Quelles sont les mesures à adopter par les entreprises pour respecter l'obligation d'accountability imposée par le Règlement (UE) 2016/679 relatif à la protection des données personnelles ?

Auteur : Kalinski, Coraline
Promoteur(s) : Van Cleynenbreugel, Pieter
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en droit, à finalité spécialisée en droit économique et social
Année académique : 2023-2024
URI/URL : http://hdl.handle.net/2268.2/19732

LIÈGE université
Droit, Science Politique & Criminologie

Département de Droit

Quelles sont les mesures à adopter par les entreprises pour respecter l'obligation d'*accountability* imposée par le Règlement (UE) 2016/679 relatif à la protection des données personnelles ?

Coraline KALINSKI

Travail de fin d'études

Master en droit à finalité spécialisée en droit économique et social

Année académique 2023-2024

Recherche menée sous la direction de :

Monsieur Pieter VAN CLEYNENBREUGEL

Professeur ordinaire

RÉSUMÉ

L'ère numérique a vu les données personnelles devenir des actifs cruciaux, nécessitant une protection rigoureuse. En Europe, cette protection est principalement régulée par le Règlement Général sur la Protection des Données (RGPD), qui impose un cadre strict pour le traitement des données personnelles.

Une des principales innovations du RGPD est l'introduction de l'obligation d'*accountability*, qui contraint les entreprises non seulement à adopter des mesures techniques et organisationnelles appropriées pour respecter le RGPD, mais également à démontrer activement cette conformité. La consécration explicite de ce principe, qui existait déjà auparavant de manière implicite, représente un changement de paradigme par rapport au régime de la Directive 95/46/CE. Il marque le passage d'une déclaration préalable *a priori* à un contrôle *a posteriori*, illustrant la volonté du législateur européen de responsabiliser les entreprises, ainsi que de remédier à l'ineffectivité de l'ancien régime.

Bien que le principe d'*accountability* soit mentionné de manière générale à l'article 5, paragraphe 2 du RGPD, celui-ci se caractérise, en pratique, par une série d'obligations concrètes à charge des entreprises.

Cette étude se concentrera sur l'article 24 et sur ces obligations spécifiques qui découlent du principe d'*accountability.* Nous explorerons les implications pratiques de l'*accountability*, dans l'objectif d'identifier clairement les mesures techniques et organisationnelles que les entreprises doivent adopter pour se conformer. En particulier, nous analyserons en profondeur les mesures organisationnelles, telles que la désignation d'un délégué à la protection des données, la tenue d'un registre des activités de traitement, la réalisation d'une analyse d'impact relative à la protection des données, les codes de conduite et certification, ou encore la formation et sensibilisation du personnel au RGPD.

REMERCIEMENTS

Ce travail marque la fin de mon parcours universitaire en droit et le début d'un nouveau chapitre de ma vie.

Je tiens à exprimer ma sincère gratitude au professeur Van Cleynenbreugel pour sa disponibilité et son soutien tout au long de ce projet. La liberté de choisir mon sujet ainsi que l'autonomie dont j'ai bénéficié à chaque étape m'ont permis d'explorer pleinement mes intérêts académiques.

TABLE DES MATIÈRES

LISTE DES ABBRÉVIATIONS

AIPD	Analyse d'impact relative à la protection des données
APD	Autorité de protection des données
CEPD	Comité européen de la protection des données
CIL	Correspondant informatique et libertés
CNIL	Commission nationale de l'informatique et des libertés
DPD	Délégué à la protection des données
DPO	Data protection officer
G29	Groupe de travail « Article 29 »
RGPD	Règlement général sur la protection des données

INTRODUCTION

À l'ère de la digitalisation et du développement incessant des technologies de l'information, les données personnelles émergent comme le nouvel « or noir » du 21ème siècle[1]. Le mot « données » provient du latin « *datum* » et signifie « don, cadeau »[2]. Elles représentent à la fois des ressources précieuses, des actifs et du capital[3] ; et induisent une création de valeur sans précédent. Cette transformation marque l'avènement d'une nouvelle ère pour l'humanité : celle de la civilisation numérique[4], où les données sont au cœur des activités humaines et des relations de pouvoir[5]. En raison de leur importance, il devient crucial de renforcer la législation pour assurer leur protection.

En Europe, le droit à la protection des données personnelles a émergé dans les années 1970, et s'est progressivement développé pour devenir un concept à part entière, distinct du droit fondamental au respect de la vie privée[6].

Adopté en avril 2016 et devenu pleinement applicable le 25 mai 2018, le Règlement général sur la protection des données[7] (ci-après « RGPD ») constitue aujourd'hui le cadre juridique de référence en la matière dans l'Union européenne[8]. Il a remplacé la Directive 95/46/CE[9] qui était en vigueur depuis vingt ans et a introduit de nouvelles obligations à charge des entreprises. Parmi ces nouveautés : l'obligation explicite de se conformer à un principe de responsabilité, l'obligation de désigner un délégué à la protection des données dans certains cas, l'obligation de réaliser une analyse d'impact relative à la protection des données lorsque le traitement « [e]st susceptible d'engendrer un risque élevé »[10], ou encore, l'obligation de respecter les principes de protection dès la conception et par défaut[11].

---

[1] A. ANCIAUX et J. FARCHY, « Données personnelles et droit de propriété : quatre chantiers et un enterrement », *Revue internationale de droit économique*, 2015, p. 307 à 331.

[2] L. YUMING *et al., Droit des données 2.0. Construction du système de droits. Laboratoire clé de la stratégie des métadonnées,* Oxford, Peter Lang, 2021, p. 58.

[3] L. YUMING, *Droit des données 3.0. Perspective législative. Laboratoire clé de la stratégie des métadonnées,* Oxford, Peter Lang, 2022, p. 3.

[4] L. YUMING, *Droit des données 2.0…, op. cit.*, p. 59.

[5] L. YUMING, *Droit des données 2.0…, op. cit.*, p. 56.

[6] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *Manuel de droit européen en matière de protection des données,* Luxembourg, Office des publications de l'Union européenne, 2019, p. 21.

[7] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.,* L 119/1, 4 mai 2016.

[8] Communication de la Commission au Parlement européen – Une meilleure protection et de nouvelles perspectives – Orientation de la Commission relative à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018, COM (2018) 43 final, 24 janvier 2018, p.1.

[9] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E..,* L 281, 23 novembre 1995.

[10] Communication de la Commission au Parlement européen – Une meilleure (…), *op. cit.,* p. 4.

[11] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *op. cit.,* p. 34.

Le principe de responsabilité ou d'« *accountability* » a été explicitement consacré et renforcé avec le RGPD et en constitue un pilier majeur[12]. Il est défini de manière générale à l'article 5, paragraphe 2, du RGPD et dispose qu'un responsable de traitement est tenu de respecter les principes du règlement ainsi que d'être en mesure de démontrer cette conformité.

En pratique, ce principe est toutefois complété et mis en œuvre par l'article 24 du règlement[13], qui énonce que « *[l]e responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement »[14].* Par conséquent, le principe d'*accountability* entraîne toute une série d'obligations concrètes dans le chef des entreprises, que l'on peut qualifier d'« obligations d'*accountability* »[15]. Il leur impose de prendre plusieurs mesures, de nature technique, d'une part, et organisationnelle, d'autre part, afin de rendre ce principe opérationnel.

L'objectif de ce travail est de répertorier et d'examiner les différentes mesures qu'une entreprise doit adopter afin de respecter l'obligation d'*accountability*, imposée par l'article 24.

Pour ce faire, nous avons fait le choix de structurer nos propos en deux parties.

Dans la première partie, nous procéderons à une analyse théorique de l'*accountability.* Nous examinerons ses deux composantes, sa redécouverte à la suite du RGPD, et les sanctions encourues en cas de non-respect.

La deuxième partie, plus pratique, sera consacrée à l'analyse de ces mesures. Premièrement, nous aborderons la marge de manœuvre octroyée aux entreprises quant au choix des mesures. Deuxièmement, nous explorerons le champ des mesures techniques et en esquisserons les principaux aspects. Cet exposé illustre notre volonté de fournir un aperçu complet et global des mesures à implémenter, bien que nous laisserons les détails aux experts en systèmes informatiques. Troisièmement, la majeure partie de notre recherche sera dédiée à l'examen des mesures organisationnelles, comprenant la désignation d'un DPO, la tenue d'un registre des activités de traitement, la réalisation d'une analyse d'impact relative à la protection des données, et les codes de conduite et certifications. En dernier lieu, nous soulignerons la nature continue du processus d'*accountability* et l'obligation consécutive de réexaminer périodiquement les mesures existantes.

En raison du cadre limité dont nous disposions, il nous était impossible d'examiner l'ensemble des mesures de manière exhaustive. Nous examinerons dès lors les plus importantes ; délimitées suivant le guide de la CNIL[16], pour les mesures techniques, et d'après le Manuel de

---

[12] C. DOCKSEY, « Article 24. Responsibility of the controller », *The EU General Data Protection Regulation (GDPR). A Commentary*, C. KUNER, L. BYGRAVE et C. DOCKSEY, Oxford, Oxford University Press, p. 557.

[13] L. FEILER, N. FORGÓ et M. WEIGL, *The EU General Data Protection Rgulation (GDPR): A Commentary*, Woking, German Law Publishers, 2018, p. 142.

[14] Art. 24, §1 RGPD.

[15] C. DOCKSEY, *op. cit.,* p. 557.

[16] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles,* 2018. Disponible sur https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_guide_securite_personnelle.pdf.

l'Agence des droits fondamentaux de l'UE et du Conseil de l'Europe, pour les mesures organisationnelles[17].

[17] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *op. cit.,* p. 194.

I. PRÉSENTATION THÉORIQUE DE L'OBLIGATION *D'ACCOUNTABILITY*

A. Définition

Le terme « *accountability* » est communément traduit en français par « responsabilité » et signifie « obligation de rendre des comptes ». Définir avec précision l'« *accountability* » est toutefois loin d'être évident. Dans le RGPD, ce concept fait référence à « la mise en œuvre des principes de protection des données ». Il souligne la manière d'endosser la responsabilité et de la contrôler, et joue un rôle primordial pour assurer la confiance et permettre la bonne gouvernance[18].

Néanmoins, la traduction de ce terme porte à confusion et a donné lieu à de nombreuses difficultés en raison de la diversité des systèmes juridiques des pays européens[19]. Un grand nombre de juristes francophones regretteront la polysémie du terme « responsabilité » ; le principe de responsabilité au sens du règlement ne devant pas être confondu avec le principe de responsabilité civile en droit belge[20]. Par ailleurs, d'autres préfèrent parler de principe de « redevabilité »[21]. Face à cette ambiguïté et par souci de clarté, nous avons choisi d'employer le terme anglais et nous parlerons d'*accountability*.

Le principe d'*accountability* est défini de façon générale à l'article 5, paragraphe 2, du RGPD et constitue l'une des pierres angulaires du règlement. Il impose au responsable de traitement de respecter les principes du RGPD, énoncés à l'article 5, paragraphe 1, ainsi que d'être en mesure de démontrer cette conformité[22]. Autrement dit, en vertu de cet article, le responsable de traitement doit, d'une part, respecter le règlement et, d'autre part, pouvoir prouver qu'il le respecte. Cela implique de pouvoir démontrer le respect des six principes fondamentaux qui sous-tendent le RGPD : le principe de licéité, de loyauté et transparence du traitement, le principe de finalité, le principe de minimisation des données, le principe d'exactitude des données, le principe de limitation de la conservation des données, et le principe d'intégrité et de confidentialité des données[23].

