre d'un projet européen Interreg IV, elle a ensuite été déployée plus largement dans le cadre des travaux prospectifs du Forem sur plusieurs dizaines de métiers[6].

Ce rapport comprend deux parties. La première présente une synthèse des résultats reprenant l'ensemble du profil d'évolution et les activités clés pour l'avenir.

La seconde reprend dans le détail l'ensemble du processus d'analyse dans l'ordre chronologique de son déroulement. Le lecteur y retrouvera notamment des recommandations sur les compétences pointées comme importantes par les experts pour la réalisation des activités clés.

[4] Une série de rapports sectoriels sont publiés dans la rubrique « Métier d'Avenir 4.0 – La transition numérique », téléchargeables sur https://www.leforem.be/chiffres-et-analyses/metiers-d-avenir-transition-numerique.html.

[5] Voir notamment, Godet M., Manuel de Prospective stratégique - Tome 1 : *Une indiscipline intellectuelle*, Paris, Dunod, 2007 et Godet M., Manuel de Prospective stratégique - Tome 2 : L'art et la méthode, Paris, Dunod, 2007.

[6] Chaque analyse par métier a fait l'objet d'un rapport consultable sur le site du Forem via le lien : https://www.leforem.be/chiffres-et-analyses/metiers-d-avenir-prospectives-abilitic2perform.html.

Partie 1 - Synthèse des résultats

Au cœur de la transformation numérique des entreprises, le DPO ne doit plus seulement être un analyste juridique doublé d'un connaisseur des systèmes d'information. Il doit également contribuer au développement d'une véritable culture d'entreprise qui intègre autant le potentiel des données que l'éthique nécessaire à leur traitement.

Mai 2018, le Règlement Général européen sur la Protection des Données est entré en application. Ce texte renforce et unifie la protection des données personnelles pour les individus au sein de l'Union européenne. Parmi les mesures phares, figure la désignation d'un « *délégué à la protection des données* », un DPO. Il s'agit d'une obligation pour toute autorité publique ou entreprise privée dont les activités de base les amènent à réaliser un suivi systématique et régulier des personnes à grande échelle ou à traiter des données dites « sensibles ». Selon l'Autorité de Protection des Données, la Belgique comptait 2.377 DPO en juin 2018. Il convient de garder à l'esprit que si seules certaines entreprises sont tenues de désigner un DPO, toutes doivent se conformer aux règlementations en matière de données à caractère personnel. Certaines entreprises y consacrent d'ailleurs des ressources humaines sans les nommer « DPO », en utilisant par exemple l'appellation « GDPR manager ». Certains constats du présent rapport s'adressent également à ces professionnels.

La réglementation européenne précise quatre missions du DPO :

- Informer et conseiller le responsable de traitement des données à caractère personnel ou le sous-traitant.
- Contrôler, « monitorer », le respect des règlements dans le domaine de la protection des données à caractère personnel.
- Dispenser des conseils sur demande en ce qui concerne l'analyse d'impact, soit l'analyse préalable à la mise en place d'un nouveau traitement afin d'identifier a priori les risques encourus et les mesures à prendre.
- Coopérer avec l'autorité de contrôle et faire office de point de contact avec celle-ci.

Deux missions peuvent être ajoutées à ces dernières. La première concerne la relation avec les personnes concernées[7] qui figure en filigrane dans les textes de référence. La deuxième est introduite à la demande expresse des experts participants et concerne l'appui à l'entreprise que devrait apporter le DPO dans la montée en maturité en matière de gestion des données personnelles et plus généralement en matière de gouvernance de données[8].

C'est d'ailleurs cette dernière mission qui apparaîtra comme particulièrement impactée par les grandes évolutions attendues, devant les missions de contrôle du respect des normes et de conseil auprès du responsable de traitement en général, et spécifiquement dans le cadre de l'analyse d'impact. Ces évolutions peuvent, pour la plupart, être classées en deux grandes catégories : l'une technologique, l'autre juridique.

Parmi les évolutions d'ordre technologique, la digitalisation des entreprises apparaît comme la plus influente. Ce facteur doit être compris comme la transformation des processus de production de biens ou services basés sur la technologie numérique et la donnée. Le rythme et le niveau de digitalisation des entreprises dépend de la culture de l'innovation qui y règne. Dans les trois à cinq ans, cette dernière devrait encore se développer de manière différenciée selon les secteurs, la sensibilité du management ou encore la taille de l'établissement. De nombreuses entreprises utilisent encore des outils inadaptés et moins performants dans la gestion de leurs données (par exemple n'utilisent pas d'outils de gestion intégrée). Toutefois l'évolution sociologique, dont l'apparition de *digital native* dans l'entreprise, devrait accélérer la digitalisation. Dans ce contexte, afin de venir en appui de l'entreprise dans sa montée en maturité en matière de gouvernance des données, le DPO devra être capable de

[7] Les personnes concernées sont celles dont les données personnelles sont retenues. C'est au DPO que ces personnes s'adressent pour récupérer leurs données par exemple.

[8] La gouvernance des données correspond à l'ensemble des organisations et des procédures mises en place au sein d'une entreprise afin d'encadrer la collecte de données, leur traitement, leur utilisation ou encore leur valorisation. Elle repose sur des règles, un financement, une distribution des rôles et responsabilités, … Si le DPO peut contribuer, favoriser, stimuler la mise en place de la gouvernance des données, il ne peut en être responsable. Le professionnel responsable de la gouvernance des données est en général le « Chief Data Officer ».

mobiliser les membres de l'organisation et les sensibiliser aux enjeux liés à la donnée. Développer un discours en faveur de l'innovation et l'adapter selon les interlocuteurs, parmi lesquels le comité de direction. Il devra en outre disposer de connaissances dans le domaine de la gestion du changement ou en organisation des entreprises et pouvoir l'analyser et diagnostiquer les problèmes liés à la gouvernance des données.

De la maturité en matière de digitalisation de l'entreprise, dépendront également les compétences nécessaires à la mission de conseil relatif à l'analyse d'impact. Cette analyse de risque sera, pour le DPO, l'occasion de développer dans l'entreprise une culture du risque liée à la donnée, qu'il devra au préalable comprendre, et dont il devra maîtriser les méthodes d'analyse. Il devra être apte, sur base d'une analyse tant juridique que stratégique de conseiller le responsable de traitement des données dans l'arbitrage entre les intérêts de l'entreprise et ceux des personnes concernées. Cela demande en outre, au DPO, un certain degré d'empathie envers ces dernières.

