Projet BOOST - Booster la connaissance et le respect du RGPD chez les PME belges, en se concentrant sur trois thèmes principaux

MISE EN ŒUVRE DU RGPD DANS LES PETITES ET MOYENNES ENTREPRISES EN BELGIQUE : LES CONNAISSANCES ACTUELLES, LA SENSIBILISATION ET LES DEFIS DU POINT DE VUE DES ORGANISATIONS SECTORIELLES

Wauters, Chantal
Imec-SMIT VUB

Heyman, Rob
Imec-SMIT VUB

Introduction

La présente étude s'inscrit dans le cadre du projet de recherche plus large BOOST, une collaboration entre l'Autorité belge de protection des données (APD), la Katholieke Universiteit Leuven, la Vrije Universiteit Brussel et l'Université de Namur. Le projet de recherche BOOST vise à sensibiliser et à accroître les connaissances au sujet du Règlement général sur la protection des données (RGPD) dans les petites et moyennes entreprises (PME) en Belgique. Ce rapport concerne les résultats du programme de travail 2, production 2.2., dont le but est de recenser les connaissances et défis actuels des PME dans le contexte de la mise en œuvre du RGPD. Cette production a été préparée par la Vrije Universiteit Brussel.

Nous commencerons par expliquer la finalité de l'étude. Ensuite, nous aborderons les résultats de l'étude qui permettent de comprendre davantage les connaissances actuelles, la sensibilisation et les défis des PME par rapport au RGPD. Enfin, nous formulerons quelques conclusions qui peuvent se révéler intéressantes pour les prochaines étapes du projet de recherche BOOST.

Ce projet est financé par le programme Droits, Egalité et Citoyenneté REC-AG-2019 de l'Union européenne.

Cadre méthodologique

Pour pouvoir recenser les connaissances et les défis actuels des PME à l'égard du RGPD, nous avons organisé des réunions avec des organisations sectorielles. La pratique démontre que les PME qui ont des questions et des difficultés se tournent vers les organisations sectorielles. Ces organisations ont la meilleure vue d'ensemble de la situation dans leur propre secteur. Au départ, nous souhaitions réunir physiquement à la fois les organisations sectorielles et quelques-uns de leurs membres (PME) afin de pouvoir leur poser nos questions. Suite aux mesures imposées dans le contexte de la crise du COVID-19, il n'a plus été possible d'organiser des réunions physiques dans le cadre de l'étude. Les réunions prévues ont eu lieu sous forme numérique. Ceci (et le fait que les PME ont montré un faible intérêt pour participer à cette étude), nous a finalement conduit à consulter principalement des organisations sectorielles. Seules deux organisations sectorielles ont pu impliquer des PME individuelles dans l'exercice : Agoria (18 répondants) et Scwitch (6 répondants).

Pour sélectionner les organisations sectorielles, nous avons fait appel à des listes de contacts existantes, fournies par l'APD et les autres partenaires du consortium. Cette sélection a été complétée par des sources en ligne. Vu la portée limitée de l'étude, il a été décidé de procéder à une sélection d'organisations sectorielles, étant donné qu'il n'était pas possible d'y associer tous les secteurs. Ce sont finalement les organisations sectorielles ci-dessous qui ont été consultées. Des informations sur la mission et les membres de ces organisations figurent dans les annexes (annexe 1, p. 11). L'organisation sectorielle Scwitch a une composition différente, ses membres étant notamment des associations sans but lucratif (asbl) du secteur socioculturel. Dans les résultats, nous parlons toujours de PME, incluant les membres de Scwitch. Si les résultats diffèrent dans les deux groupes, nous le mentionnons explicitement.

- Agoria
- Association Pharmaceutique Belge (APB)
- Bzb-Fedafin
- Federgon
- Feprabel
- Scwitch

La consultation au cours des réunions a été structurée à l'aide d'une liste de sujets établie préalablement (voir annexe 2, p.12). Cette liste de sujets permet de comparer les différentes réunions. Cette forme ouverte a laissé aux organisations la possibilité de faire leurs propres observations lors de la consultation.

Les trois thèmes centraux suivants du projet relatifs au RGPD ont été abordés : la transparence, les notions de responsable du traitement (controller en anglais) et de sous-traitant (processor en anglais) et l'analyse d'impact relative à la protection des données (AIPD). Nous avons ensuite abordé les défis auxquels les PME font face par rapport à ces trois thèmes, la pertinence du projet de recherche, l'aide apportée par les organisations sectorielles et les recommandations à l'égard du projet de recherche BOOST et de l'APD.

Volet empirique : résultats d'étude

Le RGPD : un thème d'actualité ?

