Le rôle du DPO dans la mise en oeuvre de la directive sur les lanceurs d'alerte

Lachapelle, Amelie

Published in:
DPO news

Publication date:
2021

Document Version
le PDF de l'éditeur

Le rôle du DPO dans la mise en œuvre de la directive sur les lanceurs d'alerte

Introduction

1. Parmi les directives européennes pour lesquelles une transposition de la part du législateur belge est attendue prochainement[1], la directive (UE) 2019/1937 du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union (ci-après «directive») mérite assurément l'attention des *Data Protection Officers* (ci-après DPO)[2].

   D'une part, parce que cette directive s'applique aux personnes signalant des violations en droit de l'Union notamment dans le domaine de la protection de la vie privée et des données à caractère personnel et dans celui de la sécurité des réseaux et des systèmes d'information[3]. D'autre part, parce que le fonctionnement d'un dispositif d'alerte repose quasi automatiquement sur la collecte et l'exploitation de données à caractère personnel[4]. Il s'ensuit que les règles européennes de protection des données doivent être respectées dans ce cadre.

   Le DPO est donc susceptible d'être interpellé tant en amont qu'en aval de la procédure de signalement.

2. Parmi les obligations prévues par la directive, une obligation mérite, en particulier, d'être épinglée car sa mise en œuvre devra nécessairement avoir lieu en concertation avec le DPO, si une telle personne a été désignée au sein de l'organisation. Il s'agit de l'obligation pour les entités juridiques des secteurs public et privé, ainsi pour les autorités compétentes, d'établir des canaux de signalement interne et externe (dispositifs de *whistleblowing*).

   Cette obligation pose spécialement trois questions que nous traiterons après avoir défini la portée de l'obligation mentionnée.

I. L'obligation d'établir des canaux et des procédures de signalement (*whistleblowing*)

3. Conformément à l'article 8 de la directive, les entités juridiques des secteurs privé et public doivent établir des canaux et des procédures pour le signalement interne de violations au sens de la directive et pour le suivi, après consultation des partenaires sociaux et en accord avec ceux-ci lorsque le droit national le prévoit.

   Il est important de garder à l'esprit que ces mécanismes de signalement représentent un dispositif *complémentaire* à côté des autres dispositifs habituels de contrôle et de *reporting* (représentants des travailleurs, ligne hiérarchique, audit, service d'inspection, etc.)[5].

4. La notion d'entité juridique du secteur privé est entendue largement de telle sorte qu'elle devrait couvrir toutes les personnes morales visées par le Code des sociétés et des associations (CSA), à savoir toute organisation dotée de la personnalité juridique qui exerce une ou plusieurs activités déterminées dans un but lucratif ou non (sociétés, ASBL et fondations) dès l'instant où elle compte 50 travailleurs ou plus. Les entités du secteur privé relevant du champ d'application des actes sectoriels (notamment le secteur financier) sont visées par l'obligation indépendamment du nombre de travailleurs.

   La notion d'entité juridique du secteur public est également entendue largement comme désignant *a priori* tout pouvoir public, qu'il relève du pouvoir exécutif, législatif ou judiciaire, qu'il émane de l'autorité fédérale, des collectivités fédérées ou des pouvoirs locaux. À la différence des entités juridiques du secteur privé, les entités juridiques du secteur public sont soumises à l'obligation indépendamment du nombre de travailleurs.

5. Toute violation du droit de l'Union n'est pas visée par la directive. La directive s'attaque aux violations du droit de l'Union qui surviennent dans des domaines où une violation peut porter gravement atteinte à l'intérêt public[6]. Le législateur national est néanmoins libre d'étendre le champ d'application matériel de la directive dans le cadre de la loi de transposition[7].

   La notion de « violation » est large puisqu'elle englobe quatre catégories d'actes : (i) les actes ou omissions qui sont illicites et ont trait aux actes de l'Union et aux domaines relevant du champ d'application matériel visé à l'article 2 de la directive (activités illicites), (ii) les actes ou omissions qui vont à l'encontre de l'objet ou de la finalité des règles prévues dans les actes de l'Union et les domaines relevant du champ d'application matériel visé à l'article 2 de la directive (activités abusives), (iii) les violations qui ne se sont pas encore matérialisées mais qui vont très probablement avoir lieu ainsi que les actes ou omissions que l'auteur de signalement a des motifs raisonnables de considérer comme des violations et, enfin, (iv) les tentatives de dissimulation de violations.