En pratique, le principe d'*accountability* entraine toute une série d'obligations dans le chef des entreprises qui traitent des données à caractère personnel. Il est mis en œuvre par l'article 24 du règlement, qui précise les mesures à prendre afin de respecter, concrètement, ce principe. En vertu de cette disposition, le responsable de traitement a l'obligation de mettre en œuvre des « *[m]esures techniques et organisationnelles appropriées pour s'assurer et être*

[18] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 8.
[19] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 8.
[20] B. LAMON, « Le principe d' « *accountability* » et les instruments de mise en conformité », *Le règlement général sur la protection des données. Aspects institutionnels et matériels*, A. BENSAMOUN et B. BERTRAND (dir.), Mare & Martin, 2020, p. 219.
[21] B. LAMON, *ibidem*, p. 219.
[22] Art. 5, §2 RGPD.
[23] Art. 5, §2 RGPD.

en mesure de démontrer que le traitement est effectué conformément au présent règlement »[24]. Le principe d'*accountability* comporte donc deux éléments distincts[25].

1. Premier volet : Adopter des mesures techniques et organisationnelles appropriées pour respecter le RGPD

Premièrement, le responsable de traitement est tenu d'adopter des mesures appropriées et efficaces afin de respecter les principes et obligations contenus dans le règlement[26].

Ces « mesures techniques et organisationnelles appropriées » sont destinées à mettre concrètement en œuvre la règlementation, et visent à intégrer le RGPD et la protection des données personnelles dans l'organisation concrète de l'entreprise[27].

Dans ses considérants, le règlement insiste sur le fait que ces mesures doivent être « effectives », c'est-à-dire efficaces pour garantir ce double but de conformité et de documentation[28]. En outre, elles doivent être déterminées en tenant compte de la réalité globale du traitement, et notamment de « [l]a nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques »[29]. Le concept de « mesures techniques et organisationnelles » est plus complet dans le RGPD qu'il ne l'était auparavant dans la Directive et vise l'ensemble des mesures destinées à garantir et à prouver la mise en conformité avec les règles de protection des données[30]. Ces mesures peuvent, notamment, inclure l'adoption de politiques internes appropriées et autres mécanismes en matière de protection des données[31]. Il importe de noter que les mesures doivent respecter les principes de protection des données dès la conception et par défaut, visés à l'article 25, paragraphes 1 et 2[32].

Il revient à l'entreprise de définir les mesures nécessaires pour assurer que ses opérations soient conformes aux dispositions du règlement et d'en vérifier régulièrement l'efficacité[33]. Cette obligation constitue une obligation proactive[34]. Pour accompagner les entités dans leur démarche et faciliter ce processus, de nombreuses autorités de contrôle ont élaboré des plans méthodologiques détaillés, étape par étape[35]. Par exemple, en France, la Commission Nationale de l'Informatique et des Libertés (ci-après, la « CNIL ») propose un plan en six étapes : désigner un pilote pour la gouvernance des données, cartographier les traitements, prioriser les actions à mener, gérer les risques, organiser les processus internes, et

---

[24] Art. 24, §1 RGPD.
[25] O. TAMBOU, *Manuel de droit européen de la protection des données à caractère personnel,* Bruxelles, Bruylant, 2020, p. 251.
[26] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 9.
[27] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 12.
[28] Cons. 74 RGPD.
[29] Cons. 74 RGPD.
[30] L. FEILER, N. FORGÓ et M. WEIGL, *op. cit.*, p. 143.
[31] Art. 24, §2 RGPD.
[32] L. FEILER, N. FORGÓ et M. WEIGL, *op. cit.*, p. 143.
[33] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 12.
[34] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *op. cit.,* p. 195.
[35] O. TAMBOU, *op. cit.*, p. 252.

documenter la conformité[36] [37]. De manière comparable, d'autres praticiens suggèrent de prendre en compte sept étapes, qui sont l'inventaire ou la cartographie, la mise en œuvre de procédure internes et de formations, la formation de la documentation et des registres, l'étude d'impact, la fixation d'une gouvernance de la protection des données personnelles, l'adoption de procédures d'exécution des droits des personnes concernées, et enfin, l'obligation d'assurer la sécurité des données[38].

2. Deuxième volet : Être en mesure de démontrer sa conformité

Deuxièmement, l'*accountability* impose l'obligation, pour le responsable de traitement, de pouvoir prouver que de telles mesures appropriées et efficaces ont été prises si on le lui demande[39].

L'entreprise doit être capable de démontrer, c'est-à-dire de documenter, sa conformité[40]. Elle doit pouvoir prouver qu'elle met effectivement en œuvre le RGPD et qu'elle opère en respectant les principes de protection des données[41]. À ce sujet, le Comité européen de la protection des données (ci-après « CEPD ») a affirmé que « [l]e principe de responsabilité, qui consiste à démontrer le respect de la protection des données, doit être *au cœur de toute activité de traitement* »[42]. De la même manière, l'Autorité de protection des données (ci-après « APD ») a insisté sur le fait que cette obligation de documentation comme preuve de sa responsabilité constitue une disposition clé du RGPD[43].

Concrètement, cela implique l'obligation de tenir une *documentation* interne et de documenter toutes ses démarches[44]. Cette documentation interne doit contenir les informations sur les traitements effectués, les réflexions menées et les mesures prises pour respecter le règlement[45]. Autrement dit, « [v]ous devez pouvoir expliquer ce que vous faites, pourquoi vous le faites, et comment vous le faites ».[46]

Selon certains, cette disposition renvoie à la charge de la preuve et rappelle que c'est au responsable de traitement qu'incombe la tâche de prouver le respect du RGPD[47]. D'autres auteurs estiment, au contraire, que cette interprétation est incompatible avec la présomption

---

[36] https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes, consulté le 19 mars 2024.
[37] O. TAMBOU, *op. cit.*, p. 253.
[38] B. LAMON, *op. cit.*, p. 225.
[39] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 10.
[40] O. TAMBOU, *op. cit.*, p. 251.
[41] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, *Règlement général sur la protection des données. Préparez-vous en 13 étapes,* p. 6. Disponible sur https://www.autoriteprotectiondonnees.be/publications/plan-en-13-etapes.pdf.
[42] COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Documenter le traitement des données : Le guide du CEPD pour garantir l'obligation de rendre compte*, Luxembourg, Office des publications de l'Union européenne, 2019, p. 3. Disponible sur https://op.europa.eu/en/publication-detail/-/publication/09445291-adbc-11e9-9d01-01aa75ed71a1/language-fr/format-PDF/source-310658513.
[43] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, *Règlement général sur la protection des données. Préparez-vous en 13 étapes,* p. 5.
[44] COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Documenter (…),* p. 3.
[45] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *op. cit.,* p. 153.
[46] COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Documenter (…),* p. 3.
[47] B. LAMON, *op. cit.*, p. 221.

d'innocence de l'article 48, paragraphe 1, de la Charte ; notamment au vu de l'imposition d'amendes administratives en application de l'article 83 du règlement[48]. D'après ce point de vue, le second élément de l'*accountability* consisterait plutôt en une obligation matérielle de démontrer la conformité[49].

Quoi qu'il en soit, tout le processus de raisonnement et de décision relatif à un traitement doit impérativement être conservé et consigné. Cette démarche a pour objectif de garder des preuves qui serviront à expliquer et à légitimer les décisions prises pour garantir la conformité. En effet, cette documentation sera demandée en cas de contrôle par l'Autorité de protection des données, et le responsable de traitement doit être prêt à fournir les justificatifs attestant de son respect du RGPD à tout moment[50]. Il doit également pouvoir démontrer sa conformité aux personnes concernées et au grand public[51].

B. Consécration et renforcement à la suite du RGPD

Le principe d'*accountability* a été explicitement consacré et renforcé avec l'entrée en vigueur du RGPD. Il constitue une des innovations les plus importantes du règlement[52]. Toutefois, ce principe n'est pas une nouveauté en soi dans le domaine de la protection des données. Bien que la Directive 95/46/CE ne mentionnait pas explicitement le terme « *accountability* » comme principe ou obligation, sa consécration à l'article 5, paragraphe 2, et à l'article 24 du RGPD est une réaffirmation forte d'une obligation qui existait déjà auparavant de manière implicite[53]. Certaines dispositions de la directive sous-tendaient déjà cette idée d'*accountability*, notamment l'article 6, qui traite des principes relatifs à la qualité des données et dont la formulation rappelle l'actuel article 5, paragraphe 2, du règlement[54]. D'autres articles établissaient également des obligations qui, *de facto*, engageaient la responsabilité des responsables de traitement ; comme l'article 17, qui imposait l'obligation de garantir la sécurité des données, ou l'article 18, qui établissait l'obligation de notification auprès de l'autorité de contrôle[55].

Le RGPD a ainsi érigé l'*accountability* en véritable principe fondamental. Cette consécration représente un profond changement de paradigme et une évolution significative par rapport à la directive. Elle marque le passage d'un contrôle *ex-ante*, qui repose sur l'obligation de faire une déclaration préalable à l'autorité de contrôle, au profit d'un contrôle *a posteriori*[56]. En remplaçant cette obligation de notification préalable par l'obligation de prendre des mesures proactives, le règlement instaure un régime de responsabilité active et de démonstration de conformité, qui met l'accent sur la capacité du responsable de traitement à prouver, à tout

[48] L. FEILER, N. FORGÓ et M. WEIGL, *op. cit.*, p. 143.
[49] L. FEILER, N. FORGÓ et M. WEIGL, *op. cit.*, p. 143.
[50] O. TAMBOU, *op. cit.*, p. 253.
[51] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *op. cit.,* p. 151.
[52] C. DOCKSEY, *op. cit.,* p. 557.
[53] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 9.
[54] B. LAMON, *op. cit.*, p. 220.
[55] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 9.
[56] C. DOCKSEY, *op. cit.,* p. 557.

moment, sa conformité, sans que cela ne nécessite une intervention préalable des autorités de contrôle[57].

La *ratio legis* de ce nouveau texte était clairement de responsabiliser le responsable de traitement, c'est-à-dire de créer un sentiment de responsabilité plus grand dans le chef des entreprises[58]. Outre la consécration du principe et ce changement de paradigme, deux éléments ont également contribué à cette responsabilisation des acteurs. D'une part, une activité accrue des autorités de contrôle[59], et, d'autre part, une augmentation des sanctions prévues par le RGPD, bien plus sévères que celles prévues sous la directive[60].

En introduisant cette nouvelle disposition, le législateur européen avait pour objectif de remédier au problème d'ineffectivité des normes qui avait affecté la directive, et spécialement l'obligation de faire une déclaration préalable auprès de l'autorité de contrôle, qui n'était pas respectée en pratique. Ce changement d'approche répond à une critique largement partagée par le Groupe de travail « Article 29 » (« G29 »), selon laquelle le cadre juridique de la directive n'était pas pleinement efficace pour garantir la transposition des exigences en matière de protection des données et offrir une protection réelle et effective[61]. Par conséquent, il était primordial de combler ces lacunes afin d'assurer, dans les faits, le respect de ces obligations[62].