Le RGPD est-il un thème d'actualité pour les PME en Belgique ? Les résultats indiquent que les organisations sectorielles accordent une attention à ce thème et sont régulièrement confrontées à des questions et défis auxquels les PME font face à l'égard du RGPD. Les entreprises sont de plus en plus confrontées à de nouveaux défis et prescriptions, qui les obligent à prendre des mesures. Mais le RGPD n'est plus d'une brûlante actualité pour les PME. Certaines PME ne sont pas intéressées à accorder une grande attention au sujet. **Plusieurs PME font appel à des organisations sectorielles et à d'autres instances externes pour mettre en œuvre au mieux le RGPD.** Ces instances répondent aux questions spécifiques des PME et rendent des avis au besoin.

Les ASBL interrogées via Scwitch indiquent également que la plupart des organisations répondent aux obligations minimales et ne considèrent dès lors plus le thème comme étant prioritaire. Le RGPD est rarement traité de manière structurelle. On y consacre seulement de l'attention lorsqu'un problème concret se présente dans l'organisation. Selon Scwitch elle-même, de nombreuses associations ont fourni des efforts pour respecter les obligations principales, mais des moyens financiers sont nécessaires pour évoluer vers une politique mieux fondée et plus élaborée en matière de RGPD au sein des organisations.

Nous constatons enfin que **peu de PME souhaitent participer aux réunions dans le cadre de BOOST**. Cela peut s'expliquer en partie par le fait que les PME qui ont des questions et des difficultés s'adressent généralement aux organisations sectorielles. Par ailleurs, cela peut indiquer un manque d'intérêt et/ou de conscience de l'importance du RGPD. D'après les organisations sectorielles, une partie des PME est par exemple convaincue que le RGPD ne s'applique pas au sein de leur propre organisation. Contrairement aux PME, les organisations sectorielles consultées manifestent un intérêt particulier pour la thématique et la plupart sont disposées à collaborer au projet de recherche. Les réunions informelles nous permettent de conclure que toutes les organisations sectorielles concernées consacrent déjà une attention à la thématique et ont développé une offre pour aider leurs propres membres à respecter le RGPD.

Le rôle des organisations sectorielles dans l'aide aux PME

Ce qui est frappant dans les résultats, c'est que selon les organisations sectorielles interrogées, **la plupart des PME ne sont pas en mesure de mettre le RGPD en œuvre correctement sans aide externe**. Les résultats décrits ci-dessous et qui se rapportent aux défis des PME, y compris à l'égard des trois thèmes, portent dès lors principalement sur les PME qui ne peuvent pas faire appel à un service juridique interne ou à un consultant externe. Le recours à un conseiller externe ou interne ne s'applique toutefois qu'aux entreprises qui disposent des moyens à cet effet. **Pour de nombreuses petites et moyennes entreprises (y compris des associations socioculturelles), le manque de moyens est un des principaux défis pour respecter le**

RGPD. Sans conseiller, il est en effet difficile d'appréhender la réglementation juridique complexe. Selon les organisations sectorielles, les informations transparentes, accessibles et spécifiques sont rares.

Les PME adressent leurs questions et difficultés au sujet du RGPD aux organisations sectorielles. Ces organisations tentent d'assister leurs membres de trois manières : 1/ la formulation d'avis et de réponses aux questions pratiques, 2/ l'information des membres et 3/ le soutien aux membres via des outils et documents (en ligne).

Premièrement, en ce qui concerne les avis, les organisations sectorielles adoptent généralement des points de vue officiels, étant donné que selon elles, le RGPD est trop abstrait et manque de clarté dans sa formulation. **Les organisations sectorielles souhaitent que l'APD adopte plus souvent des points de vue clairs afin de les assister dans leurs efforts visant à clarifier la mise en œuvre du RGPD dans le contexte de leur propre secteur**. Quelques organisations sectorielles indiquent disposer d'un groupe de travail RGPD, au sein duquel des entreprises se réunissent afin d'exposer les principaux défis et d'identifier les autres besoins.

Deuxièmement, les organisations sectorielles sont prêtes à répondre aux questions (généralement pratiques) de leurs membres. À cet égard, nos répondants font remarquer que les points de vue des organisations sectorielles n'ont pas été approuvés par l'Autorité belge de protection des données. Cela engendre des incertitudes au sein du secteur. Une partie de ce problème est traité en posant des questions à l'APD, mais il est rare que les réponses aux questions soumises à l'APD soient suffisamment spécifiques, indiquent certaines organisations.

