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

LA CONNAISSANCE ET LA COMPREHENSION DU REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES (RGPD) AU SEIN DES PME

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) au sein des petites et moyennes entreprises (PME) en Belgique. Ce rapport concerne les résultats du programme de travail 2, production 2.4., dont le but est de recenser la connaissance et la compréhension du RGPD au sein des PME. Cette production a été préparée par la Vrije Universiteit Brussel.

Nous aborderons successivement les sujets suivants : la connaissance et la compréhension des données à caractère personnel et des processus de traitement, le traitement de données à caractère personnel par les PME, la connaissance et la compréhension des notions de "responsable du traitement" et de "sous-traitant", la transparence des PME dans le contexte du RGPD, la connaissance et la compréhension de l'analyse d'impact relative à la protection des données (AIPD), des thèmes compliqués relatifs au RGPD et enfin le soutien des PME.

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

Cadre méthodologique

L'objectif de la production 2.4 est, au moyen d'un questionnaire quantitatif, 1/ de cerner la connaissance et la compréhension du RGPD au sein des PME et 2/ d'identifier les aides existantes et nécessaires ainsi que les problématiques urgentes. Le questionnaire mettait l'accent sur trois thèmes centraux dans le projet de recherche BOOST : la transparence, les notions de responsable du traitement et de sous-traitant et l'analyse d'impact relative à la protection des données. Le questionnaire se trouve dans les annexes (voir Annexe 1 : Enquête RGPD auprès des PME).

La première partie du questionnaire se composait d'un quiz de connaissances visant à évaluer la connaissance et la compréhension du RGPD au sein des PME et au besoin, à apporter les rectifications nécessaires. Le quiz comportait dix questions. Après avoir répondu à chaque question, les répondants recevaient les bonnes réponses ainsi que des explications. Par ces explications, nous entendions augmenter les connaissances du RGPD au sein des PME. La deuxième partie du questionnaire, composée de 17 questions, portait sur l'application du RGPD dans les entreprises elles-mêmes et sur les mécanismes d'aide existants et nécessaires.

Le questionnaire entendait répondre aux questions d'enquête suivantes :

- Les PME ont-elles une connaissance et une compréhension des notions de "données à caractère personnel" et de "traitement de données à caractère personnel", et quel est le rôle du traitement de données pour les PME ?
- Les PME connaissent-elles et comprennent-elles les trois thèmes centraux, à savoir les notions de "responsable du traitement" et de "sous-traitant", la transparence et l'analyse d'impact relative à la protection des données (AIPD), et comment appréhendent-elles ces notions dans la pratique ?
- Quels sont les thèmes du RGPD pour lesquels les PME éprouvent le plus de difficultés ?
- À quels acteurs et à quelles sources d'aide les PME font-elles appel afin de respecter le RGPD et quelles sont celles qui manquent ?

Le questionnaire était rédigé en français et en néerlandais. Les deux versions ont été utilisées en ligne du 08/05/2020 au 02/06/2020, en utilisant Qualtrics, et diffusées via le site Internet de l'APD et du Kenniscentrum Data & Maatschappij (Centre de connaissances Données et Société, https://data-en-maatschappij.ai). Il a été demandé par e-mail aux organisations sectorielles déjà impliquées (production 2.2) de diffuser le questionnaire à leurs propres membres. Sur demande, les PME pouvaient en outre compléter une version hors ligne du questionnaire. Les différences significatives dans les résultats des répondants francophones et néerlandophones sont abordées dans le volet empirique, si d'application.

Au total, 252 répondants ont complété le questionnaire. Toutefois, sur les 191 répondants néerlandophones, 97 ont complété l'enquête intégralement et 52 seulement partiellement. 42 répondants n'ont pas complété l'enquête et ne sont pas pris en considération. Sur les 61 répondants francophones, 28 répondants ont complété l'enquête intégralement et 11 seulement partiellement. 22 répondants n'ont pas complété l'enquête et ne sont pas pris en considération. Cela donne un nombre total de **188** répondants, dont **149 répondants néerlandophones et 39 répondants francophones**. À noter que nous avons pu atteindre un nombre plus important de répondants néerlandophones que de francophones.

Pour l'analyse des résultats, nous tenons toujours compte, pour chaque question, du nombre total de répondants ayant répondu à la question. Un aperçu est repris dans les annexes (voir Annexe 2 : Nombre de répondants par question). Nous sommes bien conscients du fait que le nombre définitif de répondants est insuffisant que pour tirer des conclusions représentatives pour l'ensemble des PME en Belgique. Les résultats de l'enquête n'en restent pas moins importants, car ils donnent un aperçu général de la situation actuelle au niveau de la connaissance et de la compréhension du RGPD au sein des PME et génèrent des informations permettant de concrétiser les étapes suivantes du projet de recherche.

Volet empirique : résultats d'étude

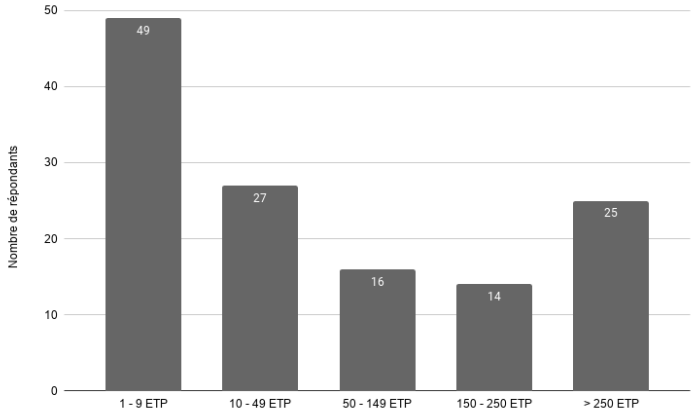
1. Caractéristiques des PME interrogées

Pour dresser un aperçu général des caractéristiques des PME interrogées et vérifier s'il y a des différences significatives sur la base de ces caractéristiques, nous nous sommes penchés sur 1/ le secteur d'activité de l'entreprise (voir Annexe 1 : Q10), 2/ le nombre d'ETP de l'entreprise (voir Annexe 1 : Q11) et 3/ le chiffre d'affaires annuel (voir Annexe 1 : Q12). Un total de 102 répondants néerlandophones et de 29 répondants francophones ont répondu à ces trois questions. Nous ne pouvons dès lors pas relier les données des répondants n'ayant pas répondu à ces questions à des caractéristiques spécifiques telles que le secteur ou la taille.

Pour commencer, parmi les répondants néerlandophones, la majorité indique travailler dans les secteurs de l'ICT, de la consultance et du management, du transport et de la logistique, de l'industrie, de l'intérim et des professions libérales. Un nombre important (N = 22) a complété un choix propre, les suivants étant les plus fréquents : e-commerce, traitement des salaires, sport, chèques-services, traduction et ingénierie, commerce, services, autorité publique, secteur juridique. Parmi les répondants francophones, la plupart des PME proviennent des secteurs ICT, de la consultance et du management ainsi que de l'industrie. Les chiffres exacts se trouvent dans les annexes (voir Annexe 3 : Secteurs des PME interrogées).