L'intelligence artificielle (IA) et le développement du « big data » sur laquelle elle repose, est un enjeu majeur pour le DPO. Selon les experts, la formation d'un écosystème en Wallonie autour des technologies IA en faciliterait l'exploitation par les PME dans les années à venir. Les solutions IA seraient de plus en plus accessibles, notamment au travers de services externalisés de type « AIaaS » (Artificial Intelligence as a Service). Outre une veille juridique en vue d'alimenter la rédaction de politiques internes aux entreprises, le DPO devra disposer de compétences techniques afin de comprendre les répercussions de l'intelligence artificielle sur la gestion des données à caractère personnel. Il devra notamment comprendre les enjeux liés au « profiling », soit la combinaison de données collectées dans différentes sources pour établir des profils de comportement des personnes en matière de consommation, d'opinion, … Il devra être sensible aux processus de *désanonymisation* potentiellement à l'œuvre : le croisement automatisé de données anonymisées peut permettre dans certains cas l'identification des personnes concernées et entrer par conséquent dans le périmètre du RGPD. Le DPO développera une approche éthique de la donnée et comprendra les principes de marquage des données, soit les métadonnées informant des traitements autorisés sur les données. L'intelligence artificielle, comme toutes technologies liées aux données, obligera le DPO à entretenir une réflexion constante sur l'évolution du métier. Pour ce faire, il conviendra au DPO de s'intégrer dans un réseau et d'échanger avec ses pairs.

Le développement de l'internet des objets aura également un impact sur l'activité du DPO. Ce développement, qui devrait se produire dans un cadre réglementaire plus sécurisé (la sécurité des nouveaux objets connectés devrait être certifiée), générera de nouveaux processus producteurs de données potentiellement personnelles. L'effet sur les besoins en compétences se rapproche de ceux pointés précédemment dans le paragraphe consacré à l'intelligence artificielle, les deux technologies étant intimement liées.

Mi-technologique, mi-juridique, le déploiement, éventuellement obligatoire, de l'*open data* nécessitera du DPO qu'il comprenne la cartographie des données et les outils utilisés par les professionnels de l'informatique tels que les analystes ou les architectes. Toutefois, les experts nuancent le déploiement de l'*open data*. À moyen terme, rendre les données exploitables et disponibles sera encore considéré comme un coût. Loin du paradigme de *« l'open data by default »*, les autorités publiques ouvriront leurs données uniquement sur demande et ne feront pas la promotion des possibilités existantes. L'ouverture des données pourrait se développer davantage dans certains secteurs comme la santé, l'énergie ou encore la mobilité. Toutefois, de manière globale, les experts s'attendent à ce que des freins subsistent en raison d'un retard de numérisation et à des difficultés liées au format ou à la fiabilité des données.

La raison d'être du DPO étant d'assurer la conformité des traitements des données à caractère personnel avec les différentes règlementations en la matière, la diversité et l'évolution de ces dernières constituent un enjeu majeur.

Dans trois ou cinq ans, les réglementations, notamment internationales, devraient rester morcelées, multiples et générer un certain flou juridique. Chaque État devrait persister à conserver ses propres données et s'assurer une certaine autonomie. La donnée pourrait devenir à l'avenir une « arme stratégique », faisant de la géolocalisation des données un enjeu im-

portant et du « hosting » de données un véritable business[9]. La directive européenne *E-privacy*[10] actuellement en préparation pourrait ainsi s'ajouter au RGPD et avoir un impact important sur l'*e-marketing*.

Outre la diversité des textes, le DPO devra faire face à leur évolution. Les réglementations en matière de vie privée évoluent constamment. Même si les experts s'attendent à l'avenir à ce que la communication de ces changements se fasse correctement laissant aux entreprises le temps de s'adapter, le suivi et les mises à jour des textes législatifs et des *guidelines* constituent un challenge important pour les DPO.

L'évolution de la jurisprudence mérite également d'être prise en compte par le DPO. En particulier celle relative aux fonctions réputées incompatibles avec celle de DPO. Cette liste évolue « au cas par cas » et plutôt sous forme de recommandations.

Dans ce contexte où les textes se multiplient et évoluent, le DPO devra assurer une veille juridique, y compris des textes internationaux (éventuellement rédigés en anglais) ou des normes de qualité privées (ex : ISO 27001) et un suivi des bonnes pratiques en fréquentant par exemple des cercles DPO ou des groupes sectoriels. Il devra également être doté d'une bonne capacité d'analyse, tant organisationnelle (mécanismes et politiques internes de transfert de données, audit des organisations) que juridique (conflit entre RGPD et autres législations, impact des différents textes sur l'activité de l'entreprise, …). Enfin le DPO devra se montrer apte à réagir aux évolutions règlementaires, à en organiser la traçabilité et un suivi. Il devra être capable d'alerter les directions quand une législation a un impact sur l'activité, d'établir un tableau de bord des actions mises en œuvre pour être en conformité avec les différentes réglementations, ou encore collecter et stocker les preuves des démarches entreprises. La rigueur apparait alors comme la qualité première du DPO.

Les deux derniers facteurs sont difficilement classables dans la catégorie technique ou juridique. Le premier concerne la politique de contrôle adoptée par l'Autorité de Protection des Données (APD [11]). À moyen terme, les experts s'attendent à ce que l'APD continue à disposer de peu de moyen, menant peu de contrôle et de manière sectorielle. Des sanctions seront probablement prises pour servir d'exemples. Par ailleurs les plaintes ne devraient pas être nombreuses.

Enfin un dernier facteur a trait quant à lui au retour d'expérience après quelques années de RGPD. Dans trois à cinq ans, des échanges de bonnes pratiques devraient se développer sous différentes formes. Plutôt sectoriels, ces échanges seront davantage accessibles aux grandes entreprises qu'aux PME. En outre, de nouveaux services payants pourraient voir le jour comme des certifications ISO ou des assurances. Les retours d'expériences s'avèrent essentiels à l'évolution du métier, c'est pourquoi le DPO ne devra pas hésiter à échanger avec ses pairs et s'inscrire dans des cercles ou groupements de DPO.

Finalement, le présent travail invite à situer le DPO dans un cadre plus large que celui des missions strictement mentionnées dans les textes de référence. L'originalité de l'étude réside dans l'ancrage du métier dans un contexte non seulement en évolution tant au niveau technologique que juridique, mais surtout marqué par un manque de maturité des organisations dans le domaine de la donnée. En plus de prendre conscience de la valeur des données, et donc de l'intérêt de les exploiter et de les protéger, ce qui ne relève pas de la fonction de DPO, les entreprises et autres organismes doivent adopter une approche éthique de la donnée intégrant au cœur de leur traitement le respect du caractère privé des données personnelles. Les y aider constitue peut-être le défi le plus important que doit relever le DPO, seul ou en équipe.

---

[9] Pour illustrer le caractère stratégique que peut prendre l'hébergement de données, mentionnons la loi fédérale russe N 242-FZ qui oblige les organismes étrangers à stocker les données personnelles des ressortissants russes sur le territoire russe (voir : http://www.cil.cnrs.fr/CIL/spip.php?article2751).

[10] *E-privacy* est le nom donné à la Proposition de règlement du parlement européen et du conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »). Elle concerne notamment la politique de cookies. Selon une enquête de Deloitte, *ePrivacy* pourrait ainsi être responsable de la chute de 30 % des revenus de la presse nationale à l'horizon 2020 (cité dans l'article d'Europe 1 *Quel est ce projet "ePrivacy" qui fait polémique ?* du 8 mars 2018 (http://www.europe1.fr/societe/quel-est-ce-projet-eprivacy-qui-fait-polemique-3594062).