Troisièmement, les organisations sectorielles s'emploient à informer les PME. Agoria organise des réunions *(Agoria Academy)* avec des membres pour les informer sur la réglementation et réagir aux difficultés pratiques. Agoria a en outre lancé en 2017 le *GDPR Compass*, un outil de mise en conformité permettant aux entreprises de répondre à des questions pour savoir quelles mesures doivent être mises en œuvre pour respecter le RGPD en ce qui concerne le traitement de données. Bzb-Fedafin met des cours en ligne à disposition et organise sporadiquement des ateliers et séminaires pour informer les membres. Federgon met également un webinar à disposition, propose des sessions d'information, un self scan, un groupe de travail, diverses directives ainsi qu'un plan par étapes. Feprabel a désigné un chef de projet RGPD qui informe les PME individuellement sur la réglementation et les mesures nécessaires. Scwitch organise des sessions d'information, met des outils pratiques à disposition et assiste les associations dans la mise en œuvre du RGPD, notamment en collaborant avec un conseiller externe. Par ailleurs, nous constatons que les organisations sectorielles ont à disposition plusieurs outils et documents pour aider les PME à respecter le RGPD. Les organisations sectorielles travaillent principalement avec des templates que les PME peuvent utiliser par exemple pour établir un contrat de sous-traitance, rédiger une clause de confidentialité, créer un registre de traitement[1], etc. Par ailleurs, les organisations sectorielles diffusent des manuels avec un plan échelonné afin de se mettre en

[1] Une organisation sectorielle que l'on ne nommera pas a indiqué que le modèle de registre de traitement de l'APD n'était pas pratique car il était trop long.

conformité avec le RGPD. Feprabel a développé une plateforme sur laquelle les membres peuvent établir un dossier RGPD propre en collaboration avec le chef de projet. À l'aide d'un questionnaire pratique, d'informations et de documents qui lui sont propres, la PME obtient un dossier individuel qui peut être présenté en cas de contrôle. Les PME sont ainsi accompagnées et informées individuellement par l'organisation. Lors de la consultation, les membres de Scwitch indiquent être à la recherche de telles plateformes d'aide en ligne qui permettent de suivre leurs propres progrès dans la mise en œuvre du RGPD.

Les résultats nous amènent à conclure que l'aide apportée aux PME par les organisations sectorielles est considérable. Les organisations sectorielles essaient principalement d'aider les PME de la manière la plus pratique et la plus spécifique possible, afin qu'elles soient juridiquement en ordre avec le RGPD. Toutefois, les documents, outils et informations qu'elles mettent à disposition dans ce cadre n'ont pas été officiellement vérifiés par l'APD. Ce qui nous interpelle, c'est que de nombreuses organisations sectorielles indiquent que sans leur aide, les PME prendraient peu d'initiatives en vue du respect du RGPD. Bon nombre d'entre-elles ne réalisent pas qu'il est important de respecter le RGPD. Un grand nombre de PME commettent l'erreur de croire que le RGPD ne s'applique qu'aux grandes entreprises.

Les principaux défis des PME

Nous avons demandé à chaque organisation sectorielle d'énumérer les principaux défis des PME en ce qui concerne le respect du RGPD. Dans les paragraphes qui précèdent, nous avons déjà mis en avant que le manque de sensibilisation à la prise de responsabilités individuelles chez les PME constituait un défi pour les secteurs. Nous avons ensuite abordé le manque d'informations pratiques et simples à comprendre au sujet du RGPD. Les PME sont confrontées à toutes sortes de sources qui diffusent des informations juridiques complexes, peu claires et généralement contradictoires. Federgon indique par exemple qu'il existe un besoin de communication accessible aux PME. Ce point de vue a également été suivi par les autres organisations sectorielles. Par ailleurs, les défis suivants ont été évoqués par la plupart des organisations sectorielles interrogées : **1/ la collaboration avec des parties tierces en tant que sous-traitant, 2/ le manque de moyens financiers pour prendre des mesures et s'informer suffisamment, 3/ le manque de connaissances au sujet des droits des personnes concernées et 4/ le découragement engendré par les processus administratifs compliqués**.

En ce qui concerne la collaboration avec des sous-traitants, les PME éprouvent notamment des difficultés au niveau de la rédaction et/ou de la conclusion d'un contrat de sous-traitance. Bien que de nombreuses organisations sectorielles mettent des templates à disposition, **il n'est pas toujours évident de savoir clairement quand et sous quelles conditions les PME doivent établir un contrat et/ou doivent conclure un contrat de tiers**. Les PME estiment également qu'il est problématique de contrôler des sous-traitants externes pour ce qui est de la prise de mesures techniques et organisationnelles afin de protéger les données à caractère personnel. Le manque de contrôle engendre beaucoup d'incertitudes dans le chef des PME. Selon Scwitch, le plus grand défi pour les associations est de collaborer avec des tiers. D'une part, il y a beaucoup

d'imprécisions quant au partage de données à caractère personnel avec des partenaires et d'autre part, les associations sont confrontées à des directives et conventions complexes émanant des instances publiques avec lesquelles elles collaborent. D'après l'organisation sectorielle, les autorités ont plus de moyens à consacrer à la mise en œuvre du RGPD et attendent la même chose des associations avec lesquelles elles collaborent.