En ce qui concerne la taille des entreprises, nous avons obtenu les résultats suivants. La majorité des répondants (N = 49) emploient 1 à 9 ETP, mais de façon assez marquante, un nombre important d'entreprises (N = 25) emploient plus de 250 ETP, ce qui ne relève plus de la définition européenne de "PME"[1].

Graphique 1 : Nombre d'ETP des PME interrogées (Q11)



En ce qui concerne le chiffre d'affaires annuel, nous constatons que la plupart des PME interrogées (N = 38) se trouvent dans l'échelle inférieure, à savoir < 500.000 €. Par ailleurs, un grand nombre se trouvent dans l'échelle 2.000.000 € - 10.000.000 € (N = 26) et dans l'échelle 10.000.000 € - 50.000.000 € (N = 25).

[1] Telle que définie dans la Recommandation de la Commission du 6 mai 2003 *concernant la définition des micro, petites et moyennes entreprises,* C(2003) 1422, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32003H0361&from=FR

Nous pouvons en conclure que parmi les PME impliquées dans l'enquête, il y a une répartition selon la taille et le secteur, mais lorsque nous combinons les deux caractéristiques, il apparaît que la majorité des entreprises se trouvent dans l'échelle 1 - 9 ETP avec un chiffre d'affaires de < 500.000 € ainsi que dans l'échelle > 250 ETP avec un chiffre d'affaires de 10.000.000 € - 50.000.000 €. 25 entreprises contactées ne relèvent pas de la définition européenne de PME mais se comptent quand même dans ce groupe cible. Nous intégrons ces réponses dans notre analyse.

2. Connaissance et compréhension des données à caractère personnel et des processus de traitement

Nous avons commencé l'enquête par deux questions se rapportant à la connaissance et à la compréhension des PME au sujet 1/ des données à caractère personnel et 2/ du traitement de données à caractère personnel selon le Règlement général sur la protection des données (RGPD). Les PME ont-elles connaissance de ces deux éléments ?

La première question (voir Annexe 1 : Q1) demandait aux répondants de désigner quels documents contiennent des données à caractère personnel et/ou quelles catégories sont considérées comme des données à caractère personnel selon le RGPD. À la deuxième question (voir Annexe 1 : Q2), les répondants devaient désigner les activités qui sont considérées comme un traitement de données à caractère personnel en vertu du RGPD. Les résultats donnent la répartition suivante, représentée dans le tableau ci-dessous.

Tableau 1 : Connaissance et compréhension des notions de données à caractère personnel et de traitement de données à caractère personnel chez les répondants (Q1 & Q2)

Quelles catégories relèvent des données à caractère personnel ?			**Quelles activités relèvent du traitement de données à caractère personnel ?**		
Réponse tout à fait correcte	Réponse partiellement correcte	Réponse incorrecte	Réponse tout à fait correcte	Réponse partiellement correcte	Réponse incorrecte
N = 106	N = 57	N = 21	N = 94	N = 53	N = 24
Nombre total de répondants		N = 184	Nombre total de répondants		N = 171

Les résultats indiquent que seule une minorité des répondants ont indiqué les possibilités de réponse erronées. À la première question, les "données anonymisées sans lien avec une personne" et "une adresse e-mail générale" ne font pas partie de ce qu'on appelle les données à caractère personnel. Seuls 19 répondants étaient convaincus qu'une adresse e-mail générale était considérée comme une donnée à caractère personnel. À la deuxième question, le simple "enregistrement d'une adresse e-mail générale d'une entreprise dans un fichier" n'est pas un traitement de données à caractère personnel, ce que seuls quelques répondants ont indiqué être

correct. Nous pouvons ensuite **conclure que la majorité des répondants ont une bonne compréhension des catégories qui relèvent bien des données à caractère personnel et du traitement de données à caractère personnel** en vertu du RGPD. Environ 58 % (N = 106) des répondants ont su répondre tout à fait correctement à la première question. Pour la deuxième question, le résultat est de 55 % (N = 94).

On peut déduire de ce qui précède que **les connaissances de base et la compréhension de ce qu'impliquent les données à caractère personnel et le traitement de données à caractère personnel sont acquises dans une forte mesure pour la grande moitié des PME interrogées**.

3. Traitement de données à caractère personnel par les PME

Nous nous sommes également demandé dans quelle mesure les PME elles-mêmes traitaient des données à caractère personnel et nous nous sommes dès lors intéressés à deux éléments : 1/ quelle est l'importance du traitement de données à caractère personnel pour les PME, et 2/ de quelles catégories de personnes concernées collecte-t-on et traite-t-on des données à caractère personnel.

Les résultats de la question de savoir quelle est l'importance du traitement de données à caractère personnel pour l'entreprise (voir Annexe 1 : Q13) laissent apparaître que pour la majorité (N = 38), le **traitement de données vient en appui de l'activité principale.** Dans quelques cas (N = 38), le traitement de données à caractère personnel fait partie du modèle d'entreprise. Seuls quelques répondants (N = 3) pourraient travailler sans traitement de données à caractère personnel.

Tableau 2 : Importance du traitement de données pour le nombre total de répondants

Données à caractère personnel occupant une place centrale dans le modèle d'entreprise	Données à caractère personnel en appui à l'activité principale	Possibilité de travailler sans données à caractère personnel	*Aucune idée*
N = 38	N = 82	N = 3	N = 8
Nombre de répondants : 131			

Si on analyse les résultats par secteur, on ne relève pas de différence significative. Ce qui frappe dans l'analyse des résultats, c'est le fait que les PME du même secteur donnent généralement chacune un retour différent, ce qui nous permet de conclure que soit les répondants ne sont pas suffisamment au courant de l'importance du traitement de données pour leur propre entreprise, soit qu'il y a des différences entre les PME qui travaillent dans le même secteur.

Ensuite, lorsque nous analysons les résultats en combinaison avec la connaissance de l'entreprise au sujet du RGPD – sur la base des scores obtenus pour les questions de connaissance du questionnaire -, nos constatations sont les suivantes. La majorité des entreprises pour lesquelles le traitement de données à caractère personnel occupe une place centrale dans le modèle d'entreprise ont une connaissance moyenne à bonne du RGPD, mais un nombre important n'a qu'une connaissance et une compréhension moyennes à insuffisantes. Il en va de même pour les entreprises pour lesquelles le traitement de données à caractère personnel

constitue un soutien à l'activité principale. Cela signifie que pour un certain nombre de PME, le traitement de données à caractère personnel est essentiel à l'activité de l'entreprise, mais la connaissance et la compréhension du RGPD sont encore insuffisantes.

À la question de savoir de quelles catégories de personnes concernées collecte-t-on et traite-t-on des données à caractère personnel (voir Annexe 1 : Q15), il apparaît qu'il s'agit principalement des catégories suivantes : **clients, collaborateurs et fournisseurs**. Viennent ensuite également des clients potentiels et des candidats. Les données à caractère personnel fournies par un donneur d'ordre et les données de visiteurs de sites Internet sont des catégories de données à caractère personnel moins fréquentes.

4. Connaissance et compréhension des notions de "responsable du traitement" et de "sous-traitant"

Le premier thème central du projet de recherche vise la connaissance et la compréhension des concepts "responsable du traitement" et "sous-traitant". Un cluster de sept questions concernait la connaissance des PME sur ces notions, ainsi que l'application en pratique.