[11] Chaque pays membre doit se doter d'une autorité responsable du respect du RGPD sur le territoire, notamment habilitée à appliquer des sanctions financières en cas de non-respect. En Belgique, ce rôle est joué par l'ancienne Commission pour la Protection de la Vie Privée, rebaptisée « Autorité de Protection des Données ».

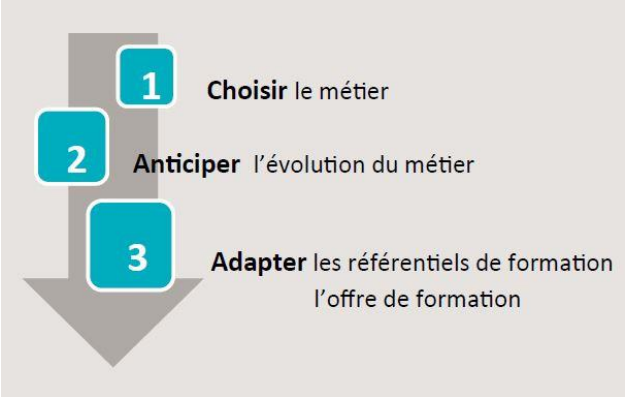
Partie 2 - La démarche et les résultats pas à pas

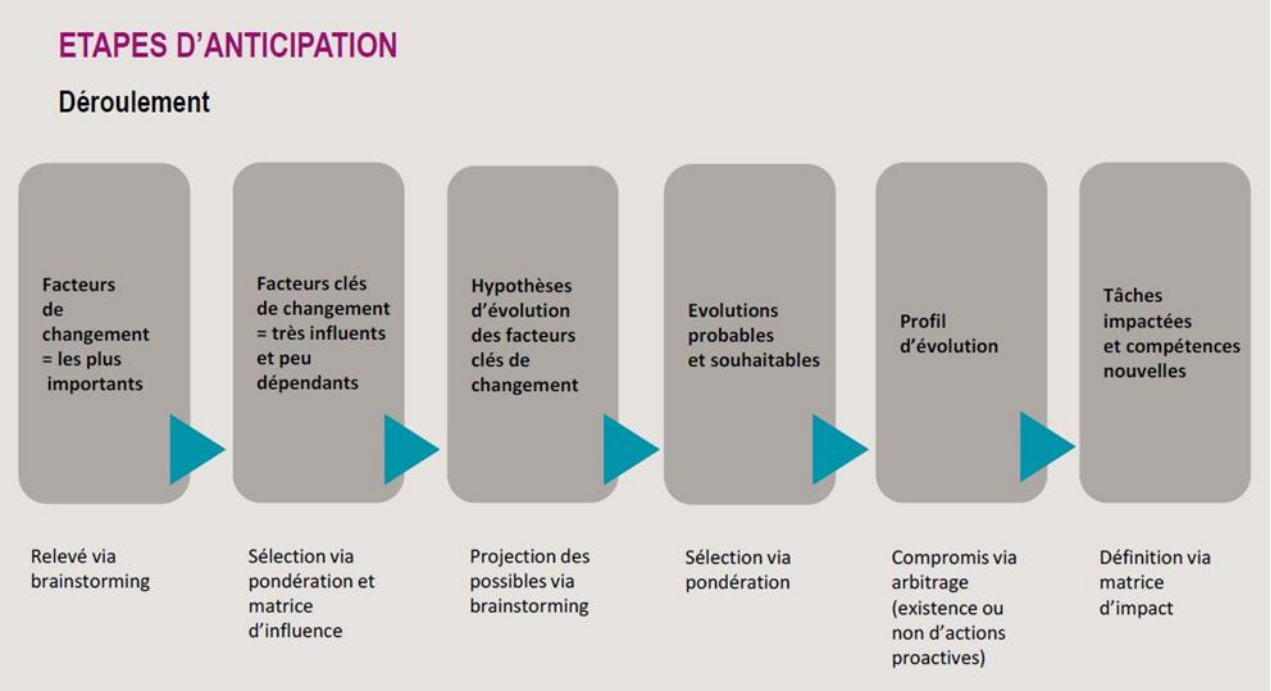
Cette partie du document décrit l'ensemble du processus suivi dans le cadre du déploiement de la méthode *Abilitic2Perform* appliquée au *délégué à la protection des données.*

La démarche se base sur la participation d'un panel d'experts à une série d'ateliers encadrés par un animateur qui conduit les réunions.

La méthode alterne, d'une part, des phases de réflexions créatives et collectives de type brainstorming et, d'autre part, des phases individuelles destinées à noter la pertinence ou l'impact des idées précédemment émises. Le traitement de ces notes par l'animateur permet d'objectiver les éléments récoltés. Les résultats obtenus au terme de chaque phase servent de matière première à la phase suivante.

Trois grandes étapes doivent être parcourues : choisir un métier, anticiper les évolutions et leurs impacts sur le métier, puis adapter les prestations. Le présent rapport se focalise essentiellement sur la deuxième phase consacrée à l'anticipation.





Les ateliers ont rassemblé une dizaine de personnes issues de différents milieux : académiques, services publics, entreprises privées de services informatiques ou de consultance, centres de compétence, opérateurs de formation et Le Forem (cf. le colophon).

Le métier de *délégué à la protection des données* a été sélectionné pour faire l'objet d'un exercice détaillé d'anticipation en raison de l'enjeu grandissant du respect du caractère privé des données personnelles, consacré par la législation européenne, dans une économie où les données occupent une place centrale dans la production de richesse.

La suite du document reprend étape par étape, la procédure d'analyse :

1. Le périmètre du métier
2. Les facteurs les plus importants
3. La sélection des facteurs les plus influents
4. Les évolutions probables et souhaitables et profil d'évolution
5. Les impacts sur les activités et les besoins en compétences

1. LE PÉRIMÈTRE DU MÉTIER

RGPD, le texte fondateur

Le 25 mai 2018, le Règlement Général relatif à la Protection des Données à caractère personnel (RGPD) entrait en application. Ce texte renforce et unifie la protection des données personnelles des individus au sein de l'Union européenne. Cette règlementation s'applique à toutes les entreprises tant publiques que privées à qui elle impose de prendre des mesures afin de garantir cette protection. Toutefois certaines entreprises[12] sont tenues à une obligation additionnelle : désigner un *délégué à la protection des données*, connu également sous l'acronyme anglosaxon « DPO » (Data Protection Officer). Le *délégué à la protection des données* contrôle les traitements de données au sein de son organisation ou de celle pour laquelle il est mandaté. Les *délégués à la protection des données* doivent s'enregistrer auprès de l'autorité de contrôle[13] : ils étaient 2.377 à l'avoir fait en Belgique au 30 juin 2018.