Pour beaucoup, le manque de moyens financiers les empêche de recourir à des conseillers internes et/ou externes. Ces PME doivent s'informer et se sensibiliser elles-mêmes à entreprendre les démarches nécessaires. Les associations socioculturelles indiquent que la réduction des subventions met encore plus la pression sur les organisations. Les PME ont recours aux organisations sectorielles, mais il faut garder à l'esprit que toutes les PME ne sont pas membres d'une organisation sectorielle. Le manque de connaissances quant aux droits des personnes concernées constitue par ailleurs un troisième défi identifié par les organisations sectorielles. Nous y reviendrons. Enfin, on note un découragement face aux processus administratifs compliqués. Pour les PME, le respect du RGPD ne fait pas partie de leur activité principale. Beaucoup d'entre elles considèrent dès lors que le fait de devoir s'occuper de toutes sortes de processus administratifs constitue une tâche rébarbative et secondaire (par exemple l'établissement d'un registre de données ou la réalisation d'une AIPD). Quelques membres de Scwitch indiquent qu'il y a un besoin important de simplification administrative.

Par ailleurs, nous constatons que les résultats diffèrent quelque peu selon le secteur. L'organisation sectorielle Agoria indique que pour les membres, il n'est pas toujours clair de savoir combien de temps les données peuvent être conservées. Ce défi est également confirmé par Feprabel, qui indique que des délais de conservation spécifiques s'appliquent pour le secteur. En outre, des membres d'Agoria s'interrogent quant à l'utilisation d'images de caméras et d'autres applications logicielles pour la surveillance des propres travailleurs. L'utilisation d'images de caméras dans le contexte du RGPD revient également dans d'autres secteurs. Les PME et organisations sectorielles indiquent que dans ce domaine, différentes réglementations s'appliquent, ce qui entraîne un manque de clarté. Les associations socioculturelles estiment aussi qu'il est difficile de déterminer quelles images peuvent être utilisées et diffusées à l'égard des consommateurs. Des membres de Scwitch éprouvent également des difficultés à sensibiliser et à former leurs propres travailleurs à l'égard du RGPD, de l'utilisation d'un fichier d'adresses pour la diffusion de lettres d'information et du respect des droits des personnes concernées.

Après avoir abordé les défis en général, nous avons abordé avec les organisations sectorielles les connaissances et les difficultés concernant les trois thèmes principaux du projet de recherche, à savoir la transparence, les notions de responsable du traitement et de sous-traitant et l'analyse d'impact relative à la protection des données (AIPD). Les résultats sont détaillés dans les paragraphes qui suivent.

Un manque de transparence

Un des principes du RGPD, et un premier thème central du projet de recherche, est la transparence. Les entreprises doivent communiquer clairement, ouvertement et loyalement à l'égard des personnes concernées au sujet des processus de traitement de données. Les informations doivent être accessibles et faciles à comprendre pour les personnes concernées. Autrement dit, une politique de confidentialité ne peut pas contenir de formulations juridiques excessives et/ou complexes et doit être facile à trouver. En tant que responsable du traitement, les PME doivent communiquer de manière proactive avec les personnes concernées et permettre l'exercice des droits des personnes concernées. Les PME sont-elles transparentes à l'égard des personnes concernées en ce qui concerne le traitement de données à caractère personnel et ont-elles connaissance des droits des personnes concernées ? Il s'agit de questions que nous avons soumises aux organisations sectorielles et aux quelques PME.

Dans la plupart des secteurs interrogés, les données à caractère personnel sont traitées à des fins de marketing et d'étude ainsi que pour l'exercice de l'activité principale des PME. Bzb-Fedafin, l'association professionnelle des intermédiaires indépendants en services bancaires et d'investissement, des intermédiaires en assurance et en crédit, indique que des données sont nécessaires pour pouvoir conseiller les clients, une obligation légale dans le secteur. Sans accès à ces données, les membres ne seraient pas en mesure de respecter cette obligation. Federgon, la fédération des opérateurs privés du marché du travail et des prestataires de services RH, indique également que les données à caractère personnel des personnes concernées sont nécessaires pour établir des contrats de travail. Cette situation est comparable à celle de Feprabel, la fédération des courtiers en assurance et intermédiaires financiers de Belgique. Les membres de l'organisation traitent des données à caractère personnel afin d'établir des offres et des contrats pour les clients. L'Association Pharmaceutique Belge indique également que les pharmaciens doivent disposer des données à caractère personnel des patients dans le cadre des dossiers de patients et des prescriptions afin de pouvoir proposer leur service. Les associations socioculturelles interrogées utilisent des données à caractère personnel principalement pour informer et contacter des clients (par exemple par des lettres d'information et des e-mails personnels) ainsi que pour l'administration du personnel et la gestion des membres.