C. Sanctions

Le RGPD prévoit des sanctions importantes pour les entreprises qui ne respectent pas leur devoir d'*accountability*. Bien que le règlement n'impose pas explicitement d'amendes administratives en cas de violation de l'article 24[63], une entreprise qui ne respecte pas certaines des obligations spécifiques qui en découlent s'expose au risque de se voir infliger une amende administrative pouvant atteindre 10 millions d'euros, ou 2% de son chiffre d'affaires annuel mondial total de l'exercice précédent, si ce montant est plus élevé[64]. Cette sanction s'applique notamment en cas de violation des obligations de tenir un registre des activités de traitements, de réaliser une analyse d'impact, ou encore de désigner un délégué à la protection des données[65]. Par ailleurs, les entreprises peuvent encourir des sanctions pénales prévues par le droit des États membres[66]. Enfin, l'obligation de démontrer sa conformité est également soumise au contrôle des autorités de surveillance, qui, dans l'exercice de leurs pouvoirs conformément à l'article 58, paragraphe 1, peuvent tenir compte de tout manquement[67].

---

[57] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *op. cit.,* p. 154.
[58] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 3.
[59] A. BENSAMOUN et B. BERTRAND, « Prolégomènes », A. BENSAMOUN et B. BERTRAND (dir.), *Le règlement général sur la protection des données. Aspects institutionnels et matériels,* Mare & Martin, 2020, p. 14.
[60] B. LAMON, *op. cit.*, p. 220.
[61] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 3.
[62] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 11.
[63] L. FEILER, N. FORGÓ et M. WEIGL, *op. cit.*, p. 142.
[64] Art. 83, §4 RGPD.
[65] Art. 83, §4, a) RGPD.
[66] O. TAMBOU, *op. cit.*, p. 262.
[67] L. FEILER, N. FORGÓ et M. WEIGL, *op. cit.*, p. 142 et 144.

II. MESURES SPÉCIFIQUES A ADOPTER POUR RESPECTER L'OBLIGATION D'*ACCOUNTABILITY*

A. Introduction

Nous avons vu que le principe général d'*accountability* mentionné à l'article 5, paragraphe 2, du RGPD est, en pratique, complété et mis en œuvre par l'article 24 qui énonce que « *[l]e responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement »*[68]. Du principe d'*accountability* découle donc un large éventail de mesures destinées à garantir que les entreprises traitent les données personnelles conformément au règlement. Cette seconde partie est consacrée à l'analyse de ces mesures et obligations.

B. Souplesse et marge de manœuvre

Pour atteindre cet objectif de mise en conformité, le RGPD impose certaines obligations très précises aux entreprises. Par exemple, l'obligation de désigner un délégué à la protection des données, d'effectuer une analyse d'impact, ou encore de maintenir un registre des activités de traitement.

Néanmoins, outre ces obligations, les responsables de traitement disposent d'une certaine marge de manœuvre dans le choix des « mesures appropriées » à adopter[69]. Le règlement ne spécifie pas une liste exhaustive de mesures concrètes à adopter[70]. Au contraire, il fait preuve d'une grande souplesse et laisse à chaque entreprise la liberté nécessaire afin qu'elle puisse choisir les mesures qui conviennent le mieux à ses besoins. Par exemple, en tenant compte des particularités de son organisation comme sa taille ou son secteur, des circonstances concrètes du traitement, des types de données traitées ou des risques associés[71].

En somme, le principe d'*accountability* se caractérise par une grande flexibilité et des dispositions ambiguës[72]. Le règlement énonce d'avantage des lignes directrices et un objectif à atteindre, sans imposer les moyens détaillés à employer pour garantir cette conformité.

En accordant cette marge de manœuvre, le second objectif du législateur était, une nouvelle fois, de responsabiliser les responsables de traitement. Il a volontairement laissé cette part d'incertitude pour créer un sentiment de responsabilité plus grand dans leur chef. En étant responsable du choix des mesures, les entreprises doivent désormais faire preuve d'une attention accrue puisqu'elles sont pleinement impliquées dans le processus de réflexion.

---

[68] Art. 24, §1 RGPD.

[69] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 2.

[70] E. KOSTA, R. LEENES et I. KAMARA, *Research Handbook on EU Data Protection Law*, Cheltenham, Edward Elgar Publishing Limited, 2022, p. 66.

[71] E. KOSTA, R. LEENES et I. KAMARA, *ibidem,* p. 67.

[72] Communication de la Commission au Parlement européen – Une meilleure (…), *op. cit.,* p. 4.

C. Mesures techniques

1. Lien avec l'obligation de sécurité (article 32)

Pour commencer, il est intéressant de remarquer que les mesures techniques appropriées qu'une entreprise doit mettre en œuvre pour respecter l'obligation d'*accountability* peuvent se chevaucher avec les mesures techniques requises pour respecter l'obligation de sécurité imposée par l'article 32. En effet, le principe de sécurité, aussi appelé principe d'intégrité et de confidentialité des données, est énoncé à l'article 5, paragraphe 1, f), et explicité à l'article 32. Ce dernier impose l'obligation d'assurer la sécurité des traitements, et plus précisément, de mettre en œuvre « *[l]es mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* », y compris la protection contre le traitement non autorisé ou illégal et contre la perte, la destruction ou les dommages d'origine accidentelle[73].

Par conséquent, le principe d'*accountability* et le principe de sécurité se font écho dans la mesure où ils soulignent l'importance d'implémenter des mesures techniques et organisationnelles pour protéger les données personnelles. Ils le font sous des angles légèrement différents, car l'article 24 met l'accent sur la responsabilité globale et la documentation de la conformité avec le RGPD, tandis que l'article 32 se concentre sur l'implémentation pratique de la sécurité des données, et précise quels types de mesures doivent être adoptées pour prévenir contre les risques spécifiques. Toutefois, les deux obligations reposent sur une approche fondée sur le risque[74]. En outre, dans une décision, la Chambre Contentieuse de l'Autorité de protection des données a rappelé que l'article 32 devait être lu en combinaison avec l'article 5, paragraphe 2, et avec l'article 24[75].

2. Mesures

Il est impératif d'adopter des mesures strictement nécessaires, adaptées aux risques et au contexte de chaque entreprise. Toutefois, il n'est pas toujours évident de mettre en œuvre une telle démarche et de s'assurer que le minimum requis a bien été mis en place[76]. En France, pour accompagner les entreprises dans leur mise en conformité, la CNIL a élaboré un guide identifiant un éventail de mesures à prendre[77]. Il constitue une aide précieuse en soulignant les mesures de bases qui doivent être appliquées de manière systématique[78]. En outre, une

---

[73] Art. 32, §2 RGPD.
[74] O. TAMBOU, *op. cit.*, p. 289.
[75] A.P.D. (Ch. Contentieuse), décision 56/2021 du 26 avril 2021, point 82. Disponible sur https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-56-2021.pdf.
[76] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 4.
[77] O. TAMBOU, *op. cit.*, p. 289.
[78] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 4.

fiche prenant la forme d'une *check-list* se trouve à la fin du guide afin d'aider l'entreprise à évaluer son niveau de sécurité des données personnelles[79].

Premièrement, il est essentiel d'assurer une *authentification des utilisateurs*, c'est-à-dire que l'utilisateur soit reconnu avant de pouvoir utiliser les moyens informatiques. Il doit posséder un identifiant qui lui est propre et s'authentifier afin de garantir qu'il accèdera uniquement aux données dont il a besoin[80]. Pour cela, il est impératif de donner un identifiant, appelé « login » en anglais, unique à chaque utilisateur, ou encore de limiter le nombre de tentatives d'accès à un compte[81]. Par ailleurs, il est fortement déconseillé de divulguer son mot de passe, de le stocker sur papier ou dans un endroit peu sécurisé, de choisir des mots de passe personnels prévisibles, ou encore de réutiliser le même mot de passe pour différents accès[82]. Pour aller encore plus loin, la CNIL recommande l'authentification forte, le renouvellement périodique du mot de passe, l'utilisation des gestionnaires de mots de passe, et le stockage des mots de passe de manière sécurisée[83].

Deuxièmement, une entreprise doit *gérer les habilitations*, ce qui signifie restreindre l'accès uniquement aux données dont l'utilisateur a besoin. À cette fin, il ne faut, par exemple, pas oublier de révoquer des autorisations temporaires octroyées à un utilisateur lors d'un remplacement, ou de désactiver les comptes utilisateurs d'employés ayant quitté l'entreprise[84].

Troisièmement, il est impératif de *tracer les accès et gérer les incidents*[85]. Il s'agit de garder un historique de tous les utilisateurs qui ont accédé aux systèmes de l'entreprise et d'avoir des protocoles de résolution d'incidents. Pour ce faire, la mesure principale est la journalisation, à savoir la tenue d'un registre des « log files »[86]. Bien qu'elle ne soit pas expressément mentionnée dans le RGPD, la journalisation est considérée par l'APD comme une action incontournable et constitue une bonne pratique recommandée[87].

---

[79] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 30 et 31.

[80] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 9.

[81] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 30.

[82] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 10.

[83] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 10.

[84] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 11.

[85] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 12.

[86] A.P.D. (Ch. Contentieuse), décision 56/2021 du 26 avril 2021, point 73. Disponible sur https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-56-2021.pdf.

[87] A.P.D. (Ch. Contentieuse), décision 56/2021 du 26 avril 2021, point 80 et 81. Disponible sur https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-56-2021.pdf.

Quatrièmement, il est important de *sécuriser les postes de travail*, notamment en installant des « pare-feu » ou « firewall » logiciels et des antivirus régulièrement mis à jour, ou encore en prévoyant des mécanismes de verrouillage automatique de session[88].

Cinquièmement, une entreprise doit *sécuriser l'informatique mobile* pour anticiper les atteintes à la sécurité des données qui pourraient résulter du vol ou de la perte de l'équipement[89]. Elle doit sensibiliser ses employés aux risques, tels que le vol, et aux procédures mises en place dans l'organisation pour les limiter. Il faut également sauvegarder régulièrement les données, ou encore chiffrer ces équipements mobiles.

Sixièmement, l'organisation se doit de *protéger son réseau informatique interne*[90]. Pour ce faire, il est judicieux de limiter les accès internet et imposer un VPN pour l'accès à distance.

Septièmement, elle doit *sécuriser ses serveurs ainsi que ses sites web*. En ce qui concerne les serveurs, elle doit les effectuer des sauvegardes, les vérifier de façon régulière, et assurer que seules les personnes habilitées peuvent y avoir accès[91]. Quant aux sites web, impératif de mettre en œuvre le protocole TLS[92].

Huitièmement, l'entreprise doit *sauvegarder et prévoir la continuité de son activité.* D'une part, celle-ci doit effectuer des sauvegardes régulières des données et les stocker dans un endroit extérieur et sécurisé. D'autre part, elle doit anticiper tout incident, comme une panne ou un sinistre, rédiger un plan de continuité ou de reprise d'activité, et informer ses employés sur la personne à contacter en cas d'accident[93]. Par ailleurs, les sauvegardes ne doivent pas être conservées au même emplacement que les machines qui hébergent les données.