[1] Les États membres ont jusqu'au 17 décembre 2021 pour prendre les dispositions législatives, réglementaires et administratives nécessaires à la transposition de la directive. Le délai est néanmoins plus long – jusqu'au 17 décembre 2023 – pour les entités juridiques du secteur privé comptant 50 à 249 travailleurs, s'agissant de l'obligation d'établir des canaux de signalement interne (art. 26 de la directive).

[2] Pour un commentaire de la directive sur les lanceurs d'alerte, voy. A. Lachapelle, « L'encadrement juridique du lancement d'alerte au sein de l'Union européenne. Commentaire de la directive sur les lanceurs d'alerte », *R.D.T.I.*, 2020, nos 78-79, pp. 15-52.

[3] Selon une interprétation littérale de la directive, la loi de transposition ne devrait s'appliquer qu'aux violations relevant du champ d'application des actes de l'Union expressément énumérés en annexe. Une telle interprétation nous paraît cependant trop restrictive en ce qu'elle compromet l'efficacité de la directive dont l'objectif est de favoriser le signalement de certaines violations du droit de l'Union qui peuvent porter gravement atteinte à l'intérêt public (considérant n° 3 de la directive).

[4] CPVP, Recommandation n° 01/2006 du 29 novembre 2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, p. 3. Voy. aussi APD, avis n° 128/2021 du 28 juillet 2021 ayant pour objet une demande d'avis concernant une proposition de loi tendant à offrir un statut légal et une protection aux lanceurs d'alerte, § 6.

[5] En ce sens, voy. not. B. Fasterling, « Whistleblower protection: A comparative law perspective », *in* D. Lewis, A. J. Brown et al. (éd.), *International Handbook on Whistleblowing Research*, Cheltenham, Edward Elgar Publishing, 2014, p. 345. En Belgique, voy. not. Commission de la protection de la vie privée (CPVP), Recommandation n° 01/2006 du 29 novembre 2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, p. 6.

[6] Considérant n° 3 de la directive.

[7] Art. 2, § 2, de la directive.

Comme annoncé, le domaine de la protection de la vie privée et des données à caractère personnel ainsi que celui de la sécurité des réseaux et des systèmes d'information figurent parmi les domaines couverts par la directive. Neuf autres domaines sont visés, notamment le domaine de la santé publique, celui de la protection de l'environnement ou encore celui des services, produits et marchés financiers et prévention du blanchiment de capitaux et du financement du terrorisme[8]. Sans relever d'un domaine particulier, sont également couvertes par la directive les violations portant atteinte aux intérêts financiers de l'Union ainsi que les violations relatives au marché intérieur, y compris les violations en matière de concurrence et d'aides d'État, de fraude fiscale et d'abus fiscal[9].

6. À qui s'adressent les dispositifs de signalement ? Les canaux et procédures s'adressent en premier lieu aux travailleurs de l'entité. Au sens strict, seul un travailleur peut bénéficier du statut de lanceur d'alerte. Le statut protecteur est, en effet, classiquement justifié au regard de la situation de vulnérabilité économique dans laquelle se trouve le travailleur qui s'expose à un risque de représailles s'il décide de signaler des faits dont il a eu connaissance sur son lieu de travail et qui se sont produits sous la responsabilité de son employeur[10]. Dans un arrêt récent, rendu dans le cadre de la célèbre affaire *Lux Leaks*, la Cour européenne des droits de l'homme souligne que le devoir de loyauté, de réserve et de discrétion qui découle du lien de subordination entre le travailleur et l'employeur « constitue une caractéristique particulière de la notion de lancement d'alerte »[11]. Les canaux et procédures de signalement interne peuvent également être ouverts aux autres personnes énumérées à l'article 4, § 1er, de la directive qui sont en contact avec l'entité juridique dans le cadre de leurs activités professionnelles, à savoir les indépendants, les actionnaires, les membres des organes de l'entreprise, les bénévoles et les stagiaires, ainsi que les contractants et les fournisseurs, de même qu'aux personnes visées à l'article 4, § 2 de la directive, à savoir les anciens travailleurs.