Être *délégué à la protection des données* est avant tout une responsabilité au regard de la loi, une fonction au sein de l'entreprise. Il ne s'agit pas a priori d'un métier au sens strict. Ce rôle peut être exercé sous des formes diverses. Il peut s'agir d'une personne qui exerce cette fonction au sein de l'entreprise, éventuellement à plein temps ou couplée avec d'autres responsabilités, ou bien d'une personne externe agissant au titre de consultant. Enfin si les textes légaux imposent qu'une personne soit désignée, il peut s'agir d'une personne morale, ou encore d'une personne physique qui s'appuie sur une équipe pluridisciplinaire. En effet, les missions du DPO reposent sur des compétences multiples relevant du domaine du droit, de l'informatique ou encore de la gestion des organisations.

Sur le marché de l'emploi, Le Forem a diffusé durant le premier semestre 2018 au moins 180 propositions de recrutement à l'intention de DPO ou de *délégué à la protection des données*[14], ce qui incite à penser qu'il s'agit de concepts qui font sens. Ces appellations n'existent pas dans la nomenclature métier du Forem (REM), ces libellés sont ceux renseignés spontanément par l'émetteur de l'offre. À des fins de standardisation, ces offres sont reformulées selon le référentiel métier officiel. Les offres de DPO ont tantôt été liées à des appellations métiers propres à l'informatique tantôt aux professions juridiques ou de gestion des organisations. Cela illustre le caractère hybride ou polyvalent du DPO à la croisée de différentes disciplines.

De la conformité au règlement à la gouvernance des données

Pour beaucoup d'entreprises, engager un *délégué à la protection des données* vise essentiellement à se mettre en conformité avec le RGPD. Elles attendent de ce dernier qu'il les mette à l'abri des sanctions. Selon les experts participants, cette conception « minimaliste » du DPO s'avère particulièrement problématique en raison du manque de maturité des entreprises et organismes européens en général, et a fortiori wallons, en matière de gouvernance des données. Les conclusions de l'enquête publiée par Digital Wallonia[15] à la veille de l'entrée en application du RGPD illustrent cette relative indifférence des entreprises vis-à-vis de la gestion formelle des données : alors que potentiellement toutes les entreprises gèrent des données à caractère personnel (ne fut-ce que les fichiers clients), seuls 46 % d'entre elles se disaient

[12] La désignation d'un délégué est obligatoire pour :
- les autorités ou les organismes publics ;
- les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ;
- les organismes dont les activités de base les amènent à traiter des données dites « sensibles ».

[13] En Belgique, il s'agit de l'Autorité de Protection des Données, anciennement Commission de protection de la vie privée. https://www.autoriteprotectiondonnees.be.

[14] Sur base des offres d'emploi contenant les termes DPO, *Délégué à la protection des données*, RGPD ou GDPR dans l'intitulé du poste à pourvoir.

[15] Digital Wallonia.be, *RGPD : Les entreprises wallonnes sont-elles prêtes ?* 16 mai 2018. Consultable sur : https://www.digitalwallonia.be/fr/publications/rgpd-entreprises-wallonnes.

informées de l'entrée en vigueur du règlement européen et 57 % affirmaient ne pas traiter de données à caractère personnel. Dans un contexte économique où la donnée devient un actif de l'entreprise et source de production de richesse, l'arbitrage entre le respect des normes, dont le RGPD, et la maximisation du potentiel des données constitue un enjeu majeur.
Il convient dès lors d'élargir la conception du DPO et d'y inclure des dimensions stratégiques afin qu'il contribue à transformer l'entreprise.

Profil et contenu de la fonction

Le RGPD stipule simplement que le *« délégué est désigné sur la base de ses qualités professionnelles et de sa capacité à accomplir ses missions ».*[16]

Les lignes directrices du G29, le groupe rassemblant les différentes autorités nationales de protection des données, précisent les compétences et l'expertise nécessaires à la réalisation des missions[17]. Le DPO doit disposer :

- d'une expertise relative aux législations nationale et européenne en matière de protection des données, y compris une connaissance approfondie du RGPD ;
- d'une compréhension des opérations de traitement effectuées ;
- d'une compréhension des technologies de l'information et de la sécurité des données ;
- d'une connaissance du secteur d'activité et de l'organisme ;
- d'une capacité à promouvoir une culture de protection des données au sein de l'organisme.

Si les textes légaux donnent assez peu d'éléments concernant le profil requis pour la fonction, il ressort de cette précision du G29 que l'exercice de la fonction repose tant sur des compétences juridiques qu'informatiques.

Le RGPD précise néanmoins les conditions dans lesquelles le DPO doit exercer selon trois critères :

- la position dans l'entreprise : être reconnu et soutenu par la direction, disposer de moyens nécessaires à l'exercice de la fonction (budget, infrastructure, temps, …) ;
- l'indépendance ;
- les conflits d'intérêt : notamment, le délégué ne peut occuper une fonction au sein de l'organisme qui le conduit à déterminer les finalités et les moyens du traitement de données à caractère personnel.

Le dernier point est essentiel dans la mesure où il précise ce que le DPO ne peut pas faire. Globalement il ne peut rien faire qui l'assimilerait au responsable de traitement des données.
Enfin les missions du DPO sont, quant à elles, clairement définies dans l'article 39 du RGPD. Ce sont ces missions qui serviront de profil de fonction du DPO utilisé dans le présent travail. Ces missions sont reprises dans le tableau ci-après. En concertation avec le groupe d'experts, deux missions ont été ajoutées.
La première a trait à la relation avec les personnes concernées et a été ajoutée sur base d'informations publiées par ailleurs. La deuxième a été ajoutée à la demande expresse des experts qui ont souhaité intégrer la dimension « d'appui à l'entreprise dans sa montée en maturité en matière de gestion des données à caractère personnel, et plus globalement en matière de gouvernance des données ».
En face de ces missions, et à titre illustratif, sont reprises les différentes « compétences requises » publiées par l'autorité de protection de données belge[18].
La suite des travaux portera sur les missions plutôt que sur la liste de compétences requises, lesquelles s'avèrent trop détaillées que pour être opérationnelles dans le cadre de la méthode Abilitic2perform.

[16] Article 37 du règlement général européen pour la protection des données (http://www.privacy-regulation.eu/fr/37.htm).
[17] https://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf.
[18] Commission de protection de la vie privée, ÉLÉMENTS ESSENTIELS MINIMUMS QU'UNE FORMATION DPD DOIT CONTENIR, janvier 2018.