Neuvièmement, elle doit *archiver de manière sécurisée* les données qui ne sont plus utilisées mais qui ne sont pas encore arrivées au terme de leur délai limite de conservation en vertu de l'article 5, paragraphe 1, e), puis en assurer un effacement sécurisé[94].

De la même manière, une mesure supplémentaire consiste à *encadrer la maintenance et la destruction* des données, et inclut l'obligation d'insérer une clause de sécurité dans les contrats de maintenance effectuée par des prestataires[95].

---

[88] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 13.

[89] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 15.

[90] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 16.

[91] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 17.

[92] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 19.

[93] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 20.

[94] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 21.

[95] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 22.

Onzièmement, le règlement requiert de *gérer les sous-traitants* et d'encadrer avec eux la sécurité des données qui leur sont communiquées[96]. À cet égard, l'article 28, paragraphe 3, impose de rédiger un contrat avec les sous-traitants, lequel doit définir l'objet, la durée, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées, ainsi que les obligations des parties et une série de dispositions particulières.

Douzièmement, une entreprise doit *sécuriser les échanges avec d'autres organisations* et renforcer la sécurité lorsqu'elle transmet des données. La messagerie électronique n'étant pas sécurisée, il faut être attentif lorsque l'on communique des données secrètes, tels que le résultat d'un audit financier ou d'un projet à un client. L'entreprise doit notamment veiller à chiffrer les données avant leur envoi, les scinder en les transmettant de façon distincte via deux canaux différents, et utiliser un protocole qui garantit que le transfert de fichiers sur internet se fait de manière confidentielle, comme le protocole TLS[97]. En guise d'exemple, l'APD a condamné un laboratoire pour avoir utilisé le protocole « HTTP », qui n'utilise pas le protocole TLS et ne contient pas de chiffrement, à la place du protocole sécurisé « HTTPS »[98].

Treizièmement, l'entreprise doit *protéger ses locaux*. Cela passe notamment par l'installation de serrures et alarmes mais également par la tenue d'une liste des personnes qui peuvent accéder à chacune des zones du bâtiment[99].

Enfin, d'autres mesures techniques sont à implémenter, tels que *le chiffrement, le hachage et les signatures numériques*[100] ; ou *l'encadrement des développements informatiques*, avec l'intégration de la protection des données dès la conception et par défaut, conformément à l'article 25 du règlement.

D. Mesures organisationnelles

1. Désignation d'un délégué à la protection des données

1. Introduction

« Chef d'orchestre » « garant » ou encore « pilote » de la conformité d'une entreprise au droit de la protection des données personnelles, nombreuses sont les expressions utilisées par la doctrine pour tenter de résumer le rôle du délégué à la protection des données[101].

---

[96] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 23.

[97] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 25.

[98] A.P.D. (Ch. Contentieuse), décision quant au fond 127/2022 du 19 août 2022, point 20. Disponible sur https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-127-2022.pdf.

[99] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 31.

[100] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles* (…), p. 28.

[101] O. FORET, « Le rôle du DPO », *Le règlement général sur la protection des données. Aspects institutionnels et matériels*, A. BENSAMOUN et B. BERTRAND (dir.), Mare & Martin, 2020, p.234.

Le délégué à la protection des données (DPD), plus communément appelé *Data Protection Officer* (ci-après « DPO »), constitue une nouvelle fonction introduite lors de l'entrée en vigueur du RGPD. Certains pays de l'Union européenne avaient déjà intégré des rôles similaires à celui du DPO dans leur législation nationale en matière de protection des données. En guise d'exemple, en France, le concept de Correspondant Informatique et Libertés (CIL) existait avant l'adoption du RGPD. Le CIL avait un rôle similaire en ce sens qu'il était chargé de veiller à la conformité des traitements de données personnelles au sein des organisations. Toutefois, la désignation d'un CIL n'était pas obligatoire pour toutes les entreprises et les missions n'étaient pas définies de manière aussi détaillée que dans le RGPD. Avec l'adoption du RGPD, le rôle du DPO a été formalisé et harmonisé à l'échelle de l'Union[102]. Le règlement a rendu sa désignation obligatoire dans certains cas, a renforcé ses missions, et a imposé de nouvelles obligations, telle que l'obligation de lui fournir les ressources dont il a besoin pour l'exercice de ses fonctions[103]. Le règlement vise également désormais les sous-traitants, et non plus uniquement les responsables de traitement[104]. Ce nouveau rôle est central dans la gouvernance de la protection des données au sein d'une entreprise[105].

Son statut est régi aux article 37 à 39 du règlement, qui abordent respectivement sa désignation, sa fonction et ses missions. En outre, le G29 a publié des lignes directrices d'interprétation très utiles à ce sujet[106].

2. Cas où la désignation d'un DPO est obligatoire

L'article 37, paragraphe 1, prévoit l'obligation de désigner un DPO dans trois cas particuliers : « [l]orsque le traitement est effectué par une autorité publique ou un organisme public […] ; lorsque les activités de base du responsable de traitement ou du sous-traitant […] exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou lorsque les activités de base […] consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions[…] ».

Le G29 a apporté des précisions sur certaines de ces notions clés dans ses lignes directrices.

Premièrement, il a interprété la notion d'« activités de base » comme renvoyant aux activités « principales » d'une entreprise, c'est-à-dire aux opérations « clés » nécessaires à la réalisation de ses objectifs. *A contrario*, le texte ne vise pas les activités dites « auxiliaires »[107].

---

[102] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°04/2017 du 24 mai 2017 relative à la désignation d'un délégué à la protection des données conformément au Règlement général sur la protection des données (RGPD), en particulier l'admissibilité du cumul de cette fonction avec d'autres fonctions dont celle de conseiller en sécurité (CO-AR-2017-008), p. 8 (point 17).

[103] O. FORET, *op. cit.*, p. 234.

[104] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°04/2017 (…), *op. cit.,* p. 8 (point 17).

[105] B. LAMON, *op. cit.*, p. 224.

[106] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016.

[107] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 6.

Ensuite, le G29 rappelle que la notion de traitement « à grande échelle » est éclairée par le considérant 91 du règlement, lequel évoque une opération de traitement destinée à traiter « un volume considérable de données »[108]. Bien qu'il soit impossible de déterminer un nombre précis de données ou d'individus concernés, plusieurs critères peuvent être pris en considération lors de l'appréciation, tels que le nombre de personnes concernées, le volume des données, la durée du traitement, ou encore l'étendue géographique du traitement[109].

Enfin, quant à la notion de « suivi régulier et systématique », le G29 précise que l'idée de « suivi du comportement des personnes concernées » est évoquée au considérant 24[110]. Selon celui-ci, une personne peut être considérée comme « suivie sur internet » en cas de profilage ; notamment dans un objectif de publicité comportementale, qui vise à prendre des décisions concernant l'individu ou à réaliser des prédictions sur ses préférences ou ses comportements. En outre, les lignes directrices fournissent une interprétation du caractère régulier et systématique du suivi. D'une part, un suivi régulier peut notamment être un suivi en cours, constant, récurrent, ou encore ayant lieu à des intervalles réguliers. D'autre part, un traitement est systématique s'il s'opère, par exemple, de manière préétablie, organisée, méthodique ou dans le cadre d'un plan général de collecte de donnée[111].

Outre les trois cas obligatoires visés au paragraphe 1, le paragraphe 4 prévoit que l'entreprise est, toutefois, également tenue de désigner un DPO lorsque le droit de l'Union européenne ou de l'État membre l'impose[112]. Cette disposition permet dès lors aux États de prévoir des cas obligatoires de désignations dans leur droit national. La Belgique a fait usage de cette prérogative à l'article 21 de la loi du 30 juillet 2018.

Dans toutes les autres situations, l'entreprise n'est pas tenue de désigner un DPO mais dispose toutefois de la faculté de le faire si elle le souhaite[113]. Cette désignation volontaire constitue même une bonne pratique, vivement encouragée par les autorités de contrôle étant donné que cela constitue le meilleur moyen d'assurer la protection des données personnelles au sein d'une entreprise [114]. Dans ce cas, le régime des articles 37 à 39 s'appliqueront[115].

Enfin, lorsqu'une entité ne désigne pas de DPO, une autre bonne pratique est de tout de même désigner un « référant en protection des données »[116]. Le G29 précise également qu'il est permis pour une organisation d'engager du personnel ou des consultants extérieurs pour

---

[108] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 7.

[109] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 7.

[110] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 8.

[111] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 8.

[112] Art. 37, §4 RGPD.

[113] Art. 37, §4 RGPD.

[114] O. FORET, *op. cit.*, p. 235.

[115] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 5.

[116] O. FORET, *op. cit.*, p. 235.

des tâches en la matière, à condition de clarifier expressément qu'ils n'ont pas le titre de DPO[117].

3. Profil et expertise

Une entreprise peut avoir recours à un DPO interne, c'est-à-dire désigner un membre de son personnel comme DPO, ou à un DPO externe, en exerçant ses missions sur la base d'un contrat de service[118].

Aucun diplôme ni certification spécifique n'est requis pour occuper cette fonction[119]. Toutefois, l'article 37, paragraphe 5, énonce que le DPO doit être sélectionné en fonction de ses « qualités professionnelles », spécialement de ses « connaissances spécialisées du droit et des pratiques en matière de protection des données », ainsi que de sa « capacité à accomplir les missions visées à l'article 39 ». Des explications détaillées peuvent être trouvées dans les lignes directrices du G29 ainsi que dans la recommandation de l'APD[120].

Premièrement, le niveau d'expertise exigé doit être déterminé en tenant compte des opérations de traitement effectuées, et de la protection requise pour les données traitées par l'organisation[121]. Il doit être adapté à la sensibilité, à la complexité et au volume de données traitées[122].

Deuxièmement, la notion de qualités professionnelles exige que le DPO ait une connaissance approfondie des lois et pratiques nationales et européennes de la protection des données, ainsi qu'une maîtrise du RGPD. En outre, sa connaissance du secteur d'activité et de l'organisation représente un avantage significatif[123].

Le DPO doit également posséder des connaissances techniques. En effet, il doit pouvoir échanger avec la direction générale mais également avec les directions opérationnelles concernant les aspects techniques, notamment ceux liés aux exigences de protection des données dès la conception et par défaut. À cette fin, il doit pouvoir analyser avec précision les aspects techniques pour ensuite pouvoir les interpréter juridiquement[124].

Par ailleurs, les qualités personnelles du DPO et sa position dans l'organisation ne sont pas à négliger. Celui-ci doit faire preuve d'éthique et d'intégrité[125]. Puisqu'il doit être en mesure de

---

[117] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 5.

[118] Art. 37, §6 RGPD.

[119] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°04/2017 (…), *op. cit.,* p. 16 (point 43).

[120] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°04/2017 (…), *op. cit.*

[121] Cons. 97 RGPD.

[122] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 11.

[123] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 11.

[124] A. BENSOUSSAN, « Préface », V. BENSOUSSAN-BRULÉ *et al.*, *Le Data Protection Officer. Une fonction nouvelle dans l'entreprise*, Bruxelles, Bruylant, 2017, p. IX.

[125] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 11.

coordonner les équipes de son entreprise en vue d'assurer leur conformité, il doit également être doté de solides compétences humaines et relationnelles, savoir faire preuve d'une bonne communication, et être capable de gérer les conflits[126]. Ces *soft skills* sont d'autant plus essentielles que nous verrons qu'il peut être amené à devoir gérer une équipe[127].