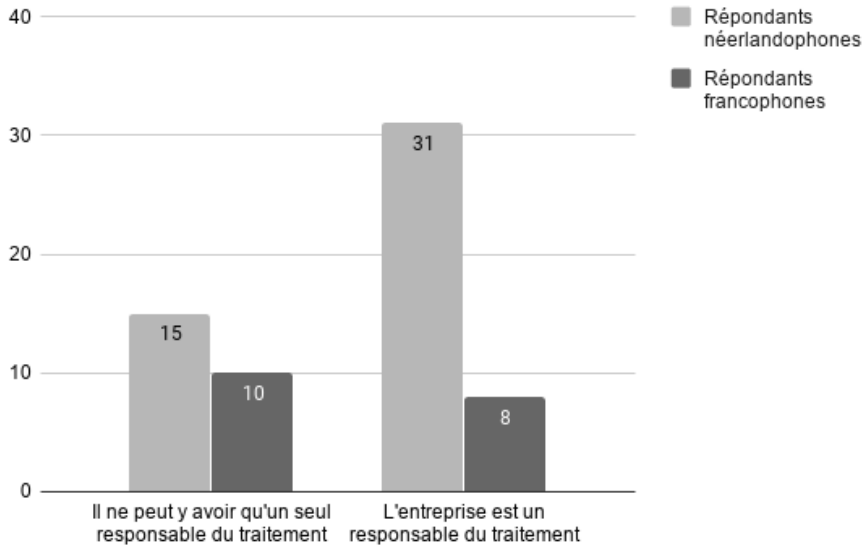
Connaissance et compréhension des deux concepts

Pour commencer, nous avons soumis aux répondants quelques affirmations concernant ces deux notions et nous leur avons demandé d'identifier celles qui sont correctes et celles qui sont incorrectes au regard du RGPD (voir Annexe 1 : Q4). Sur 120 répondants néerlandophones ayant répondu à la question, 55 ont su donner une réponse tout à fait correcte. Sur 33 répondants francophones, ils étaient 10 à pouvoir le faire. Bien que parmi les autres participants, une grande majorité a obtenu un bon score, il est néanmoins frappant de constater que de nombreuses PME ont indiqué les possibilités de réponse incorrectes, à savoir :

- "il ne peut y avoir qu'un seul responsable du traitement"
- "l'entreprise qui collecte les données à caractère personnel et les traite pour le compte d'une autre entreprise est un responsable du traitement".

Les résultats relatifs aux possibilités de réponse incorrectes se trouvent dans le Graphique 2.

Graphique 2 : Résultats concernant les affirmations incorrectes sur le "responsable du traitement" et sur le "sous-traitant" (Q4)



Ensuite, nous avons soumis aux répondants quelques affirmations pratiques sur les deux notions. La première affirmation était formulée comme suit (voir Annexe 1 : Q5) :

> *Une boulangerie collabore avec une entreprise qui propose une carte de fidélité gratuite et collecte à cet effet des données à caractère personnel de la clientèle. La boulangerie n'est pas responsable si une fuite de données se produit chez le fournisseur de la carte de fidélité."*

La bonne réponse, à savoir qu'il s'agit d'une responsabilité partagée entre la boulangerie et l'entreprise, a été donnée par environ 66 % (N = 79) des répondants néerlandophones (N = 120) et environ 63 % (N = 10) des répondants francophones (N = 16). Bien que la majorité ait évalué la situation correctement, nous devons constater qu'un grand nombre de participants ont répondu erronément.

La deuxième affirmation était formulée comme suit : "*Une entreprise de gestion des salaires est-elle responsable du traitement de données à caractère personnel qu'elle traite pour une autre entreprise ?*" (voir Annexe 1 : Q6a). La bonne réponse, à savoir que l'entreprise de gestion des salaires est un sous-traitant, a été donnée par environ 69 % (N = 81) des participants néerlandophones et par 55 % (N = 18) des participants francophones. On note qu'un grand nombre (N = 46) parmi tous les répondants estime que l'entreprise de gestion des salaires assure aussi bien le rôle de responsable du traitement que de sous-traitant.

Une question supplémentaire était posée aux répondants au sujet de cette affirmation : *"Si une fuite de données a lieu au sein de l'entreprise de gestion des salaires, doit-elle entreprendre des démarches elle-même ?"* (voir Annexe 1 : Q6b). Environ 95 % des participants néerlandophones et 79 % des participants francophones ont répondu correctement à cette question.

On peut en conclure que les **connaissances théoriques et pratiques concernant les notions de "responsable du traitement" et de "sous-traitant" ne sont suffisantes que chez un peu**

plus de la moitié des PME interrogées. La bonne évaluation du rôle et des responsabilités des deux intervenants dans des situations concrètes est une pierre d'achoppement pour une grande partie des PME. On observe une corrélation importante entre la connaissance et la compréhension des deux notions et le secteur et la taille des PME interrogées.

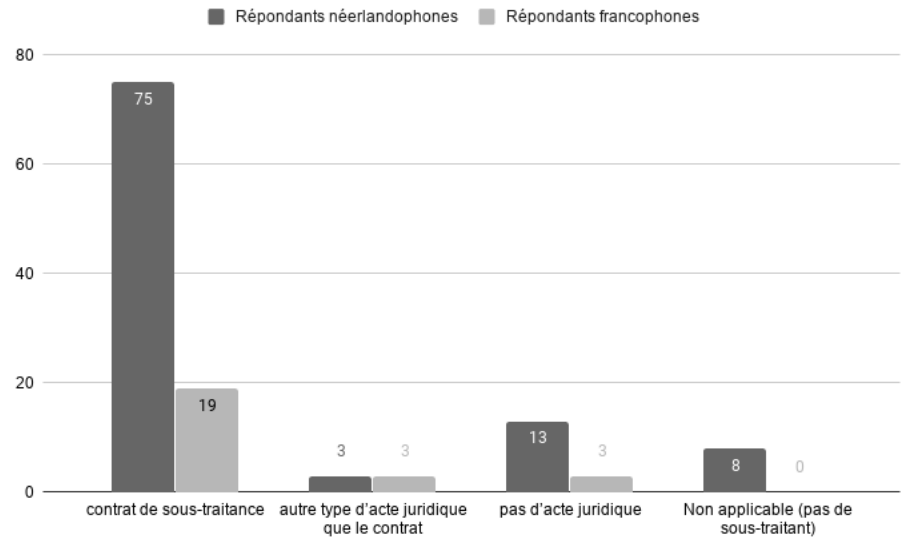
Application pratique des deux notions

En plus de déterminer la connaissance et la compréhension des notions de "responsable du traitement" et de "sous-traitant", nous avons également posé quelques questions aux PME au sujet de l'application dans leur propre entreprise.

Pour commencer, à la question de savoir si l'entreprise intervient principalement en tant que responsable du traitement, sous-traitant ou les deux (voir Annexe 1 : Q16), il apparaît qu'environ la moitié (N = 65) de tous les répondants (N = 124) agissent en tant que responsable du traitement. Ensuite, une partie (N = 38) affirme assurer les deux fonctions. Seules quelques PME (N = 17) – dont la plupart font partie du secteur ICT – indiquent assurer seulement le rôle de sous-traitant.