Missions	Activités
Informer et conseiller le responsable du traitement ou le sous-traitant.	- Aider à la création et à la gestion du registre des activités de traitement. - Mettre en place des programmes de formations pour le personnel au sujet de la protection des données.
Contrôler (monitor) le respect des règlements.	- S'assurer de la conformité avec les principes de base du traitement des données, comme le principe de finalité déterminée, de minimisation des données, d'exactitude, de limitation de la conservation, et de l'intégrité et la confidentialité des données. - Identifier avec précision la base de légitimité des traitements de données. - Analyser la compatibilité des finalités autres que celles pour lesquelles les données ont été collectées. - Déterminer s'il existe une réglementation sectorielle ou nationale qui pourrait déterminer des conditions spécifiques autres que celles qui sont prévues par le RGPD. - Vérifier les contrats signés ou envisagés aves des sous-traitants afin de s'assurer du respect des dispositions de l'article 28 du RGPD. - Identifier les situations de transferts de données personnelles en dehors de l'UE. - Identifier les mécanismes les plus adéquats pour encadrer au mieux les transferts de données personnelles. - Veiller à la rédaction et exercer un contrôle sur le contenu des « privacy policies » en conformité avec le RGPD.
Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact.	- Aider à l'analyse de risque des activités de traitement envisagées et en cours ainsi que participer à l'analyse d'impact relative à la protection des données. - Vérifier l'existence de mesures de sécurité adéquates aux risques présentés et à la nature des opérations de traitement. - Vérifier l'existence de procédures pour gérer les brèches de sécurité en conformité avec les prescrits du RGPD, en ce compris la notification à l'autorité de contrôle et la communication au public.
Coopérer avec l'autorité de contrôle / Faire office de point de contact pour l'autorité de contrôle (consultations préalables art 36).	- Être le point de contact pour les autorités de protection des données et s'assurer d'une bonne collaboration avec elles.
Relation avec les personnes concernées.	- S'assurer de la bonne information des personnes concernées via l'implémentation de procédures claires et bien définies. - Gérer les demandes des personnes concernées lorsqu'elles exercent leurs droits et mettre en place des procédures accessibles et simples pour l'exercice de ces droits. - Gérer les demandes d'information des personnes concernées par rapport au traitement de leurs données.

Missions	Activités
Venir en appui de l'entreprise dans sa montée en maturité en matière de gestion des données à caractère personnel, et plus globalement en matière de gouvernance des données.	- *Introduire le Privacy / security by design[19].* - *Déployer une démarche « qualité de la donnée ».* - *Développer une éthique des données, transparente et respectueuse des personnes concernées.* - *Accompagner la transformation organisationnelle de l'entreprise.*

***Tableau 1** : Le périmètre du métier de Délégué à la protection des données.*

Note de lecture : *Les éléments en italique ont été ajoutés sur proposition des experts participants.*

L'accès à la profession de DPO n'est pas soumis à l'obtention d'une certification spécifique. Dans les faits, un niveau de diplôme de l'enseignement supérieur, une expérience dans un service IT et une connaissance du RGPD sont le plus souvent requis. Certaines offres d'emploi mentionnent toutefois la nécessité de disposer d'un « certificat ».

Il existe en effet en Belgique francophone des formations continuées spécifiques pour DPO. D'une durée de quelques jours, elles sont proposées par des universités, des hautes écoles ou des organismes privés[20]. Un certificat interuniversitaire[21], plus long, d'une durée d'un an et demi, est organisé conjointement par l'Université de Namur et l'ICHEC.

En outre, plusieurs centres de compétences en Wallonie proposent des formations aux travailleurs ou demandeurs d'emploi en vue de devenir DPO ou d'être sensibilisé aux problématiques du RGPD[22].

[19] Le principe de la « protection de la vie privée dès la conception », privacy by design ou privacy by default, stipule que chaque nouvelle technologie traitant des données personnelles ou permettant d'en traiter doit garantir dès sa conception et lors de chaque utilisation, même si elle n'a pas été prévue à l'origine, le plus haut niveau possible de protection des données.

[20] Notamment :

- « Programme in european data protection », Solvay Brussels School ;
- « Data privacy and security management (RGPD) », ICHEC ;
- « Formation au métier de délégué à la protection des données », GDPR Agency ;
- « Certificat en protection des données », Data Protection Institute ;
- « Certificat en protection des données », Wolters Kluwer ;
- « Data Protection Officer course », Deloitte.

[21] Plus connu sous le nom du programme Datasafe.

[22] Formation « Protection des données » de Technofutur TIC ; « GDPR, comment organiser la mise en conformité de mon entreprise ? », Technifutur ; « RGPD/GDPR - Concrètement on commence par quoi ? », Technobel.

2. LES FACTEURS LES PLUS IMPORTANTS

L'anticipation des facteurs de changement s'effectue, selon la méthodologie Abilitic2Perform, en deux étapes : d'abord, le recensement le plus large possible des facteurs de changement puis la sélection des plus importants d'entre eux par le biais de votes pondérés.

Concrètement, les experts ont répondu en atelier à la question suivante : Quels sont, dans un horizon de trois à cinq ans, les facteurs qui détermineront/influenceront les activités du *délégué à la protection des données* ?

Après un temps de réflexion individuelle, suivi d'une présentation à l'ensemble du groupe, les experts ont proposé un peu moins d'une cinquantaine de facteurs dont certains ont été regroupés a posteriori. Les 20 plus importants, sélectionnés sur base d'un vote pondéré, sont repris ci-après.

A1	Formations « reconnues » pour être DPO
A2	Apparition de nouveaux métiers liés aux données
A3	Certifications officielles de processus (de type ISO par exemple)
A4	Réglementation du profil requis pour être DPO
A5	Digitalisation (transformation des processus de production, gestion, communication, … basée sur le numérique et la donnée)
A6	Open data et obligation d'ouvrir les données
A7	Règlementations multiples relatives aux données et domaines connexes (notamment internationales)
A8	Prise de conscience du management de l'importance de la donnée et de sa protection
A9	Développement de l'intelligence artificielle
A10	Développement du big data
A11	Retour d'expériences sur x années de RGPD
A12	Diversité des attitudes et sensibilités des personnes (selon les générations, niveau d'éducation, …)
A13	Chartes sectorielles relatives aux données à caractère personnel (code de conduites officiels à portée sectorielle)
A14	Politique de contrôle de l'Autorité de Protection des Données
A15	Évolution de la jurisprudence en termes d'incompatibilité / autorisation de cumul[23]
A16	Les décisions en matière de cumul CSI (Conseiller en sécurité de l'information)[24] - DPO dans le secteur public
A17	Développement des technologies « blockchain[25] »
A18	Développement du *DPO as a service*[26]
A19	Internet Of Things, développement des objets connectés et des données produites par ces derniers
A20	Suivi des mises à jour des textes législatifs et *guidelines*

***Tableau 2** : Les 20 facteurs de changement importants.*

[23] Pour rappel le DPO ne peut pas réaliser d'activités assimilables au traitement de données.
[24] Entre temps, la loi belge du 5 septembre 2018 qui institue le Comité de sécurité de l'information et modifie diverses lois concernant la mise en œuvre du 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, fait disparaître la fonction de CSI au profit de celle de DPO.
[25] La blockchain, ou chaîne de blocs, est une technologie de stockage et de transmission de données non centralisée. Elle repose sur un cryptage des échanges et une validation par chacun des membres de la chaîne.
[26] On appelle « DPO as a service », les solutions en ligne standardisées, proposées aux entreprises souhaitant sous-traiter l'activité de DPO.

3. LA SÉLECTION DES FACTEURS LES PLUS INFLUENTS

Durant l'étape suivante, les experts ont évalué l'influence que ces 20 facteurs « importants » exerçaient les uns sur les autres. Entre le premier et le second atelier, les experts ont été invités à compléter une matrice en y notant l'influence des 20 facteurs en ligne sur les mêmes 20 facteurs en colonne
(0 : aucune influence ; 1 : influence faible ; 2 : influence moyenne ; 3 : influence forte).