En résumé, un DPO doit posséder un ensemble de compétences, tant juridiques, que techniques, organisationnelles et stratégiques[128].

4. Ressources nécessaires à la réalisation de sa mission

Afin de garantir la protection des données au sein de l'organisation, il est impératif que le DPO dispose des moyens adéquats pour remplir efficacement ses fonctions.

D'une part, cela signifie une implication précoce du DPO dans les projets de traitements des données. L'article 38, paragraphe 1, impose en effet à l'entreprise de veiller à associer le DPO « [d]'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données ». Son intégration dès les premières étapes de tout projet simplifie la mise en conformité au RGPD, mais garantit également une approche intégrant la protection de la vie privée dès la conception conformément à l'article 25, paragraphe 1[129]. En outre, le G29 mentionne l'importance de considérer le DPO comme un « partenaire de discussion » au sein de l'entreprise. À cette fin, une entreprise doit notamment le convier aux réunions managériales, solliciter sa présence lors des prises de décisions affectant les données personnelles, lui communiquer les informations nécessaires à temps pour qu'il puisse fournir un avis, ou encore tenir compte de son avis[130].

D'autre part, le second paragraphe de l'article 38 impose au responsable de traitement de fournir au DPO les « ressources nécessaires » pour exercer ses missions, ainsi que l'accès aux données et aux opérations de traitement. Cela implique de mettre à sa disposition des ressources financières suffisantes et des infrastructures et équipements adéquats. De plus, celui-ci doit également disposer de suffisamment de temps pour réaliser ses missions, ainsi que de la possibilité de suivre une formation continue pour rester à jour en matière du droit de la protection des données personnelles[131]. Par ailleurs, cette disposition oblige également de mettre à sa disposition les moyens humains dont il a besoin, de sorte que le DPO est parfois

---

[126] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°04/2017 (…), *op. cit.,* p. 16 (point 44).

[127] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°04/2017 (…), *op. cit.,* p. 16 (point 47).

[128] A. BENSOUSSAN, « Préface », V. BENSOUSSAN-BRULÉ *et al.*, *Le Data Protection Officer. Une fonction nouvelle dans l'entreprise*, Bruxelles, Bruylant, 2017, p. IX.

[129] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 13.

[130] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 13.

[131] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 14.

assisté d'une équipe pluridisciplinaire composée de juristes, mais également d'ingénieurs en sécurité informatique[132].

5. Indépendance

Afin de garantir l'efficacité de son action, il est essentiel que le DPO puisse exercer ses missions en toute indépendance[133]. Parmi ces garanties d'autonomie, le règlement prévoit que le DPO ne doit recevoir aucune instruction se rapportant à l'exercice de ses fonctions et qu'il ne doit subir aucune influence interne ni externe lorsqu'il effectue son travail. Deuxièmement, celui-ci a le devoir de rapporter directement au plus haut niveau de direction. Il est également protégé contre les représailles en ce qu'il ne peut être ni pénalisé, ni licencié, ni menacé d'être licencié pour ses avis et actions prises dans le cadre de ses fonctions[134]. Pour finir, bien que le DPO puisse remplir des rôles supplémentaires au sein de l'organisation, ces responsabilités ne doivent pas entraîner de conflit d'intérêts avec ses devoirs en matière de protection des données[135]. En guise d'exemple, une entreprise a été sanctionnée pour avoir nommé comme DPO son directeur des services d'Audit interne, de *Risk Management* et de *Compliance*[136].

6. Missions

Le DPO est un pilier central pour assurer le respect par une entreprise de l'obligation d'*accountability* en ce qu'il est la personne chargée de veiller à ce que qu'elle agisse en conformité avec le RGPD[137]. De ce fait, au vu de ces missions, il peut également se révéler être un précieux outil de compétitivité pour les entreprises[138]. Ses missions sont décrites à l'article 39 du règlement.

Premièrement, il a pour rôle d'informer et de conseiller l'organisation ainsi que ses employés sur leurs obligations en matière de protection des données[139]. Cela consiste, par exemple, en des formations du personnel et des actions des sensibilisation[140].

Deuxièmement, le DPO est chargé de vérifier le respect du RGPD au sein de l'entreprise[141], ce qui peut inclure la réalisation d'audits et la formulation de recommandations[142].

Troisièmement, il joue un rôle déterminant dans le cadre des analyses d'impact sur la protection des données en prodiguant des conseils au responsable de traitement qui le demande, et en vérifiant leur exécution, conformément à l'article 35, paragraphe 2[143]. Il le

---

[132] O. FORET, *op. cit.*, p. 238.
[133] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *op. cit.,* p. 198.
[134] Art. 38, §3 RGPD.
[135] Art. 38, §6 RGPD.
[136] A.P.D. (Ch. Contentieuse), Décision quant au fond 18/2020 du 28 avril 2020, p. 17.
[137] H. LEGRAS, « Les missions du DPO », V. BENSOUSSAN-BRULÉ *et al.*, *Le Data Protection Officer. Une fonction nouvelle dans l'entreprise*, Bruxelles, Bruylant, 2017, p. 27 et 45.
[138] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°04/2017 (…), *op. cit.*, p. 8 (point 18).
[139] Art. 39, §1, a) RGPD.
[140] O. FORET, *op. cit.*, p. 237.
[141] Art. 39, §1, b) RGPD.
[142] O. FORET, *op. cit.*, p. 237.
[143] Art. 39, §1, c) RGPD.

guide notamment quant à la nécessité de réaliser une AIPD, la méthode à privilégier, ou encore les mesures techniques et organisationnelles à mettre en œuvre pour minimiser les risques[144].

Enfin, le DPO doit coopérer avec l'autorité de contrôle et il agit comme point de contact entre celle-ci et l'entreprise, notamment concernant les demandes de conseils, la gestion des plaintes, et la gestion des contrôles[145].

2. Tenue d'un registre des activités de traitement

1. Définition et objectifs

Lorsqu'une entreprise traite des données à caractère personnel, une des premières démarches à entreprendre est de rédiger un registre des activités de traitement (ci-après « le registre »). L'obligation de tenir un registre est imposée par l'article 30 du règlement et s'applique à la quasi-totalité des responsables de traitements et des sous-traitants.

La rédaction du registre consiste à cartographier les traitements de données envisagés ou réalisés par une organisation[146]. Il s'agit d'un document qui recense de manière exhaustive et détaillée les activités de traitements, dans l'objectif pour l'entreprise de bénéficier d'une vue d'ensemble de ces traitements et des données personnelles qu'elle possède[147]. En ce sens, le registre constitue un véritable « outil de l'*accountability* »[148]. Il représente un document fondamental pour assurer la conformité d'une entreprise au droit de la protection des données personnelles et garantir son respect des principes et obligations imposés par le RGPD[149].

D'autre part, ce registre constitue une mine d'informations et est destiné à être remis à l'APD en cas de contrôle de conformité[150]. Il s'agit d'une des premières pièces que l'autorité de contrôle demandera, et que le responsable de traitement devra fournir en vertu de l'article 30, paragraphe 4[151].

2. Cas où la tenue d'un registre est obligatoire

En vertu de l'article 30, paragraphes 1 et 2, tous les responsables de traitement et sous-traitants – et le cas échéant, leur représentant – sont soumis à cette obligation de tenir un registre. La notion de responsable de traitement vise l'entité qui détermine les finalités et les moyens du traitement, tandis que le sous-traitant est celui qui traite des données à caractère

---

[144] Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016, p. 17.
[145] O. FORET, *op. cit.*, p. 237.
[146] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n° 06/2017 du 14 juin 2017 relative au Registre des activités de traitements (article 30 du RGPD) (CO-AR-2017-011), p. 20.
[147] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n° 06/2017 (…), *op. cit.,* p. 8 (point 22).
[148] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n° 06/2017 (…), *op. cit.,* p. 7 (point 21).
[149] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 20.
[150] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 8 (point 24).
[151] B. LAMON, *op. cit.*, p. 223.

personnel pour le compte du responsable de traitement. Ces notions sont respectivement définies aux articles 4, paragraphes 7 et 8 du règlement et ont fait l'objet de développements par l'APD auxquels nous renvoyons pour d'avantage de précisions[152].

Par exception, une entreprise qui compte moins de 250 employés ne doit toutefois pas établir de registre, à moins que le traitement présente un risque pour les droits et libertés des personnes concernées, que le traitement soit régulier et non pas occasionnel, ou qu'il concerne des données sensibles énumérées à l'article 9, paragraphe 1 ou des données pénales mentionnées à l'article 10[153]. En ce qui concerne le potentiel « risque » pour les droits et libertés des personnes concernées, cette notion est éclairée par le considérant 75, qui cite par exemple le cas d'un traitement pouvant entraîner une discrimination, un vol, une usurpation d'identité ou encore une perte financière.

Cela étant dit, l'APD encourage fortement toutes les entreprises à documenter leurs traitements et à dresser un registre, même lorsque cela n'est pas obligatoire[154]. La rédaction d'un tel registre constitue une bonne pratique, vivement conseillée par les autorités de contrôle car il s'agit d'un moyen efficace pour démontrer sa conformité.

3. Contenu

Le registre d'une entreprise agissant en qualité de responsable de traitement doit contenir *a minima* une série d'informations essentielles. Celles-ci sont énumérées à l'article 30, paragraphe 1, et incluent le nom et les coordonnées du responsable de traitement, les finalités du traitement, une description des catégories de personnes concernées et des catégories de données traitées pour chaque finalité[155], les catégories de destinataires, les éventuels transferts de données vers des pays tiers ou à des organisations internationales, les délais prévus pour l'effacement des données, et enfin, une présentation des mesures de sécurité techniques et organisationnelles mises en place conformément à l'article 32, paragraphe 1[156].

Dans le cas d'une entreprise qui effectue des traitements en qualité de sous-traitant, le contenu du registre diffère légèrement et est détaillé au second paragraphe de l'article 30[157].

Outre ces mentions obligatoires, l'entreprise est libre d'ajouter des informations complémentaires utiles à sa mise en conformité et à la documentation de celle-ci[158]. Par exemple, le registre pourrait mentionner le service responsable pour l'exercice du droit d'accès, les mesures prévues pour l'exercice de ce droit, l'inventaire des violations de données à caractère personnel, la nécessité de réaliser une AIPD selon la nature du traitement[159], un registre des consentements, ou encore une hiérarchisation des traitements selon leur

---

[152] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 3 et 4.
[153] Art. 30, §5 RGPD.
[154] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 7 (point 19).
[155] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 13.
[156] Art. 30, §1 RGPD.
[157] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 15.
[158] O. TAMBOU, *op. cit.*, p. 277.
[159] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 16 et 17 (point 42).

sensibilité afin de déterminer où agir en priorité[160]. D'autres éléments comme la dénomination du traitement[161], sa base légale, ou sa date de création, sont également pertinents pour améliorer la transparence et la précision du registre[162].

Chaque traitement devant être documenté dans le registre et un traitement étant identifié par sa finalité, les informations ci-dessus doivent être spécifiées pour chacune des finalités de traitement distincte.

4. Forme

Le règlement n'impose pas de format strictement réglementé ou de modèle type pour le registre, permettant une certaine flexibilité, mais ce dernier doit cependant respecter certaines caractéristiques pour être conforme.