Les personnes concernées ont-elles connaissance de ces processus de traitement ? Feprabel affirme que les personnes concernées sont informées via une fiche client, qu'ils doivent ensuite signer. Selon Bzb-Fedafin, les membres informent également les individus du traitement de leurs données à caractère personnel, mais une remarque critique s'impose : les personnes concernées ne savent pas nécessairement ce qu'il advient de leurs données à caractère personnel. Si une PME informe par exemple une personne concernée au début d'une conversation téléphonique que celle-ci sera enregistrée, il apparaît que cette personne concernée ne réalise pas toujours qu'il existe des enregistrements de telles conversations. Nous constatons que les organisations sectorielles tentent de sensibiliser les PME au niveau de l'information des personnes concernées, mais que cela n'est pas toujours une réussite dans tous les secteurs. La conscience de

communiquer de la manière la plus transparente possible aux personnes concernées n'est pas toujours présente

Un autre aspect de la transparence est le fait de permettre l'exercice des droits des personnes concernées. Il s'agit d'un élément identifié par les organisations sectorielles comme étant un des défis les plus pertinents des PME à l'égard du RGPD. Toutefois, beaucoup de PME manquent de connaissances au sujet de ces droits, d'une part, et il n'est pas toujours possible de faciliter leur exercice, d'autre part. Les personnes concernées ont par exemple le droit de faire supprimer des données à caractère personnel, mais dans certaines situations, c'est contraire à d'autres réglementations. Dans le secteur pharmaceutique, les PME doivent par exemple conserver les prescriptions pendant une durée déterminée, ce qui engendre une incertitude lorsque les personnes concernées demandent de supprimer des données. Les membres de Scwitch indiquent également ne pas avoir de connaissances au sujet de la suppression de données et ne seraient pas, d'après eux, en mesure de satisfaire les droits des personnes concernées.

Analyse d'impact relative à la protection des données : une obligation complexe comme cerise sur le gâteau

Un deuxième thème majeur du projet de recherche est l'analyse d'impact relative à la protection des données (AIPD). Une AIPD doit obligatoirement être réalisée lorsque le traitement de données peut engendrer un risque élevé pour les droits et libertés des personnes physiques. Il n'existe pas de définition univoque des processus de traitement à risque, mais bien quelques critères auxquels le traitement de données peut être confronté. Cela doit en d'autres termes être évalué au cas par cas par l'entreprise. L'AIPD doit être réalisée avant que les processus de traitement de données n'interviennent. Grâce à un registre de données, l'organisation a un aperçu de ses propres processus de traitement et l'on peut décider si la réalisation d'une AIPD est nécessaire. Il faut ensuite décider si l'organisation doit désigner un délégué à la protection des données (ci-après DPO, pour data protection officer). Autrement dit, différentes étapes doivent finalement conduire à la réalisation ou non d’une AIPD.

En ce qui concerne les risques des processus de traitement, quelques organisations sectorielles indiquent qu'il faut rarement réaliser des AIPD, étant donné que le traitement de données à caractère personnel n’entraîne pas d'emblée des conséquences risquées pour les personnes concernées. Les membres de Scwitch qui ont été interrogés affirment également que de nombreuses organisations dans le secteur sont convaincues qu'il n'y a pas de risques liés au traitement de données à caractère personnel. Nous constatons toutefois que quelques organisations sectorielles sont confrontées à des cyberattaques dans les PME. Selon les organisations interrogées, y compris les membres de Scwitch, il s'agit d'un risque significatif. Par ailleurs, Bzb-Fedafin affirme qu'il faut toujours tenir compte des erreurs humaines ainsi que des erreurs qui peuvent être commises par les fournisseurs de logiciels qui interviennent en tant que sous-traitants. Feprabel affirme que ses propres membres prennent suffisamment de mesures pour protéger les données à caractère personnel. Le contrôle des travailleurs au niveau des mesures de sécurité reste toutefois un défi pour les PME dans de nombreux secteurs. À la

question de savoir où la plupart des données à caractère personnel sont enregistrées, on répond que les PME utilisent des logiciels et des bases de données en ligne, fournies par des organisations externes. APB et Feprabel indiquent que les membres utilisent parallèlement des bases de données papier, laissant également la porte ouverte à des risques. Les membres de Scwitch le reconnaissent pour leur propre secteur. La perte de données papier et/ou d'appareils numériques (par exemple des ordinateurs portables) constituerait un risque significatif pour les associations.

Si une fuite de données se produit, les PME pourraient-elles entreprendre les démarches nécessaires ? Les résultats démontrent que de nombreuses PME ne savent pas quand il est question d'une fuite de données et ne savent pas comment y réagir concrètement. Dans le contexte du RGPD, chaque entreprise doit instaurer des procédures pour notifier des violations de données à caractère personnel, d'une part à l'APD, et d'autre part aux personnes concernées. On peut déduire des résultats que la sensibilisation en matière de fuites de données est absente chez beaucoup de PME et qu'elles font largement appel à l'aide des organisations sectorielles. Toutefois, il y a un risque qu'un certain nombre de fuites de données existantes passent ainsi sous le radar.