Nous nous sommes ensuite penchés sur la collaboration avec les sous-traitants en demandant quels documents juridiques les PME utilisent pour encadrer un traitement de données à caractère personnel par un sous-traitant (voir Annexe 1 : Q17). D'après les résultats, la majorité (N = 94) du nombre total de répondants ayant répondu à la question (N = 124) utilisent principalement des contrats de sous-traitance. D'autres types de contrats ou de documents juridiques ne sont que rarement utilisés. Les résultats indiquent (voir Annexe 1 : Q18) que la majorité des PME utilisent pour ces documents juridiques un modèle propre ou un modèle établi par des experts externes.

Graphique 3 : Encadrement du traitement de données à caractère personnel par des sous-traitants (Q17)



5. La transparence des PME dans le contexte du RGPD

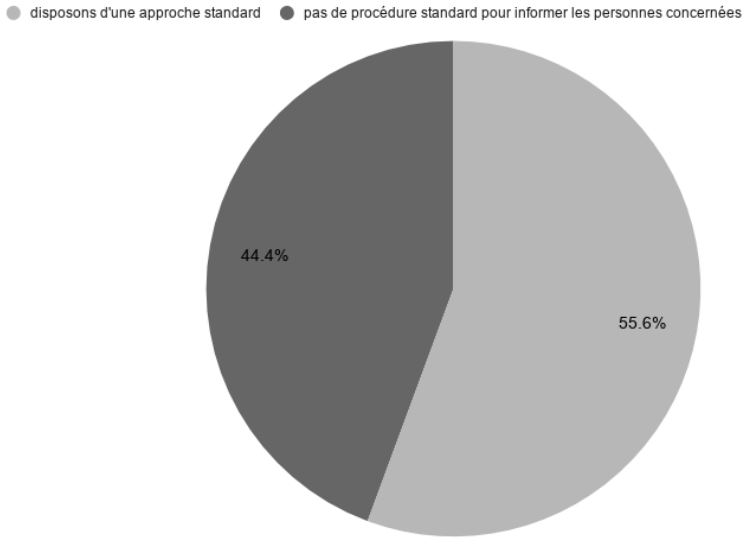
Le deuxième thème central de la recherche était la transparence. Pour être transparentes, les entreprises doivent informer les personnes concernées du traitement de données à caractère personnel. Un langage clair et simple doit être utilisé. Les déclarations de confidentialité jouent ici un rôle crucial. Nous avons demandé aux PME quelles informations devaient être reprises dans une déclaration de confidentialité (voir Annexe 1 : Q8) afin de cerner leur connaissance et leur compréhension en matière de transparence.

Sur 114 répondants néerlandophones ayant répondu à la question, seuls 22 ont su répondre tout à fait correctement. Même si les autres répondants ont obtenu un bon score, nous constatons que 36 répondants néerlandophones ont indiqué la mauvaise possibilité de réponse, à savoir "les démarches que vous entreprenez pour réaliser une analyse d'impact relative à la protection des données (AIPD)". Chez les 31 participants francophones ayant répondu à la question, 11 ont su donner une réponse tout à fait correcte. Seuls 4 répondants ont indiqué la mauvaise possibilité de réponse. De manière générale, on peut affirmer que – principalement chez les répondants néerlandophones – **la connaissance et la compréhension théoriques à l'égard des déclarations de confidentialité est insuffisante.**

Nous nous sommes ensuite intéressés à l'application des déclarations de confidentialité dans les entreprises elles-mêmes (voir Annexe 1 : Q19). Les résultats indiquent que la majorité des répondants estiment que leurs **propres déclarations de confidentialité 1/ contiennent toutes les informations en vertu du RGPD et 2/ sont mises à jour et disponibles de manière visible (sur le site Internet)**. On remarque que neuf répondants néerlandophones et cinq répondants francophones indiquent n'utiliser aucune déclaration de confidentialité, bien que ce soit bel et bien nécessaire pour l'entreprise en vertu du RGPD.

Enfin, à quel point les PME s'estiment-elles transparentes à l'égard des personnes concernées ? À la question de savoir si les PME disposent d'une procédure standard (par exemple un template, un site Internet, un fichier) pour informer les personnes concernées d'un traitement de données (voir Annexe 1 : Q20), environ 56 % des répondants réagissent par l'affirmative. Les autres participants déclarent ne pas disposer d'une approche standard.

Graphique 4 : Disponibilité d'une procédure standard pour informer les personnes concernées (Q20)



6. Connaissance et compréhension de l'analyse d'impact relative à la protection des données (AIPD)

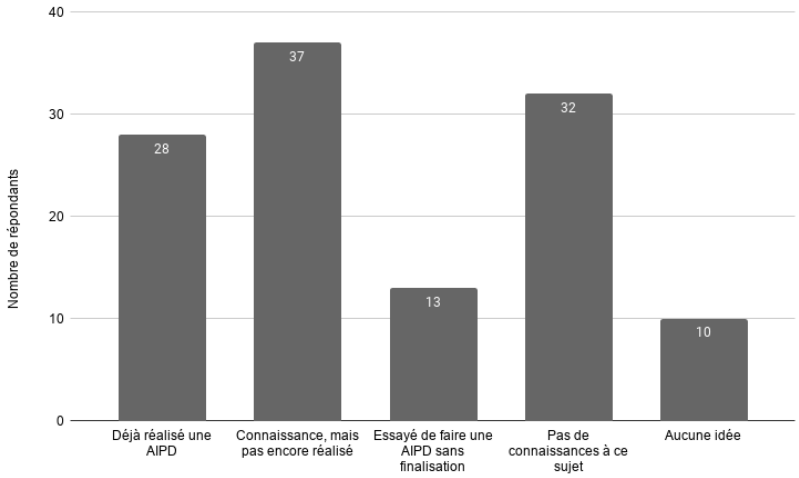
Le troisième et dernier thème central du projet de recherche est l'analyse d'impact relative à la protection des données (AIPD). Selon le RGPD, les entreprises doivent réaliser une AIPD si le traitement de données à caractère personnel peut donner lieu à des risques pour les personnes physiques. Les PME connaissent-elles et comprennent-elles cela ?

Nous avons demandé aux répondants s'ils savaient dans quelle situation une AIPD doit être réalisée, avec quelques situations d'illustration à sélectionner (voir Annexe 1 : Q9). La simple situation suivante est erronée **:**
"Un magazine en ligne utilisant un listing d'adresses pour envoyer un message générique quotidien à ses abonnés. Le traitement est à grande échelle, mais le risque est faible et la personne concernée peut se désinscrire facilement."

Sur 104 répondants néerlandophones, 44 ont su répondre tout à fait correctement à la question et 22 ont donné une réponse erronée. Sur 30 répondants francophones, 13 ont répondu tout à fait correctement à la question et 12 ont donné la mauvaise possibilité de réponse. Cela signifie qu'un grand nombre **des PME interrogées n'ont pas de connaissances suffisantes des situations dans lesquelles une AIPD doit être réalisée**.

Nous avons ensuite interrogé les PME sur l'application de l'AIPD dans leur propre entreprise en leur demandant si leur entreprise sait quand et comment une AIPD doit être réalisée correctement (voir Annexe 1 : Q21).