Premièrement, le registre doit impérativement être écrit[163]. Bien qu'il puisse techniquement être tenu sous forme papier, la forme électronique est toutefois fortement conseillée pour des raisons pratiques et de conformité[164].

Ensuite, l'entreprise doit garder à l'esprit que le registre est destiné à être consulté par l'autorité de contrôle. Il doit dès lors être rédigé dans un langage clair et accessible, ainsi qu'être lisible et compréhensible pour l'APD[165].

Face à la diversité des opérations de traitement, le règlement n'impose aucun modèle unique pour le registre[166]. Cependant, pour aider les entreprises dans cette démarche, l'APD a élaboré un exemple de modèle prenant la forme d'un tableau, disponible sur son site internet[167]. En outre, elle encourage vivement les associations professionnelles à suggérer des canevas-type personnalisables qui tiennent compte des spécificités sectorielles[168]. Cette absence de forme obligatoire offre une certaine flexibilité, permettant une conception adaptée aux besoins de chaque organisation. Une entreprise a dès lors la possibilité de choisir la configuration du registre qui lui semble la plus adaptée à ses activités et à sa structure opérationnelle.

Lorsqu'une entreprise assume à la fois les rôles de responsable de traitement et de sous-traitant, elle doit en principe tenir deux registres distincts[169]. Néanmoins, l'APD souligne une nouvelle fois la flexibilité qui doit être laissée. Elle précise que d'autres options sont

---

[160] O. TAMBOU, *op. cit.*, p. 277.
[161] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 16 (point 42).
[162] B. LAMON, *op. cit.*, p. 223.
[163] Art. 30, §3 RGPD.
[164] https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/registre-des-activites-de-traitement/comment-etablir-un-registre-
[165] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 18 et 21.
[166] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 18 (point 46).
[167] https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/registre-des-activites-de-traitement/comment-etablir-un-registre-
[168] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 18 (point 48).
[169] O. TAMBOU, *op. cit.*, p. 267.

concevables, telles que la tenue d'un registre unique avec deux volets distincts, ou d'un registre qui, pour chaque traitement, indique si ce dernier est réalisé en qualité de responsable de traitement ou de sous-traitant[170]. La décision entre ces options dépendra des spécificités de l'entreprise, de la complexité et du volume des traitements de données qu'elle gère, ainsi que de ses capacités à maintenir à jour ces informations de manière efficace. Pour les entreprises ayant des opérations de traitement moins complexes ou un nombre limité de traitements pour lesquels elles agissent comme sous-traitant, un registre unique avec des volets distincts peut être la solution la plus pratique. Cela permet une vue d'ensemble cohérente et centralisée des activités de traitement, tout en respectant les exigences réglementaires pour chaque rôle.

Enfin, l'entreprise est libre de choisir la langue dans laquelle rédiger son registre. Lors de l'examen du registre par l'autorité de contrôle, cette dernière pourra cependant exiger qu'il soit traduit dans l'une des langues nationales aux frais de l'entreprise[171].

3. Réalisation d'une analyse d'impact relative à la protection des données

1. Définition et objectifs

L'obligation pour le responsable de traitement d'effectuer une analyse d'impact relative à la protection des données, ci-après « AIPD », est prévue à l'article 35 du RGPD. L'AIPD est un instrument essentiel pour assurer la mise en œuvre du principe d'*accountability* dans la mesure où elle permet à l'entreprise d'assurer le respect des normes du RGPD, mais également de démontrer cette conformité[172].

Il s'agit d'une mesure préalable que le règlement impose de réaliser avant certains traitements[173]. En tant qu'outil d'évaluation des risques, l'AIPD est conçue pour identifier et gérer les risques pour les droits et libertés des personnes physiques avant le début du traitement[174]. Ce processus permet aux entreprises de développer des stratégies pour atténuer ces risques en amont[175] [176]. En outre, nous verrons que cette analyse d'impact a

---

[170] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 18 (point 49).

[171] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 19 (point 52).

[172] Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01, p. 4.

[173] Art. 35, §1 RGPD.

[174] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation N° 01/2018 du 28 février 2018 concernant l'analyse d'impact relative à la protection des données et la consultation préalable (CO-AR-2018-001), p.4.

[175] COMMISSION EUROPÉENNE, *Le RGPD : nouvelles opportunités, nouvelles obligations. Tout ce que les entreprises doivent savoir à propos du règlement général européen sur la protection des données,* Luxembourg, Office des publications de l'Union européenne, 2018, p. 16.

[176] COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Documenter (…),* p. 5.

également pour objectif de déterminer s'il est nécessaire de consulter l'autorité de contrôle préalablement au traitement[177].

2. Cas où la réalisation d'une AIPD est obligatoire

Le RGPD n'impose pas de réaliser une AIPD pour chaque opération de traitement[178].

De manière générale, une entreprise qui envisage de traiter des données a l'obligation d'effectuer une AIPD *lorsque le traitement « [e]st susceptible d'engendrer un risque élevé* » pour les droits et libertés des personnes physiques[179]. Le considérant 75 énonce qu'un traitement présente des risques élevés s'il est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral[180]. Pour plus de précisions, nous renvoyons à la liste exemplative figurant à ce considérant.

L'article 35, paragraphe 3, énonce trois cas dans lesquels une opération de traitement est considérée comme présentant un risque élevé, et pour lesquels une AIPD est requise en tout état de cause[181]. Il s'agit du cas d'un traitement automatisé qui vise un profilage décisionnel ; d'un traitement à grande échelle de données visées aux articles 9, paragraphe 1, et 10 ; et de la surveillance systématique à grande échelle d'une zone accessible au public.

Par ailleurs, dans ses lignes directrices, le G29 a identifié neuf critères pour aider les entreprises à évaluer si un traitement est susceptible de présenter un risque élevé et nécessite, par conséquent, une AIPD[182]. Ces critères sont l'évaluation ou la notation (dont le profilage), la prise de décisions automatisée avec effet juridique ou similaire significatif, la surveillance systématique, la présence de données sensibles ou pénales, le traitement de données à grande échelle, le croisement ou la combinaison d'ensemble de données, le traitement de données concernant des personnes vulnérables, l'utilisation innovante ou l'application de nouvelles solutions technologiques ou organisationnelles, et enfin, les traitements susceptibles d'exclure du bénéfice d'un droit, d'un service ou d'un contrat[183]. Des explications détaillées et des exemples sont disponibles dans ces lignes directrices[184]. En règle générale, le G29 estime qu'une AIPD doit être effectuée dès lors que le traitement répond à au moins deux des critères établis[185]. Toutefois, le responsable de traitement peut parfois

---

[177] B. LAMON, *op. cit.*, p. 224.

[178] Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01, p. 5.

[179] Art. 35, §1 RGPD.

[180] B. LAMON, *op. cit.*, p. 224.

[181] Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01, p. 10.

[182] *Ibidem*, p. 10.

[183] *Ibidem*, p. 10 à 12.

[184] *Ibidem* p. 10 à 14.

[185] *Ibidem* p. 13.

estimer qu'une AIPD est nécessaire bien qu'un seul critère soit rencontré[186]. Lorsqu'il estime qu'une opération de traitement répondant aux critères ne présente pas de risque élevé, il doit justifier et documenter sa décision de ne pas réaliser une AIPD, en incluant l'avis du DPO[187]. Enfin, le G29 affirme qu'une AIPD peut être indispensable notamment lorsque le traitement met en œuvre une nouvelle technologie[188].

En outre, l'article 35, paragraphe 4, énonce que les autorités de contrôle doivent établir et publier une liste des types d'opérations de traitement nécessitant une AIPD[189]. En Belgique, l'APD a fait usage de cette disposition et a énuméré huit cas supplémentaires dans lesquels une AIPD est obligatoire[190] [191]. Le paragraphe 5 du même article habilite quant à lui les autorités de contrôle à établir et publier une liste des opérations de traitement qui ne requièrent pas la réalisation d'une AIPD[192].

Pour finir, en cas d'incertitude sur la nécessité de réaliser une AIPD, le G29 recommande d'y procéder en ce qu'elle constitue une des bonnes pratiques d'une entreprise[193] [194].

3. Contenu

L'article 35, paragraphe 7, énonce les informations minimales devant figurer dans une AIPD.

Premièrement, celle-ci doit comporter une description systématique des opérations de traitement envisagées et des finalités du traitement[195]. Cette description contient une série d'éléments obligatoires, tels que des renseignements sur les données, les destinataires, les personnes concernées, la durée du traitement, ou encore les actifs sur lesquels les données reposent[196].

Deuxièmement, une AIPD doit impérativement contenir une évaluation de la nécessité et de la proportionnalité du traitement au regard de ses finalités[197].

---

[186] *Ibidem* p. 13.
[187] *Ibidem* p. 14.
[188] *Ibidem* p. 16.
[189] *Ibidem*, p. 14.
[190] O. TAMBOU, *op. cit.*, p. 266.
[191] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation N° 01/2018 (…), *op. cit.,* p. 43 et 44.
[192] Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01, p. 15.
[193] Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01, p. 9.
[194] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, *Règlement général sur la protection des données. Préparez-vous en 13 étapes,* p. 10.
[195] Art. 35, §7, a) RGPD.
[196] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation N° 01/2018 (…), *op. cit.,* p. 17.
[197] Art. 35, §7, b) RGPD.

Elle doit également inclure une évaluation des risques potentiels pour les droits et libertés des personnes concernées, une notion qui fait référence à la procédure d'identification, d'analyse et d'évaluation des risques[198].

Enfin, l'entreprise doit y mentionner les mesures qu'elle prévoit de mettre en place pour faire face aux risques[199].

4. Moment de réalisation

Conformément aux principes de protection des données dès la conception et par défaut, l'AIPD doit être réalisée avant le traitement[200]. Elle doit être initiée dès le début du cycle de conception d'un nouveau traitement, idéalement au moment où « l'idée de la création » survient[201]. Toutefois, nous verrons que la réalisation d'une AIPD est un processus continu, qui doit également fait l'objet d'un réexamen régulier tout au long du traitement[202].

5. Acteurs

Plusieurs acteurs prennent part à l'élaboration de l'AIPD. En premier lieu, l'obligation de réaliser l'analyse d'impact incombe au responsable de traitement. Celui-ci a la possibilité de l'effectuer en interne ou de confier cette tâche à un organisme externe. Cependant, il conserve la responsabilité finale de s'assurer qu'elle est correctement exécutée[203]. Deuxièmement, selon la nature du traitement, le sous-traitant est tenu d'assister le responsable de traitement dans sa réalisation de l'AIPD en lui fournissant toutes les informations dont il a besoin[204]. Cette obligation de coopération découle de l'article 28, paragraphe 3, f)[205] [206]. Lorsqu'un DPO a été désigné par l'entreprise, celle-ci doit impérativement l'associer au processus et lui demander conseil[207]. Ce troisième acteur lui communique son avis concernant la nécessité d'effectuer une AIPD, la méthodologie à utiliser, le choix de la réalisation en interne ou externe, ou encore, sur les garanties et mesures à adopter[208]. Le responsable de traitement est également tenu de demander l'avis des

---

[198] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation N° 01/2018 (…), *op. cit.,* p. 19.

[199] Art. 35, §7, d) RGPD.

[200] Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01, p. 17.