Les PME ont-elles ensuite une idée des flux d'information au sein de leur propre organisation ? Selon les organisations sectorielles interrogées, de nombreuses PME ne seraient pas en mesure d'établir un registre de traitement et/ou d'avoir une vue d'ensemble des flux d'information. Il s'agit là d'un défi car les données sont stockées sur différents serveurs de différents sous-traitants externes. Nous constatons que certaines organisations sectorielles offrent leur aide à cet égard. Feprabel établit par exemple en collaboration avec les membres un inventaire des sous-traitants avec lesquels il existe une collaboration et propose un registre de traitement standard via une application pour les membres. Scwitch souligne que la réalisation d'une présentation graphique des flux d'information est un exercice difficile pour de nombreux membres, mais que la majorité d'entre eux a quand même réussi à créer un registre de traitement. Les membres interrogés le confirment.

Enfin, de nombreuses PME manquent de connaissances en matière de réalisation d'une AIPD. Les PME ne savent pas suffisamment de quelle manière ni dans quelle situation elles doivent obligatoirement réaliser une AIPD. La réglementation serait en effet trop complexe. Les organisations sectorielles proposent des outils à cet égard (des templates par exemple) afin de venir en aide aux PME. Malgré tout, certaines d'entre elles indiquent qu'il manque chez beaucoup de PME non seulement des connaissances mais aussi la conscience de devoir réaliser une AIPD. D'autres organisations sectorielles affirment également qu'une AIPD est rarement nécessaire dans leur propre secteur. Parallèlement, les PME ne sauraient pas suffisamment dans quelles situations ni de quelle manière elles doivent désigner un délégué à la protection des données (DPO). Selon les organisations sectorielles, dans les informations diffusées, notamment par l'APD, l'accent est trop mis sur les responsabilités que doit assumer un DPO. Les PME voudraient plutôt savoir dans quelles situations elles sont obligées concrètement de désigner un DPO.

Les membres de Scwitch signalent aussi que la désignation d'un DPO est difficile pour beaucoup, vu le manque de temps et de moyens financiers.

En ce qui concerne la réalisation d'une AIPD et la désignation d'un DPO, nous concluons qu'il y a un besoin de disposer d'informations concrètes et applicables en pratique. Quelques organisations sectorielles indiquent que les secteurs ont besoin d'outils pratiques, développés et/ou vérifiés par l'APD.

Responsable du traitement et/ou sous-traitant ?

Le troisième thème de recherche concerne les notions de responsable du traitement et de sous-traitant, ainsi que leurs responsabilités décrites dans le RGPD. Selon le RGPD, le responsable du traitement est celui qui détermine la finalité et les moyens du traitement. L'entreprise qui traite des données à caractère personnel pour le compte d'un responsable du traitement est appelée sous-traitant. Toutefois, dans la pratique, il apparaît que la différence entre les deux n'est pas toujours claire.

Nous avons demandé aux organisations sectorielles dans quelle mesure les PME avaient connaissance de ces deux notions et si elles savaient dans quelle situation elles interviennent elles-mêmes en tant que responsable du traitement et/ou sous-traitant. De manière générale, les organisations sectorielles indiquent que les PME jouent dans la plupart des cas le rôle de responsable du traitement, mais qu'elles ne connaissent pas toujours elles-mêmes la différence entre les deux notions. Nous remarquons par exemple que Federgon déclare que pour de nombreux membres, il n'est pas toujours clair de savoir quand ils sont responsables du traitement. Vu la relation complexe entre les bureaux d'intérim et leurs clients, les membres ont des difficultés principalement avec la question de savoir quand le client est également responsable du traitement et si, en pareille situation, un contrat de sous-traitance doit être conclu entre les deux. Federgon indique aussi que pour les bureaux d'intérim, il est difficile également de déterminer s'ils sont eux-mêmes sous-traitants lorsque leur consultant traite des données à caractère personnel du client. L'organisation sectorielle adopte quand même un point de vue clair à l'égard de ses membres en ce sens qu'ils ne sont pas un sous-traitant notamment pour le travail intérimaire.

Bzb-Fedafin souligne aussi que pour les courtiers et les agents bancaires et d'assurances, il n'est pas évident de savoir quand ils sont responsables du traitement et/ou sous-traitants. Selon l'organisation, il est nécessaire de disposer d'un point de vue officiel des associations professionnelles et/ou de l'APD afin de pouvoir conseiller les PME dans certaines situations. Les membres de Scwitch affirment que les organisations connaissent les différences et les responsabilités théoriques, mais que l'application dans la pratique est difficile. Selon Scwitch elle-même, beaucoup ne savent pas clairement qui joue quel rôle en cas de coopération avec des tiers.