Graphique 5 : Connaissance concernant l'AIPD dans la propre entreprise (Q21)



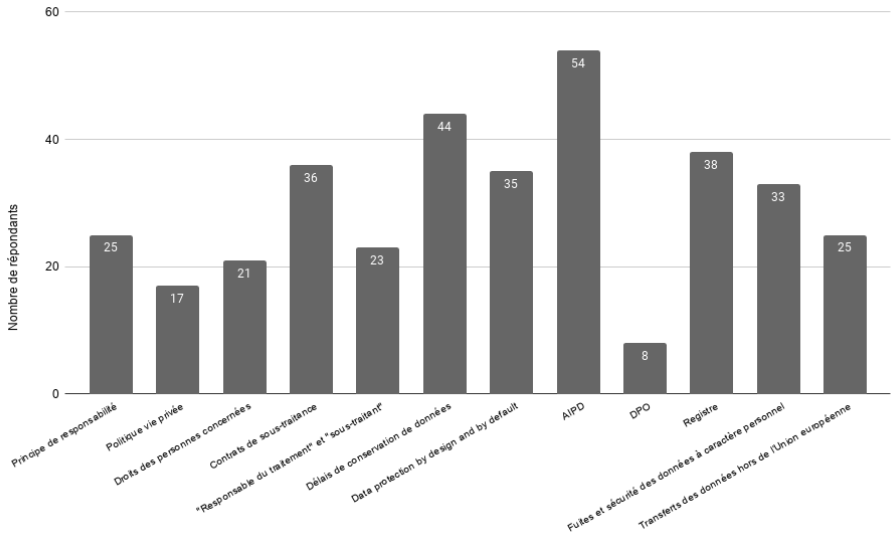
Les résultats font apparaître que la majorité des répondants (N = 37) indiquent disposer de connaissances pour réaliser une AIPD, mais qu'ils n'ont pas encore dû l'appliquer en pratique. On note qu'un grand nombre **de PME (N = 32) déclare ne pas disposer de connaissances suffisantes pour savoir quand et comment réaliser une AIPD correctement**. En outre, de très nombreux répondants (N = 28) ont déjà réalisé eux-mêmes une AIPD dans l'entreprise. Autrement dit, les résultats sont très disparates d'une PME à l'autre.

7. Thèmes compliqués du RGPD pour les PME

Outre les trois thèmes centraux du projet de recherche, nous nous sommes également intéressés à d'autres sujets qui suscitent des difficultés pour les PME. Nous leur avons demandé quels thèmes du RGPD posaient le plus de problèmes aux entreprises, avec une liste de possibilités, ainsi que l'option champ libre permettant d'indiquer eux-mêmes des problèmes (voir Annexe 1 : Q25). Plusieurs thèmes ont pu être identifiés.

Si on analyse conjointement les résultats des répondants francophones et des répondants néerlandophones, nous en arrivons à la conclusion suivante, illustrée dans le graphique ci-dessous.

Graphique 6 : Thèmes du RGPD les plus difficiles pour les PME (Q25)



Les résultats indiquent que les PME ont principalement des difficultés (et ont besoin d'aide) avec les thèmes suivants : l'analyse d'impact relative à la protection des données (AIPD), les délais de conservation de données à caractère personnel, le registre des processus de traitement de données, les contrats de sous-traitance avec des externes et les principes de "protection des données dès la conception et par défaut". On ne relève pas de différence significative entre répondants néerlandophones et répondants francophones, mais il convient toutefois de noter que les fuites de données et la sécurité des données à caractère personnel sont aussi des thèmes fréquemment indiqués par les participants francophones.

Si on analyse les résultats plus en détail au vu de la taille de l'entreprise, on remarque qu'il n'y a pas de différence significative, à l'exception du fait que les petites entreprises comptant 1 - 9 ETP ont essentiellement des problèmes avec les thèmes contrats de sous-traitance avec des tiers, AIPD, registre des activités de traitement et les principes de "protection des données dès la conception et par défaut". Pour les autres catégories d'entreprises, les scores sont plus disparates dans les divers thèmes.

Nous en concluons que les PME éprouvent divers problèmes dans la mise en œuvre du RGPD, où principalement l'AIPD correspond à un des trois thèmes centraux du projet de recherche. La majorité des répondants a sélectionné entre un et trois thèmes pour lesquels ils éprouvent des difficultés. Seuls quelques-uns en ont sélectionné plus de six.

8. Le soutien des PME concernant le respect du RGPD

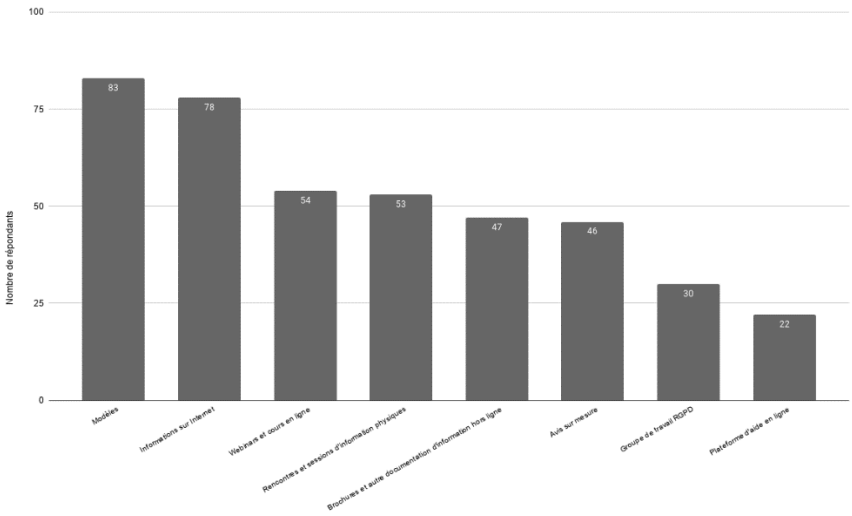
Pour terminer, nous avons posé quelques questions aux PME concernant le soutien qu'elles reçoivent pour respecter le RGPD. Tout d'abord, à quels acteurs les PME font-elles appel (voir Annexe 1 : Q22) ? Les résultats indiquent que les répondants demandent conseil principalement aux organisations sectorielles ou professionnelles (N = 67), ont recours à des informations disponibles en ligne (N = 42), à un DPO interne (N = 41) et/ou à des consultants ou à un service

juridique externes (N = 40). L'Autorité de protection des données est moins fréquemment mentionnée (N = 33), mais se révèle être aussi une source d'aide importante. À noter que seuls dix participants indiquent ne faire appel à aucun acteur pour obtenir de l'aide.

Les résultats indiquent clairement que les petites entreprises (catégories 1 à 149 ETP) font plutôt appel à des organisations sectorielles et professionnelles et/ou à des consultants et services juridiques externes. Pour les grandes entreprises (catégories > 150 ETP), on fait plutôt appel à des délégués à la protection des données en interne (Data Protection Officers ou DPO) et/ou à un service juridique interne.