[201] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation N° 01/2018 (…), *op. cit.,* p. 15.

[202] Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01, p. 17.

[203] *Ibidem* p. 17.

[204] *Ibidem* p. 17.

[205] Commission nationale de l'informatique et des libertés, « Lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD) » du 11 octobre 2018, p. 3

[206] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation N° 01/2018 (…), *op. cit.,* p. 29.

[207] Art. 35, §2 RGPD.

[208] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation N° 01/2018 (…), *op. cit.,* p. 30.

personnes concernées ou de leurs représentants[209]. Pour finir, d'autres personnes doivent idéalement être impliquées, telles que le responsable de la sécurité des systèmes d'information, les concepteurs de nouvelles applications, les juristes d'entreprise, les analystes, les employés qui utilisent ces données pour l'exercice de leurs tâches, des experts, etc.[210].

6. Forme et méthodologie

Le RGPD offre une flexibilité permettant au responsable de traitement de choisir parmi différentes méthodologies et de déterminer la structure et la forme spécifiques de l'AIPD[211], sans imposer de procédure exacte à suivre[212]. La méthodologie sélectionnée doit toutefois répondre aux critères d'acceptabilité d'une AIPD, définis par le G29 dans ses lignes directrices du 4 octobre 2017[213]. Comme pour le registre des activités de traitement, cette souplesse offre aux entreprises la possibilité de concevoir une AIPD dont la forme et la structure s'adaptent parfaitement à leurs pratiques du travail[214].

Plusieurs outils existent pour aider les entreprises et faciliter la conduite des AIPD. D'une part, des cadres européens génériques ont été proposés par certaines autorités de protection des données nationales[215]. Parmi ces initiatives, nous tenons à souligner le cas de la CNIL, qui a développé un logiciel « PIA » distribué en *open source* sur son site internet ainsi que plusieurs guides méthodologiques[216].

D'autre part, des cadres sectoriels ont également été publiés[217]. Le G29 incite à la création de tels cadres puisqu'ils permettent de tenir compte des particularités des traitements propres au secteur[218].

Par ailleurs, nous observons l'arrivée sur le marché de nouveaux outils issus d'acteurs privés, regroupés sous l'appellation de « RegTech »[219]. Ces logiciels permettent aux entreprises de gérer leurs obligations règlementaires de manière plus efficace, en ce qu'ils automatisent le processus d'évaluation des risques et comportent des questionnaires préconfigurés. Parmi leurs fonctionnalités, ces logiciels sont conçus pour être en conformité avec les législations spécifiques, pour faciliter la collaboration, et pour permettre une gestion centralisée de la documentation. Ils génèrent également des tableaux de bord visuels et des rapports détaillés, ainsi que des recommandations pour les mesures d'atténuation des risques. En outre, ils

---

[209] Art. 35, §9 RGPD.
[210] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation N° 01/2018 (…), *op. cit.,* p. 27.
[211] Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01, p. 20.
[212] *Ibidem*, p. 24.
[213] *Ibidem*, p. 26.
[214] *Ibidem*, p. 20.
[215] *Ibidem*, p. 24.
[216] https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
[217] *Ibidem*, p. 24.
[218] *Ibidem*, p. 21.
[219] B. LAMON, *op. cit.*, p. 226.

peuvent proposer des fonctionnalités de suivi continu, permettant de réévaluer périodiquement les traitements. Nous soulignons que ces outils ne sont pas spécifiques aux AIPD mais qu'ils sont, par exemple, également une aide à la rédaction du registre des activités de traitement. Pour une solution complète de gestion de la conformité, nous citons notamment le leader OneTrust[220]. Des inventaires détaillés de ces solutions sont toutefois disponibles sur internet[221] [222].

7. Consultation préalable

En vertu de l'article 36, paragraphe 1, le responsable de traitement est contraint de consulter l'autorité de contrôle préalablement au traitement quand l'AIPD fait apparaître que ce dernier présente un « risque résiduel élevé ». Cela sera le cas si l'entreprise est incapable d'identifier des mesures suffisantes pour diminuer les risques à un niveau acceptable[223].

4. Codes de conduite et certification

L'article 24, paragraphe 3, du règlement énonce expressément que l'adoption de codes de conduite, prévus aux article 40 et 41, et l'implémentation de mécanismes de certification, visés aux articles 42 et 43, constituent un moyen pour une entreprise de démontrer sa conformité au RGPD[224].

1. Codes de conduite

Les codes de conduite sont des ensembles de règles élaborées spécifiquement pour un secteur d'activité par des associations professionnelles ou des organismes représentant des catégories de responsables de traitement ou de sous-traitants[225]. Issus d'initiatives volontaires[226], ces codes sont conçus pour aider les entreprises, particulièrement les micro-entreprises et les PME, à respecter le RGPD[227]. Ils détaillent les pratiques optimales de gestion des données personnelles pour les entreprises d'un secteur donné. Ce faisant, ils traduisent les dispositions parfois abstraites du règlement en un ensemble de règles pratiques, leur permettant une mise en conformité simplifiée et à moindre coût[228].

---

[220] TNP, *Benchmark TNP. Outils DPO, CDO & CISO. Edition #4,* p. 40. Disponible sur https://www.tnpconsultants.com/benchmark-edition-4-gdpr-outils-dpo-cdo-ciso/.

[221] B. LAMON, *op. cit.*, p. 226.

[222] https://www.tnpconsultants.com/wp-content/uploads/2023/03/TNP-BENCHMARK-DES-OUTILS-DPO-CDO-CISO.pdf

[223] Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01, p. 22.

[224] Art. 24, §3 RGPD.

[225] Comité européen de la protection des données, « Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement (UE) 2016/679 », version 2.0, 4 June 2019, p. 7.

[226] https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-le-code-de-conduite

[227] Art. 40, §1 RGPD.

[228] Comité européen de la protection des données, « Lignes directrices 1/2019 (…), *op. cit.,* p. 9.

Les codes de conduite présentent donc une multitude d'avantages. Comme exposé ci-dessus, ils constituent un outil d'*accountability* en permettant de démontrer le respect du RGPD, ils offrent un cadre adapté aux besoins des micro, petites et moyennes entreprises, et ils permettent une application du règlement plus rentable et performante. Mais cela n'est pas tout. L'adhésion à un code de conduite permet de renforcer la confiance des personnes concernées[229], des clients, des partenaires, et des professionnels du secteur[230]. Cette démarche illustre, en effet, la volonté de l'entreprise d'instaurer une culture de protection des données allant au-delà de la simple conformité. En renforçant la transparence[231], les codes permettent dès lors d'améliorer sa réputation[232] et sa compétitivité[233].

2. Certification

La certification est un mécanisme permettant aux entreprises de démontrer officiellement qu'elles agissent conformément au RGPD. Selon les cas, cette certification est délivrée par des organismes accrédités selon l'article 43, ou directement par l'autorité de contrôle compétente[234]. Il s'agit d'un processus individuel[235], transparent et volontaire[236], qui est toutefois juridiquement contraignant une fois le certificat obtenu[237]. La durée de validité de cette certification est de trois ans au maximum, avec la possibilité d'un renouvellement[238].

Tout comme les codes de conduite, la certification présente de nombreux avantages. D'une part, elle permet d'informer les personnes concernées sur le degré de protection des données offert par les produits, services et systèmes de données de l'entreprises[239]. D'autre part, elle permet également de répondre spécifiquement aux besoins des micro, petites et moyennes entreprises[240]. En outre, ce mécanisme accroît la transparence[241], et par conséquent, renforce la crédibilité, la confiance et la visibilité de l'entreprise ; autant d'éléments essentiels dans le monde des affaires[242].

5. Autres mesures organisationnelles

Outre les mesures exposées précédemment, d'autres actions contribuent à permettre à une entreprise d'être conforme à l'obligation d'*accountability* et au règlement.

---

[229] Comité européen de la protection des données, « Lignes directrices 1/2019 (…), *op. cit.,* p. 10.
[230] https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-le-code-de-conduite
[231] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *op. cit.,* p. 204.
[232] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *op. cit.,* p. 204.
[233] O. TAMBOU, *op. cit.*, p. 298.
[234] Art. 42, §5 RGPD.
[235] O. TAMBOU, *op. cit.*, p. 302.
[236] Art. 42, §3 RGPD.
[237] https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-la-certification
[238] Art. 42, §7 RGPD.
[239] https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-la-certification
[240] https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-la-certification
[241] O. TAMBOU, *op. cit.*, p. 302.
[242] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *op. cit.,* p. 205.

En premier lieu, une entreprise se doit de mettre en œuvre des *programmes de formation et de sensibilisation réguliers du personnel* au RGPD[243]. Il est généralement conseillé d'agir en deux temps. Premièrement, une organisation dispense une formation générale, destinée à éduquer tous les employés sur les principes fondamentaux du RGPD, leurs responsabilités en matière de traitement des données, ainsi que les conséquences d'une non-conformité. Dans un second temps, l'organisation développe des formations plus spécialisées, propres aux profils, aux rôles et aux services[244]. En guise d'exemples, une formation spécifique sera dédiée aux collaborateurs chargés du traitement des données dans l'exercice de leurs missions, tels que les directeurs des ressources humaines, les directeurs informatiques, les développeurs, ou les directeurs d'entités opérationnelles[245]. L'objectif de cette démarche est de s'assurer que le personnel de l'entreprise est non seulement conscient des règles à suivre, mais aussi qu'il comprend l'importance de la protection des données personnelles et sait comment agir conformément aux exigences légales. Cette sensibilisation est cruciale car elle aide à prévenir les violations de données et renforce la culture de la protection des données au sein de l'organisation.

De plus, il est vivement conseillé à une entreprise d'élaborer, préalablement au traitement, une série de mécanismes et de procédures internes à suivre[246]. Celle-ci doit établir des procédures de gestion des demandes d'accès, de rectification et d'effacement, afin d'être en mesure de répondre rapidement aux demandes qui lui sont adressées par les personnes concernées. Elle doit également mettre en œuvre un mécanisme interne de gestion des plaintes, mais aussi une procédure de gestion et de déclaration efficace des infractions[247].

À ces mesures s'ajoutent la réalisation d'audits internes [248], la gestion et l'évaluation des sous-traitants et des prestataires tiers afin de s'assurer de leur conformité, ou encore, comme exposé précédemment, la mise en place de plans destinés à assurer la continuité ou la reprise des activités de l'entreprise ultérieurement à un sinistre ou une panne[249].

E. Réévaluation des mesures

Comme énoncé par la CNIL, « [l]a conformité n'est pas gravée dans le marbre et figée »[250]. Le respect de l'obligation d'*accountability* est un processus continu et dynamique, qui nécessite une attention constante tout au long du cycle de vie des traitements de données[251].