La collaboration avec des sous-traitants externes constitue un défi connexe. Les PME n'ont pas toujours connaissance des sous-traitants externes avec lesquels il existe une collaboration, ni dans quelles situations un contrat de sous-traitance doit être établi. Agoria indique par exemple que les PME ne savent pas clairement quand c'est nécessaire, et qu'il y a parallèlement un besoin de disposer d'outils pratiques pour établir de tels contrats. Selon Federgon et Feprabel, c'est également un défi pour les membres de pouvoir appréhender des contrats qui sont établis par des tiers. Si le sous-traitant soumet lui-même un contrat à signer, la PME doit-elle l'accepter ? Les intérêts commerciaux du tiers peuvent jouer un rôle important à cet égard et forcer la PME à signer de tels contrats. Les organisations sectorielles apportent leur aide aux PME dans de telles situations car celles-ci n'ont elles-mêmes que peu de connaissances à cet égard.

Besoins des PME et des organisations sectorielles

Nous constatons que de très nombreuses organisations sectorielles interrogées apportent déjà leur aide aux PME, sous la forme de conseils, de réponses à des questions pratiques, d'information des membres et d'aide aux membres via des outils et documents (en ligne). Les informations et outils proposés ne sont toutefois pas officiellement approuvés par l'APD, ce qui engendre pour de nombreuses organisations sectorielles des incertitudes quant aux avis donnés. **Les organisations sectorielles attendent de l'APD davantage de points de vue clairs, des informations pratiques et utiles pour les PME ainsi qu'une vérification des outils et de la documentation propres.** Actuellement, les questions pratiques ne trouvent que rarement une réponse, laissant de ce fait tant les organisations sectorielles que les PME dans l'incertitude quant au respect correct du RGPD. Une réponse à des problèmes concrets par secteur constituerait dès lors une avancée intéressante.

Selon les organisations sectorielles et les PME interrogées, l'aide aux PME en matière de RGPD devrait se concentrer sur : des templates et des exemples concrets (par exemple d'un registre de traitement ou d'une déclaration de confidentialité), des analyses d'impact relatives à la protection des données détaillées, des logiciels permettant aux PME d'établir des dossiers RGPD étayés, un site web de l'APD accessible et des manuels et/ou brochures. Ce qui revient chez toutes les organisations sectorielles, c'est la question de **l'aide sur mesure** (par exemple des applications développées par secteur) et de la simplification administrative.

Enfin, quelques organisations sectorielles indiquent rechercher un code de conduite officiel pour le secteur. La rédaction et la mise en œuvre communes d'un code de conduite serait une opportunité pour certains secteurs (comme l'indique Feprabel). Federgon a également tenté à plusieurs reprises de faire approuver des directives, mais sans succès. Quelques actions doivent toutefois être entreprises avant de pouvoir approuver et mettre en œuvre un code de conduite.[2]

[2] "Les codes de conduite dans le secteur privé ont besoin d'un organisme de contrôle approuvé par l'APD selon certains critères d'accréditation. L'APD était l'une des cinq premières autorités de contrôle de l'UE ayant soumis le projet de ses critères d'accréditation à l'avis du Comité européen de la protection des données (avis 02/2020). Au moment d'écrire ces lignes, l'APD met la touche finale à ces critères d'accréditation et vérifie avec ses partenaires européens si le projet de critères adapté tient suffisamment compte des remarques de l'avis du Comité européen

Conclusion

On peut conclure des paragraphes qui précèdent que le respect du RGPD n'est pas toujours évident pour les PME qui n'ont pas de conseiller interne et/ou externe. Les résultats révèlent que les PME rencontrent des obstacles, tant en ce qui concerne la transparence que les analyses d'impact relatives à la protection des données ou encore les notions de responsable du traitement et de sous-traitant. Ces défis sont dus à un manque de connaissance et de sensibilisation, d'une part, et à un manque d'informations et d'outils pratiques, d'autre part. Du fait que les PME ne disposent généralement pas des moyens et des connaissances pour (faire) transposer des documentations juridiques complexes en applications pratiques, l'APD et les organisations sectorielles doivent prévoir de tels outils et informations pratiques. D'après les organisations sectorielles interrogées, les PME ne sont généralement pas intéressées individuellement de réunir des connaissances sur le RGPD ; elles souhaitent en revanche principalement être soutenues par les instances utiles, en particulier les organisations sectorielles. Il faut garder à l'esprit que toutes les PME ne sont pas membres d'une organisation sectorielle et que l'on perd ainsi de vue une partie du marché.