Quelles sources d'aide sont ensuite utilisées par les PME concernant le RGPD (voir Annexe 1 : Q23) ? Il ressort des résultats que les PME ont principalement recours à des templates (N = 83), à des informations disponibles sur des sites Internet (N = 78), à des webinaires et cours en ligne (N = 54) et à des réunions et sessions d'information physiques (N = 53). Les plateformes d'assistance en ligne et les groupes de travail RGPD ont moins souvent été sélectionnés. On n'observe pas de différence notoire basée sur le secteur et/ou la taille des entreprises interrogées.

Graphique 7 : Sources d'aide utilisées par les PME (Q23)



Enfin, quelles sources d'aide manquent selon les PME (voir Annexe 1 : Q24) ? Sur 97 répondants néerlandophones ayant répondu à la question, on note qu'une grande partie (N = 39) indique qu'aucune source d'aide ne fait défaut. Par ailleurs, les sources d'aide suivantes manquent selon les entreprises : **avis sur mesure par téléphone et/ou par e-mail, groupes de travail RGPD et plateformes d'assistance en ligne**. Chez les répondants francophones (28 ayant répondu à la question), les résultats indiquent que seuls 14 % (N = 4) estiment qu'aucune source d'aide ne manque. Les autres répondants pointent principalement l'absence de plateformes d'assistance en ligne, de templates et d'avis sur mesure par téléphone et/ou par e-mail, des résultats comparables à ceux des répondants néerlandophones.

9. Résultats globaux

Lorsque nous analysons enfin les scores des PME interrogées pour le quiz de connaissances, nous constatons que seuls cinq répondants néerlandophones ont répondu tout à fait correctement à toutes les questions. Ces PME proviennent du secteur de la consultance et du management, des services et de l'e-commerce. Deux des répondants emploient 1 - 9 ETP, deux autres 150 - 250 ETP. En outre, 22 répondants néerlandophones n'ont commis aucune erreur, mais n'ont donc pas répondu tout à fait correctement à toutes les questions. Pour qu'une réponse soit tout à fait correcte, les répondants devaient en effet avoir indiqué toutes les possibilités de réponse correctes. Parmi les répondants francophones, seules deux PME interrogées ont su répondre tout à fait correctement à toutes les questions. Ces deux entreprises emploient chacune 150 - 250 ETP et font partie des secteurs de l'ICT et de la banque-assurance. Un total de cinq répondants francophones n'ont commis aucune erreur.

Le nombre de répondants du questionnaire est trop faible pour se prononcer correctement sur l'importance de la taille et du secteur des entreprises pour la connaissance et la compréhension du RGPD. Les résultats ci-dessus ne donnent en outre que peu de corrélations en ce qui concerne les caractéristiques des PME et les connaissances en matière de RGPD.

Conclusion

Le questionnaire avait pour objectif de cerner la connaissance et la compréhension du RGPD au sein des PME ainsi que les mécanismes d'aide existants ou nécessaires. Pour le premier aspect, nous constatons de manière générale que la connaissance et la compréhension des PME ne sont pas aussi pointues dans tous les domaines. Un grand nombre d'entreprises interrogées disposent de connaissances théoriques suffisantes quant aux implications des données à caractère personnel et du traitement de données à caractère personnel en vertu du RGPD. Toutefois, pour ce qui est des trois thèmes centraux du projet de recherche (à savoir les notions "responsable du traitement" et "sous-traitant", la transparence et l'analyse d'impact relative à la protection des données (AIPD)), les résultats sont disparates.

Les connaissances théoriques et pratiques sur les notions de "responsable du traitement" et de "sous-traitant" ne sont suffisamment acquises que chez un peu plus de la moitié des PME interrogées. Pour un grand nombre de PME, la compréhension du rôle et des responsabilités des deux notions n'est pas suffisante. Concernant le thème de la transparence, nous constatons que les connaissances théoriques et la compréhension en matière de déclarations de confidentialité sont manquantes chez de nombreuses PME interrogées, bien que la majorité d'entre elles indiquent que leurs propres déclarations de confidentialité répondent aux obligations du RGPD. En outre, un peu plus de la moitié des entreprises interrogées disposeraient d'une procédure standard pour informer les personnes concernées des processus de traitement.

Le troisième thème est l'obstacle le plus important : l'AIPD. Un grand nombre des PME interrogées disposent de connaissances théoriques insuffisantes sur les situations dans lesquelles une AIPD doit être appliquée. Pour ce qui est de l'application pratique, il apparaît que la majorité des PME disposeraient des connaissances pour réaliser une AIPD, mais n'ont pas encore dû les utiliser en pratique. Malgré cela, un nombre important de PME avouent ne pas savoir suffisamment comment et quand réaliser une AIPD correctement. L'AIPD est en outre citée comme un des thèmes du RGPD pour lesquels les PME éprouvent le plus de problèmes. D'autres thèmes cités (et pour lesquels une aide est nécessaire) sont les délais de conservation des données à caractère personnel, le registre des processus de traitement de données, les contrats de sous-traitance avec des externes et les principes de "protection des données dès la conception et par défaut".

En ce qui concerne le deuxième objectif, la détermination des mécanismes d'aide existants et nécessaires, nous constatons que les PME font principalement appel à des organisations sectorielles et professionnelles et à des informations en ligne. Les "petites" entreprises s'en remettent plutôt à des consultants et à des services juridiques externes, alors que les "grandes" entreprises font généralement appel à un délégué à la protection des données (DPO) interne et/ou à un service juridique interne. Actuellement, les PME utilisent principalement des templates, des informations en ligne, des webinaires et cours en ligne ainsi que des réunions et sessions d'information physiques pour pouvoir se conformer au RGPD. Les sources d'aide manquantes sont principalement les avis sur mesure (téléphone et/ou e-mail), les plateformes d'assistance en ligne et enfin les groupes de travail.

Annexes

Annexe 1 : Enquête RGPD auprès des PME

PARTIE I : Vos connaissances du RGPD (quiz)

Pour chaque question, vous trouverez plusieurs possibilités de réponse dans un tableau. Pour chaque réponse que vous souhaitez sélectionner, veuillez mettre une X dans la colonne de gauche (si plusieurs réponses doivent être sélectionnées) ou, si indiqué, souligner la réponse correcte.

Pour certaines questions, plusieurs réponses devront être données. Ce sera indiqué chaque fois au regard de la question.

Note : Les réponses correctes du quiz sont disponibles à la fin de ce document. Veuillez toutefois laisser vos réponses initiales dans le document que vous nous renvoyez.

Q1 : Quels documents contiennent des données à caractère personnel ou quelles données relèvent des "données à caractère personnel" ? *(plusieurs réponses possibles)*

	Adresse IP
	Numéro de Registre national
	Données biométriques (par exemple une empreinte digitale)
	Certificat médical
	Photo d'un intérimaire ou d'un client
	Évaluation du personnel
	Extrait du casier judiciaire
	Fiche de salaire d'un travailleur
	Données anonymisées sans lien avec une personne (par exemple "nombre de clients qui ont commandé notre produit en 2018")
	Une adresse e-mail générale (par exemple info@wallonie.be)

Q2 : Quelles activités constituent un "traitement" de données à caractère personnel au sens du RGPD ? *(plusieurs réponses possibles)*

	Vendre une banque de données d'adresses e-mail personnelles à un tiers
	Supprimer des e-mails de clients
	Fournir au client le numéro de Registre national d'un intérimaire
	Enregistrer une lettre de candidature sur le serveur
	Tenir systématiquement des fiches papier organisées avec les données de clients
	Demander des données RH de travailleurs à l'entreprise de gestion des salaires
	Encoder l'adresse e-mail générale d'une entreprise dans un fichier électronique

Q3 : Mythe ou réalité ? Le traitement de données à caractère personnel n'est jamais permis sans le consentement de la personne concernée.