La compilation des matrices des experts est visualisée dans le graphique 1 qui représente les positions d'influence / dépendance relatives des 20 facteurs.

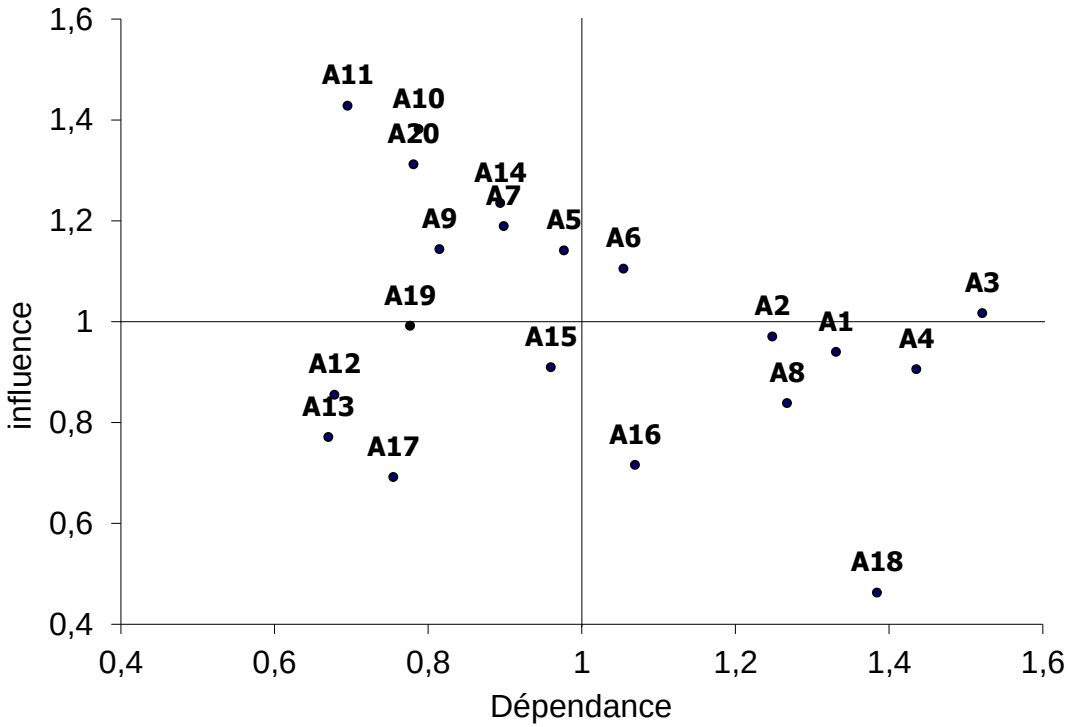
La méthode préconise de sélectionner les facteurs les plus « dominants » et les « moins influencés » repris dans le cadre supérieur gauche. Il s'agit ici des facteurs suivants :

1. Digitalisation (A5)
2. Règlementations multiples (A7)
3. Intelligence artificielle (A9)
4. Big data (A10)
5. Retour d'expériences sur x années de RGPD (A11)
6. Politique de contrôle de l'Autorité de Protection des Données (A14)
7. Suivi des mises à jour des textes législatifs et *guidelines* (A20)

Auxquels les experts ont souhaité ajouter trois facteurs relativement dominants :

8. Open data et obligation d'ouvrir les données (A6)
9. Évolution de la jurisprudence en termes d'incompatibilité / autorisation de cumul (A15)
10. Internet Of Things (A19)

À la demande des experts, les facteurs « big data » et « intelligence artificielle » seront fusionnés pour la suite des travaux.



***Graphique 1** : Compilation des matrices des votes d'influence des experts.*

4. LES ÉVOLUTIONS PROBABLES ET SOUHAITABLES ET PROFIL D'ÉVOLUTION

Une fois ces 10 facteurs déterminés, il s'agissait d'envisager leurs évolutions possibles. Pour chacun des facteurs, les experts ont proposé différentes hypothèses d'évolution. Chaque hypothèse a été débattue et reformulée en séance, afin qu'elle soit validée par le groupe.

Elles ont ensuite été soumises au vote des experts qui étaient invités à sélectionner l'hypothèse à retenir afin de constituer le scénario d'évolution, appelé aussi profil d'évolution.

Pour être retenue, une hypothèse d'évolution devait être jugée soit hautement probable ou hautement souhaitable. Le tableau ci-dessous reprend les hypothèses formulées pour chacun des facteurs, celles retenues apparaissent en caractère gras.

Facteurs	Hypothèse A	Hypothèse B
Digitalisation (transformation des processus basée sur le numérique et la donnée).	**La culture de l'innovation se développe de manière différenciée selon les secteurs, la sensibilité du management, ou encore selon la taille de l'entreprise. De nombreuses entreprises utilisent des outils inadaptés et moins performants. Toutefois l'évolution sociologique au sein des entreprises accélère le mouvement.**	La digitalisation s'étend à tous les pans de l'industrie. On observe une « culture » de l'innovation. Le management est partie prenante et moteur de celle-ci en utilisant des outils adaptés. Les pouvoirs publics (régionaux, fédéraux, européens) soutiennent ces évolutions.
Open data et obligation d'ouvrir les données.	**Rendre les données exploitables et disponibles est encore considéré comme un coût. Les autorités publiques ouvrent leurs données uniquement sur demande et ne font pas la promotion des possibilités existantes. L'Open data se développe seulement dans certains secteurs : mobilité, santé, énergie, … Il existe encore des freins liés à un retard de numérisation, aux difficultés liées au format ou à la fiabilité des données.**	Les entreprises (privées ou publiques) ont compris l'intérêt de l'exploitation des données. Grâce à ces données de nouveaux services sont développés. L'Open data par défaut prend le pas sur l'open data à la demande.
Règlementations multiples (notamment internationales).	**Les réglementations sont morcelées et multiples, générant un certain flou juridique. Chaque État veut garder ses propres données et garder une certaine autonomie par rapport à celles-ci. La donnée devient une « arme stratégique ». La géolocalisation des données est un enjeu important. L'*E-privacy* a un impact important sur l'*e-marketing*. Le *hosting* de données devient un véritable business.**	Les règlementations intercontinentales s'harmonisent au maximum dans un climat propice à la coopération internationale. Cela favorise une circulation fluide et sécurisée des données au niveau mondial et le développement de nombreux projets entre partenaires de différents pays.
Intelligence artificielle/big data.	Les PME n'ont pas les moyens d'exploiter les données et ne sont pas matures. Le big data et l'intelligence artificielle sont aux mains de quelques acteurs seulement (monopole).	**La formation d'un écosystème autour du big data et de l'intelligence artificielle rend favorable l'exploitation par les PME. Les services proposés sont de plus en plus accessibles et facilitent l'externalisation, permettant le développement de *l'IA as a service*.**