Les résultats révèlent que la plupart des PME éprouvent tout d'abord des difficultés avec les démarches administratives à entreprendre pour respecter le RGPD. Il y a un besoin de disposer d'informations pratiques et utiles, simples à comprendre et de préférence appliquées à des problèmes concrets par secteur. Les PME ne souhaitent en effet pas réunir des connaissances au sujet de l'intégralité du règlement, mais veulent simplement se conformer elles-mêmes à la réglementation obligatoire.

de la protection des données. L'APD pourra ensuite adopter officiellement les critères d'accréditation pour les organismes de contrôle."

Annexes

Annexe 1: Informations contextuelles concernant les organisations sectorielles interrogées

Agoria
Agoria est la fédération professionnelle du secteur technologique et compte 2.000 membres qui emploient environ 275.000 travailleurs.

Association Pharmaceutique Belge
L'APB est la fédération nationale des pharmaciens d'officine indépendants. Les pharmacies sont affiliées à une union professionnelle locale. L'APB assure la défense et la promotion de la profession auprès des intervenants du secteur de la santé et soutient les membres dans l'exercice quotidien de leur métier. De plus amples informations sont disponibles sur le site Internet www.apb.be.

Bzb-Fedafin
BZB-Fedafin est une association professionnelle légalement reconnue qui défend les intérêts des intermédiaires en services bancaires et d'investissement, d'assurances et de crédit. BZB-Fedafin compte aujourd'hui plus de 2500 membres. Les membres sont actifs en tant qu'indépendants avec pour activité principale l'intermédiation en services bancaires et d'investissement, en assurances et/ou en crédits. Ils peuvent s'affilier individuellement ou via une affiliation collective de leur association d'agents. De plus amples informations sont disponibles sur le site Internet www.bzb-fedafin.be.

Federgon
Federgon, la fédération des opérateurs privés du marché du travail et des prestataires de services RH au niveau fédéral, représente les intérêts des grandes, petites et moyennes entreprises de différents secteurs : outplacement, intérim, recrutement, titres-services, intérim management, project sourcing, etc. De plus amples informations sont disponibles sur le site Internet www.federgon.be.

Feprabel
Feprabel est la fédération des courtiers d'assurances et intermédiaires financiers de Belgique. De plus amples informations sont disponibles sur le site Internet www.feprabel.be.

Scwitch
Scwitch est une société coopérative à finalité sociale du, par et pour le secteur socioculturel. Elle compte des organisations socioculturelles actives dans les domaines suivants : travail socioculturel, jeunesse, migration, lutte contre la pauvreté, travail de quartier, économie des services locaux, coopération au développement et à l'éducation, action environnementale, nature, centres culturels et communautaires, pratique d'art amateur, art graphique, art littéraire, musées, patrimoine, arts pédagogiques, travail socio-artistique, bibliothèques et médiathèques, centres

d'archives et de documentation, formation professionnelle et parcours d'expérience professionnelle, pratique sportive (non commerciale), tourisme, télévision (régionale) et radio (locale). De plus amples informations sont disponibles sur le site Internet www.scwitch.be.

Annexe 2 : Liste de sujets pour les réunions informelles

Sujet 1 : BOOST

- Questions relatives au projet de recherche ?
- Future collaboration au projet de recherche ?
- Comment faciliter le rayon d'action des PME ?

Sujet 2 : Le RGPD en général

- Le RGPD est-il un thème d'actualité ?
- Que propose l'organisation sectorielle pour soutenir les PME ?
- Recommandations à l'égard de l'APD
- Quels éléments le projet BOOST doit-il prévoir ?
- À quelles instances les PME s'adressent-elles pour obtenir des informations/une aide ?

Sujet 3 : Défis

- Quels sont les principaux défis auxquels les PME sont confrontées ?
- Les trois thèmes de BOOST sont-ils pertinents ?
- Y a-t-il d'autres thèmes importants à inclure ?
- Y a-t-il des cas concrets pour lesquels nous pouvons proposer des solutions ?

Sujet 4 : Transparence

- Quels sont les finalités des processus de traitement de données ?
- Les PME connaissent-elles les droits des personnes concernées ?

Sujet 5 : AIPD

- Où conserve-t-on actuellement la plupart des données à caractère personnel dans le secteur ?
- Les PME savent-elles comment et quand réaliser une AIPD ?
- Les PME savent-elles comment et quand désigner un DPO ?
- Quel est le plus grand risque en termes de traitement de données ?
- Qu'en est-il des fuites de données ?
- Les PME ont-elles une vue sur le flux de données ?

Sujet 6 : Responsable du traitement et sous-traitant

- Les PME connaissent-elles la différence entre les deux ?
- Les PME savent-elles à quel moment elles assurent quel rôle ?
- Les PME connaissent-elles les responsabilités ?
- Les PME connaissent-elles les sous-traitants ?