Réponse : _____*(écrivez ici mythe ou réalité)*

Q4 : Indiquez ce qui est exact selon le RGPD *(plusieurs réponses possibles)*

	Le fait de déterminer les finalités du traitement des données à caractère personnel est un indice important du fait qu'on est le responsable du traitement (seul ou conjointement avec d'autres)
	Le fait de déterminer les moyens du traitement des données à caractère personnel est un indice important du fait qu'on est le responsable du traitement (seul ou conjointement avec d'autres)
	Il ne peut y avoir qu'un seul responsable du traitement

	L'entreprise qui collecte les données à caractère personnel et les traite pour le compte d'une autre entreprise est un responsable du traitement
	Le responsable du traitement détermine le fondement légal du traitement de données
	Le sous-traitant peut seulement traiter des données sur la base d'instructions du responsable du traitement

Q5 : Imaginez la situation suivante. Une boulangerie collabore avec une entreprise qui propose une carte de fidélité gratuite et collecte à cet effet des données à caractère personnel de la clientèle. La boulangerie n'est pas responsable si une fuite de données se produit chez le fournisseur de la carte de fidélité.
Veuillez indiquer une seule réponse en la soulignant.

- Faux. La boulangerie doit assumer l'entière responsabilité de la fuite de données.
- Faux. L'entreprise qui collecte les données des clients doit assumer l'entière responsabilité de la fuite de données.
- Il s'agit d'une responsabilité partagée entre la boulangerie et l'entreprise.

Q6a : Une entreprise de gestion des salaires est-elle responsable du traitement de données à caractère personnel qu'elle traite pour une autre entreprise ?
Veuillez indiquer une seule réponse en la soulignant.

- L'entreprise de gestion des salaires est responsable du traitement
- L'entreprise de gestion des salaires est un sous-traitant
- L'entreprise de gestion des salaires est un responsable du traitement et un sous-traitant

Q6b : Si une fuite de données a lieu au sein de l'entreprise de gestion des salaires, doit-elle entreprendre des démarches elle-même ?
Veuillez indiquer une seule réponse en la soulignant.

- Oui
- Non

Q7 : Mythe ou réalité : chaque entreprise est obligée de désigner un délégué à la protection des données (DPO).

Réponse : _____*(écrivez ici mythe ou réalité)*

Q8 : Quelles informations devez-vous reprendre dans une déclaration de confidentialité ? *(plusieurs réponses possibles)*

	Les catégories de données à caractère personnel que votre entreprise collecte et traite

	Les étapes que vous suivez pour réaliser une analyse d'impact relative à la protection des données (AIPD)
	Les coordonnées (nom, adresse, adresse e-mail, numéro de téléphone) du responsable du traitement
	Le fondement légal pour le traitement de données à caractère personnel
	Les coordonnées du délégué à la protection des données (si d'application)
	La manière dont votre entreprise traite des données à caractère personnel
	Le délai de conservation des données à caractère personnel ou une indication des critères utilisés pour déterminer ce délai
	Les tiers avec lesquels votre entreprise partage les données à caractère personnel et/ou qui ont accès aux données à caractère personnel
	La manière dont votre entreprise protège les données à caractère personnel
	Les droits de la personne concernée
	La source des données à caractère personnel (d'où vous obtenez les données à caractère personnel) lorsque les données n'ont pas été collectées auprès de la personne concernée

Q9 : Dans quelles situations devez-vous obligatoirement réaliser une analyse d'impact relative à la protection des données (AIPD) ? *(plusieurs réponses possibles)*

	Lors du traitement de données biométriques (par exemple la reconnaissance faciale, les empreintes digitales) en vue de l'identification des personnes concernées se trouvant dans un lieu public ou dans des lieux privés accessibles au public

	Lorsque des données de santé d'une personne concernée sont collectées par voie automatisée à l'aide d'un dispositif médical implantable actif (par exemple la mesure et l'adaptation de la glycémie via la puce)
	Lorsqu'un traitement de données à grande échelle, généré au moyen d'appareils dotés de capteurs envoyant des données via Internet ou un autre moyen (applications de l'Internet des objets), sert à analyser ou à prédire le comportement de personnes (par exemple une smartTV qui analyse les préférences et propose des programmes TV)
	Un magazine en ligne utilisant un listing d'adresses pour envoyer un message générique quotidien à ses abonnés. Le traitement se fait à grande échelle, mais le risque est faible et la personne concernée peut facilement se désinscrire.
	Une PME qui utilise une plateforme de recrutement en ligne qui sélectionne et rejette automatiquement des candidats sur la base d'une lecture automatique du C.V.
	Une PME qui observe systématiquement les habitudes de navigation de membres du personnel afin de prévenir un usage privé excessif pendant les heures de travail. Les travailleurs se trouvent dans une position subalterne et le risque est élevé.

PARTIE II : L'application du RGPD dans votre entreprise

Q10 : À quel secteur votre entreprise appartient-elle (principalement) ?
Veuillez indiquer une seule réponse en la soulignant.

- ICT
- Enseignement
- Secteur social
- Construction
- Consultance et management
- Banque et assurance
- Industrie alimentaire
- Horeca
- Soins, santé et pharmacie
- Intérim
- Agriculture et horticulture
- Transport et logistique
- Professions libérales
- Immobilier
- Autres :

Q11 : Combien d'ETP (équivalent temps plein, correspondant à un travail qui nécessite une personne affectée à plein temps) votre entreprise emploie-t-elle ?
Veuillez indiquer une seule réponse en la soulignant.

- 1 - 9 ETP
- 10 - 49 ETP
- 50 - 149 ETP
- 150 - 250 ETP
- > 250 ETP

Q12 : Quel est le chiffre d'affaires annuel de votre entreprise ?
Veuillez indiquer une seule réponse en la soulignant.

- < 500.000 euros
- entre 500.000 et 1.000.000 d'euros
- entre 1.000.000 et 2.000.000 d'euros
- entre 2.000.000 et 10.000.000 d'euros
- entre 10.000.000 et 50.000.000 d'euros
- > 50.000.000 d'euros

Q13 : Quelle est l'importance du traitement de données à caractère personnel pour votre activité ?
Veuillez indiquer une seule réponse en la soulignant.

- Le traitement de données à caractère personnel occupe une place centrale dans notre modèle d'entreprise
- Le traitement de données à caractère personnel (personnel, client, etc.) vient en appui à notre activité principale
- Nous pouvons parfaitement fonctionner sans données à caractère personnel
- Aucune idée

Q14 : Comment décririez-vous de manière générale la maturité de votre entreprise en matière de RGPD ?
Donnez un chiffre entre 1 et 5.
(1 : inexistante ; 3 : suffisante pour respecter les exigences minimales ; 5 : très fortement ancrée).