Facteurs	Hypothèse A	Hypothèse B
Retour d'expériences sur x années de RGPD.	**Des échanges de bonnes pratiques se développent sous différentes formes. Ceux-ci sont morcelés et relèvent principalement d'évènements sectoriels. Ils sont souvent accessibles aux plus grandes entreprises, les PME ont moins accès à ces échanges. Des nouveaux services payants apparaissent (assurances, certifications, …)**	L'Autorité de Protection des Données cadre les échanges de bonnes pratiques. Les échanges sont facilités et accessibles à toutes les entreprises.
Politique de contrôle de l'Autorité de Protection des Données.	**L'ADP a peu de moyens, les contrôles sont très peu nombreux et très sectoriels. Des sanctions sont prises pour servir d'exemple. Les plaintes sont peu nombreuses.**	Les moyens sont suffisants pour réaliser des contrôles de manières harmonieuses et objectives.
Évolution de la jurisprudence en termes d'incompatibilité / autorisation de cumul.	**Les jurisprudences évoluent de manière différente en fonction des États.** **La liste des fonctions incompatibles évolue au cas par cas et plutôt sous formes de recommandations.**	Les plaintes auprès de la Commission se multiplient, ce qui lui permet d'affirmer sa position, de fixer et de faire respecter les incompatibilités.
Internet Of Things.	L'IOT génère des nouveaux processus, qui génèrent eux-mêmes des données à caractère personnel. L'IOT se développe sous l'effet de la démocratisation des technologies mais, en l'absence de contrainte légales, le niveau de sécurité reste faible.	**L'IOT génère des nouveaux processus, qui génèrent eux-mêmes des données à caractère personnel.** **Les objets connectés, pour être mis sur le marché, doivent obligatoirement être certifiés en matière de sécurité. Cela garanti un niveau élevé de sécurité des données générées par les objets connectés.**
Suivi des mises à jour des textes législatifs et *guidelines.*	Les mises à jour consécutives à des décisions de justice sont nombreuses et régulières. Les entreprises peinent à suivre ces évolutions.	**La règlementation évolue constamment. La communication se fait correctement, les entreprises ont la possibilité de s'adapter rapidement.**

***Tableau 3** : Les hypothèses d'évolution pour chaque facteur de changement clé.*

5. LES IMPACTS SUR LES ACTIVITÉS ET LES BESOINS EN COMPÉTENCES

La dernière étape du travail réalisé avec les experts a porté sur l'identification des compétences que *le délégué à la protection des données* devrait maintenir ou développer d'ici 2022. L'objectif de ce recensement est d'éclairer les futurs besoins en compétences.

Dans un premier temps le groupe a identifié les missions du *délégué à la protection des données* qui seront les plus influencées par les différentes hypothèses d'évolution via un vote. Il en ressort que les missions les plus impactées sont en ordre d'importance :

- venir en appui de l'entreprise dans sa montée en maturité en matière de gestion des données à caractère personnel, et plus globalement en matière de gouvernance des données ;
- contrôler (monitor) le respect des règlements ;
- dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact ;
- informer et conseiller le responsable du traitement ou le sous-traitant.

Les missions relatives aux relations avec les « personnes concernées » et avec l'autorité de contrôle paraissent moins sensibles aux évolutions à venir.

Les facteurs qui semblent influencer le plus l'exercice du métier sont quant à eux relatifs au « Suivi des mises à jour des textes législatifs et *guidelines* » et « retour d'expérience sur plusieurs années de RGPD ».

Pour les missions les plus impactées et en fonction des évolutions qu'elles subiront, les experts ont listé les compétences nécessaires à leur réalisation.

Tâches impactées (Pour…)	Ressources (compétences) (Il faut…)	Facteur(s) d'évolution impactant (Dans un contexte où…)

Venir en appui de l'entreprise dans sa montée en maturité en matière de gestion des données à caractère personnel, et plus globalement en matière de gouvernance des données.	<u>Sensibilisation / communication</u>
	• Être capable de sensibiliser, mobiliser et faire adhérer les membres de l'organisation, la direction aux enjeux de la gouvernance des données et faire adopter de grands principes comme :
	  ◦ Le *privacy / security by design*[27].
	  ◦ Démarche « qualité » de la donnée.
	  ◦ Développer une approche éthique de la donnée.
	• Être capable de communiquer sur les besoins de changement.
	• Adapter sa communication en fonction des différents profils professionnels des interlocuteurs.
	• Développer un discours business en lien avec l'innovation.
	<u>Compétences relationnelles</u>
	• Participer régulièrement au Comité de direction, avec voix consultative.
	• Développer un réseau de partenaires.
	<u>Organisation des entreprises et gestion du changement</u>
	• Connaître les différents types d'organisation des entreprises.
	• Analyser l'organisation d'une entreprise et établir un diagnostic de problèmes liés à la gouvernance des données (à caractère personnel).
	• Connaître des modèles de gestion de changement
	  ◦ Théoriques : par exemple les modèles de mesure de maturité comme le *Capability Maturity Model Integration* (CMMI).
	  ◦ Pratiques : par exemple des initiatives qui ont fonctionné ailleurs.
		<u>Digitalisation (transformation des processus basés sur le numérique et la donnée)</u>
		La culture de l'innovation se développe de manière différenciée selon les secteurs, la sensibilité du management, ou encore selon la taille de l'entreprise. De nombreuses entreprises utilisent des outils inadaptés et moins performants. Toutefois l'évolution sociologique au sein des entreprises accélère le mouvement.

[27] Le principe de la « protection de la vie privée dès la conception », *privacy by design* ou *privacy by default*, stipule que chaque nouvelle technologie traitant des données personnelles ou permettant d'en traiter doit garantir dès sa conception et lors de chaque utilisation, même si elle n'a pas été prévue à l'origine, le plus haut niveau possible de protection des données.

Tâches impactées (Pour…)	Ressources (compétences) (Il faut…)	Facteur(s) d'évolution impactant (Dans un contexte où…)
	• Comprendre une cartographie de données. • Connaître et comprendre (pas maîtriser) les outils utilisés par les architectes informatiques, les analystes, …	<u>Open data et obligation d'ouvrir les données</u> Rendre les données exploitables et disponibles est encore considéré comme un coût. Les autorités publiques ouvrent leurs données uniquement sur demande et ne font pas la promotion des possibilités existantes. L'Open data se développe seulement dans certains secteurs : mobilité, santé, énergie, … Il existe encore des freins liés à un retard de numérisation, aux difficultés liées au format ou à la fiabilité des données.
	• Être capable de comprendre les enjeux de l'intelligence artificielle en matière de *profiling* et de gestion de données à caractère personnel. • Être sensible aux processus de désanonymisation. • Connaître et comprendre les principes d'éthique de la donnée. • Connaître et comprendre les principes de marquage de données (métadonnées relatives à ce qui peut être fait avec les données). • Réaliser une veille technologique et réglementaire (notamment en participant à des colloques). • Rédiger des politiques internes sur base de la veille règlementaire. • Être capable de réfléchir à l'évolution du métier grâce à des échanges avec les pairs.	<u>Intelligence artificielle/big data</u> La formation d'un écosystème autour du big data et de l'intelligence artificielle rend favorable l'exploitation par les PME. Les services proposés sont de plus en plus accessibles et facilitent l'externalisation, permettant le développement de *l'IA as a service*.
Contrôler (monitor) le respect des règlements.	Réaliser une veille juridique • Lire les newsletters de l'Union Européenne et les décisions de la Cour Européenne de Justice relatives aux données à caractère personnel. • Être capable de comprendre l'anglais juridique à la lecture. • Connaître les pays bénéficiant d'une décision d'adéquation des autorités européennes[28].	<u>Suivi des mises à jour des textes législatifs et *guidelines*</u> La règlementation évolue constamment. La communication se fait correctement, les entreprises ont la possibilité de s'adapter rapidement.