Concrètement, cela implique pour une entreprise l'obligation de réexaminer et mettre à jour régulièrement les mesures afin de s'assurer qu'elles restent adaptées à l'évolution des technologies et des circonstances opérationnelles de l'organisation[252]. L'article 24,

---

[243] L. FEILER, N. FORGÓ et M. WEIGL, *op. cit.*, p. 143.
[244] B. LAMON, *op. cit.*, p. 223.
[245] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 13.
[246] O. TAMBOU, *op. cit.*, p. 253.
[247] Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173, p. 13.
[248] O. TAMBOU, *op. cit.*, p. 252.
[249] https://www.pwc.be/en/services/audit-assurance/crisis-continuity-management.html
[250] https://www.cnil.fr/fr/comprendre-le-rgpd/les-six-grands-principes-du-rgpd.
[251] B. LAMON, *op. cit.*, p. 222.
[252] B. LAMON, *op. cit.*, p. 222.

paragraphe 1, stipule, en effet, que ces mesures doivent être « réexaminées et actualisées si nécessaire », reflétant l'importance d'une démarche proactive. Cette obligation s'applique à l'ensemble des mesures que nous avons examinées, tant techniques qu'organisationnelles.

Ainsi, par exemple, le registre des activités de traitement doit être régulièrement et constamment tenu à jour. L'APD parle d'un « outil vivant », en ce qu'il doit être actualisé pour suivre les changements des activités de l'entreprise[253].

En ce qui concerne l'analyse d'impact, le G29 affirme qu'elle doit être envisagée comme un exercice continu, et pas ponctuel. Elle nécessite des mises à jour régulières, pendant toute la durée du traitement, pour intégrer les changements dans le niveau de risque ou les conditions de mise en œuvre du traitement[254]. Une entreprise est tenue de procéder à des réexamens périodiques *a minima* tous les trois ans[255], ou à chaque modification significative du risque présenté par le traitement[256].

L'idée d'une responsabilité dans la durée est également présente dans les codes de conduite et la certification. En raison de leur nature juridiquement contraignante, les codes s'imposent aux entreprises qui y adhèrent et leur respect est régulièrement contrôlé via des audits internes[257]. La certification, quant à elle, n'est accordée que pour trois ans au plus, et est retirée si l'entreprise cesse de respecter les exigences[258].

De la même manière, une entreprise devra, par exemple, mettre à jour ses antivirus et adapter ses formations aux changements structurels de l'entreprise.

---

[253] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n°06/2017 (…), *op. cit.*, p. 19 (point 50).

[254] Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01, p. 17.

[255] Commission nationale de l'informatique et des libertés, « Lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD) » du 11 octobre 2018, p. 3.

[256] Art. 35, §11 RGPD.

[257] O. TAMBOU, *op. cit.*, p. 302.

[258] Art. 42, §7 RGPD.

CONCLUSION

L'*accountability* constitue une des principales innovations du RGPD, entré en vigueur le 25 mai 2018. Véritable clé de voûte du règlement, l'article 24 impose aux entreprises qui traitent des données à caractère personnel une obligation générale de « responsabilité » ou d'« *accountability* », composée de deux éléments. D'une part, les entreprises sont tenues d'adopter des mesures techniques et organisationnelles appropriées et efficaces afin de respecter le règlement. D'autre part, elles doivent tenir une documentation interne afin d'être en mesure de démontrer cette conformité.

Cette recherche avait pour ambition de fournir un aperçu global des principales mesures, techniques et organisationnelles, qu'une entreprise doit mettre en œuvre pour se conformer à son obligation générale d'*accountability*.

Dans un premier temps, nous avons tenu à explorer brièvement le champ des mesures techniques. Nous retenons qu'une entreprise se doit d'adopter des mesures strictement nécessaires, adaptées aux risques et au contexte de son organisation. Nous relevons notamment l'authentification des utilisateurs, la gestion des habilitations, le traçage des accès, la gestion des incidents, l'archivage et la destruction des données de manière sécurisée, ou encore, la protection des locaux.

Dans un second temps, nous avons analysé en profondeur les principales mesures organisationnelles. Premièrement, une entreprise est, dans certains cas, contrainte de désigner un délégué à la protection des données. Celui-ci peut être interne ou externe et doit être doté d'un ensemble de compétences juridiques, techniques, organisationnelles, et stratégiques. L'entreprise est légalement tenue de lui fournir certaines ressources, nécessaires à la réalisation de ses missions. Une attention particulière est accordée à l'indépendance du DPO et à l'absence de conflit d'intérêts. Deuxièmement, toutes les entreprises, sauf exception, ont l'obligation d'établir un registre des activités de traitement. Celui-ci doit contenir certaines informations précises, mais il peut cependant prendre une forme choisie par l'organisation, à condition de respecter certaines caractéristiques. Troisièmement, une entreprise est tenue de réaliser une analyse d'impact relative à la protection des données si le traitement qu'elle envisage est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. À nouveau, une flexibilité est laissée au responsable de traitement quant à la forme et la méthodologie, pour autant que certains critères d'acceptabilité soient rencontrés. Pour finir, il est conseillé aux organisations d'avoir recours aux codes de conduite et au mécanisme de certification, ou encore de former régulièrement son personnel au RGPD.

En définitive, le RGPD se caractérise par une grande flexibilité et une certaine souplesse octroyée aux responsables de traitement dans le choix des mesures à implémenter. Bien que cette flexibilité pose des défis pour certaines entreprises qui peinent à naviguer sans directives

précises[259], cette approche leur permet d'adopter des mesures adaptées à leurs besoins, tout en garantissant une protection substantielle pour les personnes concernées[260].

Face à l'avenir, il est impératif d'intégrer pleinement la notion d'*accountability* dans la conscience collective[261], encourageant les entreprises à adopter une culture de la responsabilité organisationnelle[262].

[259] E. KOSTA, R. LEENES et I. KAMARA, *ibidem,* p. 64.
[260] E. KOSTA, R. LEENES et I. KAMARA, *ibidem,* p. 67.
[261] E. KOSTA, R. LEENES et I. KAMARA, *ibidem,* p. 67.
[262] C. DOCKSEY, *op. cit.,* p. 568.

BIBLIOGRAPHIE

SOURCES LEGISLATIVES ET REGLEMENTAIRES

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E..,* L 281, 23 novembre 1995.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.,* L 119/1, 4 mai 2016.

Communication de la Commission au Parlement européen – Une meilleure protection et de nouvelles perspectives – Orientation de la Commission relative à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018, COM (2018) 43 final, 24 janvier 2018.

JURISPRUDENCE

A.P.D. (Ch. Contentieuse), Décision quant au fond 18/2020 du 28 avril 2020.

A.P.D. (Ch. Contentieuse), décision 56/2021 du 26 avril 2021. Disponible sur https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-56-2021.pdf.

A.P.D. (Ch. Contentieuse), décision quant au fond 127/2022 du 19 août 2022. Disponible sur https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-127-2022.pdf.

DOCTRINE

Ouvrages

COMMISSION EUROPÉENNE, *Le RGPD : nouvelles opportunités, nouvelles obligations. Tout ce que les entreprises doivent savoir à propos du règlement général européen sur la protection des données,* Luxembourg, Office des publications de l'Union européenne, 2018.

COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, *Guide de la CNIL. La sécurité des données personnelles,* 2018. Disponible sur https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_guide_securite_personnelle.pdf.

COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Documenter le traitement des données : Le guide du CEPD pour garantir l'obligation de rendre compte*, Luxembourg, Office des publications de l'Union européenne, 2019, p. 3. Disponible sur https://op.europa.eu/en/publication-detail/-/publication/09445291-adbc-11e9-9d01-01aa75ed71a1/language-fr/format-PDF/source-310658513.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS et COUNCIL OF EUROPE, *Manuel de droit européen en matière de protection des données,* Luxembourg, Office des publications de l'Union européenne, 2019.

FEILER, L., FORGÓ, N. et WEIGL, M., *The EU General Data Protection Rgulation (GDPR): A Commentary*, Woking, German Law Publishers, 2018.

KOSTA, E., LEENES, R., et KAMARA, I., *Research Handbook on EU Data Protection Law*, Cheltenham, Edward Elgar Publishing Limited, 2022.

TAMBOU, O., *Manuel de droit européen de la protection des données à caractère personnel,* Bruxelles, Bruylant, 2020.

TNP, *Benchmark TNP. Outils DPO, CDO & CISO. Edition #4,* p. 40. Disponible sur https://www.tnpconsultants.com/benchmark-edition-4-gdpr-outils-dpo-cdo-ciso/.

YUMING, L., *Droit des données 2.0. Construction du système de droits. Laboratoire clé de la stratégie des métadonnées*, Oxford, Peter Lang, 2021.

YUMING, L., *Droit des données 3.0. Perspective législative. Laboratoire clé de la stratégie des métadonnées*, Oxford, Peter Lang, 2022.

Articles de revue

ANCIAUX, A. et FARCHY, J., « Données personnelles et droit de propriété : quatre chantiers et un enterrement », *Revue internationale de droit économique*, 2015, p. 307 à 331.

Contributions à un ouvrage collectif

BENSAMOUN, A., et BERTRAND, B., « Prolégomènes », A. BENSAMOUN et B. BERTRAND (dir.), *Le règlement général sur la protection des données. Aspects institutionnels et matériels,* Mare & Martin, 2020, p. 14.

BENSOUSSAN, A., « Préface », BENSOUSSAN-BRULÉ, V., *et al.*, *Le Data Protection Officer. Une fonction nouvelle dans l'entreprise*, Bruxelles, Bruylant, 2017, p. IX.

DOCKSEY, C., « Article 24. Responsibility of the controller », *The EU General Data Protection Regulation (GDPR). A Commentary*, C. KUNER, L. BYGRAVE et C. DOCKSEY, Oxford, Oxford University Press, p. 557.

FORET, O., « Le rôle du DPO », *Le règlement général sur la protection des données. Aspects institutionnels et matériels*, A. BENSAMOUN et B. BERTRAND (dir.), Mare & Martin, 2020, p.234.

LAMON, B., « Le principe d' ''*accountability*'' et les instruments de mise en conformité », *Le règlement général sur la protection des données. Aspects institutionnels et matériels*, A. BENSAMOUN et B. BERTRAND (dir.), Mare & Martin, 2020, p. 219.

LEGRAS, H., « Les missions du DPO », V. BENSOUSSAN-BRULÉ *et al.*, *Le Data Protection Officer. Une fonction nouvelle dans l'entreprise*, Bruxelles, Bruylant, 2017, p. 27.

AVIS, LIGNES DIRECTRICES ET RECOMMANDATIONS

Article 29 Data Protection Working Part (G29), "Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2016

COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Recommandation n° 06/2017 du 14 juin 2017 relative au Registre des activités de traitements (article 30 du RGPD) (CO-AR-2017-011).

COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, *Règlement général sur la protection des données. Préparez-vous en 13 étapes,* p. 6. Disponible sur https://www.autoriteprotectiondonnees.be/publications/plan-en-13-etapes.pdf.

Commission nationale de l'informatique et des libertés, « Lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD) » du 11 octobre 2018.

Comité européen de la protection des données, « Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement (UE) 2016/679 », version 2.0, 4 June 2019

Groupe de travail « Article 29 », Avis °3/2010 sur le principe de responsabilité, WP 173.

Groupe de travail « Article 29 » (G29) sur la protection des données, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du présent règlement (UE) 2016/679 », WP 248 rév. 01.

SOURCES INTERNET

https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/registre-des-activites-de-traitement/comment-etablir-un-registre-

https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-le-code-de-conduite

https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-la-certification

https://www.pwc.be/en/services/audit-assurance/crisis-continuity-management.html

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

https://www.tnpconsultants.com/wp-content/uploads/2023/03/TNP-BENCHMARK-DES-OUTILS-DPO-CDO-CISO.pdf