Chiffre : _____*(complétez ici un chiffre entre 1 et 5)*

Q15 : De qui traitez-vous des données à caractère personnel ? *(plusieurs réponses possibles)*

	Prospects (des clients potentiels de l'entreprise)
	Clients
	Fournisseurs
	Collaborateurs
	Postulants

	Données à caractère personnel reçues d'un donneur d'ordre
	Visiteurs du site Internet
	Autre : _____ *(réponse libre)*

Q16 : Votre entreprise agit-elle principalement en qualité de responsable du traitement ou de sous-traitant ?
Veuillez indiquer une seule réponse en la soulignant.

- Principalement responsable du traitement
- Principalement sous-traitant
- Les deux s'appliquent de manière égale
- Aucune idée

Q17 : Quel type d'acte juridique utilisez-vous pour encadrer votre relation de sous-traitance ?
Veuillez indiquer une seule réponse en la soulignant.

- Nous utilisons un contrat de sous-traitance
- Nous n'utilisons pas de contrat ou d'autre instrument juridique
- Non applicable (car nous n'avons pas de sous-traitant)
- Nous recourons à un autre type de contrat ou d'instrument juridique, à savoir : _____ (réponse libre)

Q18 : D'où vient l'acte juridique que vous utilisez afin d'encadrer la relation de sous-traitance ?
Veuillez indiquer une seule réponse en la soulignant.

- Nous utilisons un modèle que nous avons établis
- Nous utilisons un modèle disponible en ligne
- Nous utilisons le modèle de notre sous-traitant, fournisseur ou donneur d'ordre
- Nous utilisons un modèle établi par une source tierce (par exemple avocats, consultants etc.)
- Non applicable (car pas de sous-traitants ou pas d'acte juridique)

Q19 : Quelles affirmations s'appliquent à la politique vie privée de votre entreprise ? *(plusieurs réponses possibles)*

	Elle est à jour, visible et disponible sur notre site web ou via un autre endroit si l'entreprise ne dispose pas d'un site web
	Elle contient toutes les informations que nous devons communiquer en vertu du RGPD
	Nous n'utilisons pas une politique vie privée, même si nous devrions le faire en vertu du RGPD

	Nous n'utilisons pas de politique vie privée car nous ne devons pas le faire en vertu du RGPD (pour les entreprises qui agissent uniquement en qualité de sous-traitants)

Q20 : Quelles affirmations s'appliquent à la transparence dans votre entreprise vis-à-vis des personnes concernées dont vous traitez des données à caractère personnel ?
Veuillez indiquer une seule réponse en la soulignant.

- Nous ne disposons pas de procédure standard pour indiquer aux personnes concernées si nous disposons ou non d'informations à leur sujet
- Nous disposons d'une approche standard (modèle, fichier, site Internet) pour indiquer aux personnes concernées quelles données nous traitons à leur sujet, si elles le demandent

Q21 : Votre entreprise sait-elle quand et comment réaliser correctement une analyse d'impact relative à la protection des données (AIPD) ?
Veuillez indiquer une seule réponse en la soulignant.

- Oui, nous avons déjà réalisé une AIPD
- Oui, mais nous n'avons encore jamais été amenés à en réaliser une
- Nous avons essayé de faire une AIPD sans parvenir à la finaliser
- Non, nous n'avons pas de connaissances à ce sujet
- Aucune idée

Q22 : À quels acteurs votre entreprise fait-elle appel pour respecter le RGPD ? *(plusieurs réponses possibles)*

	Organisation sectorielle ou professionnelle
	Service public
	Autorité de protection des données (APD)
	DPO interne
	DPO externe
	Service juridique interne
	Consultant ou service juridique externe (y compris bureau d'avocats)
	Informations disponibles en ligne (hormis les acteurs susmentionnés)

	Aucune
	Autre : _____ *(réponse libre)*

Q23 : À quelles ressources votre entreprise a-t-elle recours pour respecter le RGPD ? (plusieurs réponses possibles)

	Avis sur mesure par e-mail / téléphone (aide pour des questions spécifiques)
	Modèles
	Brochures et autre documentation d'information hors ligne
	Informations sur un site Internet
	Réunions et sessions d'information physiques
	Webinaires et cours en ligne
	Plateforme d'assistance en ligne
	Groupe de travail RGPD
	Aucune
	Autre : _____ *(réponse libre)*

Q24 : Quelles ressources manquent à votre entreprise pour respecter le RGPD ? *(plusieurs réponses possibles)*

	Avis sur mesure par e-mail / téléphone (aide pour des questions spécifiques)
	Modèles

	Brochures et autre documentation d'information hors ligne
	Informations sur un site Internet
	Réunions et sessions d'information physiques
	Webinaires et cours en ligne
	Plateforme d'assistance en ligne
	Groupe de travail RGPD
	Aucune
	Autre : _____ *(réponse libre)*

Q25 : Quels sont les thèmes du RGPD qui posent le plus de difficultés à votre entreprise et qui nécessitent une aide ? *(plusieurs réponses possibles)*

	Déclaration de confidentialité
	Droits des personnes concernées
	Contrats de sous-traitance avec des tiers
	Connaissance des notions et des responsabilités du "responsable du traitement" et du "sous-traitant"
	Délais de conservation de données à caractère personnel
	Analyse d'impact relative à la protection des données (AIPD)
	Le délégué à la protection des données (DPO)
	Registre des activités de traitement

	Fuites de données et sécurité des données à caractère personnel
	Principes de protection des données dès la conception et de protection des données par défaut
	Principe de responsabilité
	Transfert de données à caractère personnel hors Union européenne
	Autre : _____ *(réponse libre)*

Q26 : Avez-vous une question concernant l'application du RGPD dans votre entreprise ?
À compléter librement

Annexe 2: Nombre de répondants par question

	Répondants néerlandophones	Répondants francophones	Nombre total de répondants
Q1	147	37	184
Q2	136	35	171
Q3	135	35	170
Q4	120	33	153
Q5	120	33	153
Q6a	118	33	151
Q6b	117	33	150
Q7	117	33	150
Q8	114	31	145
Q9	106	30	134
Q10	102	29	131
Q11	102	29	131
Q12	102	29	131
Q13	102	29	131
Q14	102	29	131
Q15	99	28	127
Q16	99	25	124
Q17	99	25	124
Q18	99	25	124
Q19	99	25	124
Q20	99	25	124
Q21	97	28	125
Q22	97	28	125
Q23	97	28	125
Q24	97	28	125

Q25	97	28	125
Q26	13	9	22

Annexe 3: Secteurs des PME interrogées

	Répondants néerlandophones	**Répondants francophones**	**Total de répondants**
ICT	15	4	19
Enseignement	2	1	3
Secteur social	2	1	3
Construction	5	1	6
Consultance et management	17	4	21
Banque et assurance	2	2	4
Industrie alimentaire	2	0	2
Soins, santé et pharmacie	6	1	7
Intérim	9	2	11
Agriculture et horticulture	1	0	1
Transport et logistique	10	2	12
Professions libérales	9	2	11
Immobilier	0	1	1
Autres	22	8	30
TOTAL	102	29	**131**

Note : Tous les répondants n'ont pas répondu à la question portant sur leur secteur d'activité.