[28] Il s'agit des pays pour lesquels l'Union européenne considère que le niveau de protection des données à caractère personnel est au moins aussi élevé que celle en vigueur dans l'Union.

Tâches impactées (Pour…)	Ressources (compétences) (Il faut…)	Facteur(s) d'évolution impactant (Dans un contexte où…)
	Veiller les bonnes pratiques • Fréquenter les cercles DPO et groupes sectoriels. • Exploiter des sources internet comme les sites spécialisés. • Suivre l'évolution des normes ISO (p. ex. : ISO 27001 relative à la sécurité de l'information). Analyse des organisations • Pouvoir identifier les mécanismes et politiques internes (codes de conduite) de transferts de données. • Connaître l'entreprise (son réseau, ses indicateurs de performance). • Être capable d'utiliser une grille d'audit des données personnelles. Analyse juridique • Être capable d'identifier les conflits entre RGPD et d'autres règlementations (ex. : E-privacy). • Être capable d'interpréter les textes juridiques et leur impact sur l'entreprise. Être apte à réagir et organiser une traçabilité et un suivi • Être capable d'alerter les directions quand une législation a un impact sur l'activité. • Pouvoir établir un tableau de bord des actions mises en œuvre pour être en conformité avec les règlementations relatives à la protection des données à caractère personnel. • Collecter, garder, stocker les preuves des démarches entreprises. • Être rigoureux. • Être capable d'établir des priorités.	<u>Règlementations multiples (notamment internationales)</u> Les réglementations sont morcelées et multiples, générant un certain flou juridique. Chaque État veut garder ses propres données et garder une certaine autonomie par rapport à celles-ci. La donnée devient une « arme stratégique ». La géolocalisation des données est un enjeu important. *E-privacy* a un impact important sur l'e-marketing. Le *hosting* de données est un véritable business.

Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact.	• Analyse juridique et stratégique :
	  • Capable d'instruire, aider à, l'arbitrage entre les intérêts de la personne privée et la stratégie de l'entreprise.
	  • Proposer différentes alternatives.
	• Solliciter des avis externes (activer son réseau).
	• Faire preuve d'empathie, se mettre à la place de la « personne concernée » (*data ethics*).
		<u>Digitalisation</u>
		La culture de l'innovation se développe de manière différenciée selon les secteurs, la sensibilité du management, ou encore selon la taille de l'entreprise. De nombreuses entreprises utilisent des outils inadaptés et moins performants. Toutefois l'évolution sociologique au sein des entreprises accélère le mouvement.

Tâches impactées (Pour…)	Ressources (compétences) (Il faut…)	Facteur(s) d'évolution impactant (Dans un contexte où…)

	• Risk management :
	  • Comprendre la notion de risque.
	  • Utiliser des méthodes d'analyse d'impact comme celles proposées par la CNIL[29].
	  • Intégrer dans l'analyse de risques des dimensions autres que financières ou internes.
	  • S'intégrer dans, ou à défaut, implémenter une culture du risque dans l'entreprise.
	• Promouvoir une approche « privacy by design[30] ».
		Retour d'expérience après plusieurs années de RGPD
		Des échanges de bonnes pratiques se développent sous différentes formes. Ceux-ci sont morcelés et relèvent principalement d'évènements sectoriels. Ils sont souvent accessibles aux plus grandes entreprises, les PME ont moins accès à ces échanges. Des nouveaux services payants apparaissent (assurances, certifications, …).
		Suivi des mises à jour des textes législatifs et *guidelines*
		La règlementation évolue constamment. La communication se fait correctement, les entreprises ont la possibilité de s'adapter rapidement.

***Tableau 4** : Compétences majeures.*

[29] PIA est un logiciel open source qui facilite la conduite et la formalisation d'Analyses d'Impact relatives à la Protection des Données (AIPD) telles que prévues par le RGPD. Téléchargeable via le lien : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

[30] Le principe de la « protection de la vie privée dès la conception », privacy by design ou privacy by default, stipule que chaque nouvelle technologie traitant des données personnelles ou permettant d'en traiter doit garantir dès sa conception et lors de chaque utilisation, même si elle n'a pas été prévue à l'origine, le plus haut niveau possible de protection des données.

Au terme de l'analyse des besoins en compétences à trois à cinq ans, le rôle du DPO apparait ambitieux. Cela invite à aborder une double réflexion. La première concerne le profil du candidat DPO. Une personne capable d'analyser l'organisation d'une entreprise, d'y insuffler une nouvelle culture, tout en parvenant à convaincre un comité de direction de développer une véritable gouvernance de la donnée doit, *a priori,* disposer d'une certaine expérience ou d'une maturité lui assurant la crédibilité nécessaire à l'accomplissement de sa mission.

La seconde réflexion porte sur la formation. Il parait difficile de proposer des formations courtes permettant d'acquérir les compétences informatiques et juridiques nécessaires à la fonction tout en développant des savoir-faire comportementaux comme la rigueur, l'assertivité, la communication ou encore le sens de l'organisation. Les formations courtes ne peuvent prétendre qu'à couvrir une partie des compétences, complémentairement à d'autres développées dans le cadre de formations préalables ou de l'expérience acquise par ailleurs. Enfin il convient de rappeler à ce stade, que le rôle de DPO peut être assuré par une équipe pluridisciplinaire ce qui permet de répartir les multiples compétences nécessaires entre différentes personnes.

NOUS REMERCIONS POUR LEUR PARTICIPATION AU PROCESSUS EN QUALITÉ D'EXPERTS

Alain DE MAGHT, ABCD Consult
Antoine DELFORGE, Université de Namur – CRIDS
Frédéric DINON, Technobel
Isabelle DUGAILLIEZ, Union des Villes et Communes de Wallonie
Alain EJZIN, ICHEC
Julien GASSEND, Digital Wallonia
Dominique GREGOIRE, Le Forem
Claudia GROSU, NRB
Pierre LELONG, Technofutur TIC
Thomas TOMBAL, Université de Namur – CRIDS
Fabien TRAMASURE, RGPD Agency
Michel VERSTREPEN, Le Forem

ENCADREMENT MÉTHODOLOGIQUE DE LA DÉMARCHE ET RÉDACTION DU RAPPORT FINAL

Le Forem - Veille, analyse et prospective du marché de l'emploi :
William WATELET, Animation et rédaction
Cynthia CACCIATORE, Support administratif

ÉDITEUR RESPONSABLE

Marie-Kristine VANBOCKESTAL, Administratrice générale, Le Forem