7. En vertu de l'article 11 de la directive, les autorités compétentes sont pareillement tenues d'établir des canaux de signalement externe. Par « autorité compétente », il faut entendre toute autorité nationale désignée pour recevoir des signalements conformément à la directive et fournir un retour d'informations à l'auteur de signalement, et/ou désignée pour exercer les fonctions prévues par la directive, notamment en ce qui concerne le suivi[12]. Il peut s'agir d'autorités judiciaires, d'organismes de réglementation ou de surveillance compétents dans les domaines spécifiques concernés, ou d'autorités dotées de compétences plus générales au niveau de l'État central, de services répressifs, d'organismes de lutte contre la corruption ou de médiateurs[13]. Des autorités aussi variées que la FSMA, la BNB, la CTIF, l'AFSCA, l'APD, le CCB, le SPF Économie et le SPF Santé publique sont ainsi des « autorités compétentes » au sens de la directive.

   La désignation d'un DPO étant obligatoire pour les autorités publiques et les organismes publics[14], les autorités compétentes pourront compter sur l'aide du DPO dans la configuration des dispositifs de signalement externe.

   Quoique la directive ne prévoie pas expressément l'accessibilité des dispositifs de signalement externe aux particuliers, rien n'empêche le législateur belge de le prévoir dans le cadre de la transposition de la directive. Une telle mesure permettrait de faire coïncider le nouveau dispositif d'alerte avec celui qui existe déjà en pratique dans le domaine financier.

Confidentialité	• Canaux confidentiels et sécurisés • Confidentialité de l'identité de l'auteur du signalement et de tout tiers mentionné dans le signalement • Respect du RGPD
Souplesse	Par écrit, par courrier, via une ou des boîtes à suggestions physiques ou via une plateforme en ligne (intranet ou internet), ou oralement, via une permanence téléphonique ou tout autre système de messagerie vocale et même lors d'une rencontre en personne
Accusé de réception	• 7 jours à compter de la réception • Pas de forme particulière
Désignation d'un gestionnaire de signalement (*Whistleblower Officer*)	• Externalisation possible • Mutualisation possible chez une même personne (CO, AML CO ? DPO ?) • MAIS garanties en termes d'indépendance et d'impartialité + expertise professionnelle appropriée • En principe, pas l'auditeur interne
Suivi diligent	• Suivi diligent = toute mesure prise par le destinataire du signalement, ou toute autorité compétente, pour évaluer l'exactitude des allégations formulées dans le signalement et, le cas échéant, pour remédier à la violation signalée, y compris par des mesures telles qu'une enquête interne, une enquête, des poursuites, une action en recouvrement de fonds, ou la clôture de la procédure • Suivi diligent des signalements anonymes lorsque le droit national le prévoit
Retour d'informations	Max. 3 mois à compter de l'accusé de réception du signalement ou, à défaut d'accusé de réception, 3 mois à compter de l'expiration de la période de 7 jours suivant le signalement
Information	• Informations claires et facilement accessibles à l'attention des destinataires des canaux • Sensibilisation – « Culture de la bonne communication et de la RSE »

[8] Ce dernier domaine était déjà visé par des actes sectoriels de l'Union. L'article 3, § 1er, de la directive règle l'articulation de la directive avec les actes sectoriels de l'Union qui prévoient déjà un dispositif de *whistleblowing*.

[9] Art. 2, § 1er, points b et c, de la directive.

[10] Considérant no 36 de la directive.

[11] Cour eur. D.H. (3e sect.), arrêt *Halet c. Luxembourg*, 11 mai 2021, req. no 21884/18, § 91.

[12] Art. 5, 14°, de la directive.

[13] Considérant no 64 de la directive.

[14] Art. 37, § 1er, point a), de la directive.

II. Les exigences auxquelles doivent répondre les dispositifs de signalement

8. L'article 9 de la directive impose un certain nombre d'exigences dans la conception des dispositifs de signalement interne. Les exigences imposées par la directive sont synthétisées dans le tableau de la page précédente.

   La confidentialité est une mesure *ex ante* essentielle pour éviter les représailles[15]. C'est pourquoi l'article 16 de la directive lui est spécialement dédié. La confidentialité occupe, par ailleurs, une place essentielle au regard des règles européennes de protection des données. L'identité de l'auteur de signalement ne peut pas être divulguée sans le consentement exprès de celui-ci à toute personne autre que les membres du personnel autorisés compétents pour recevoir des signalements ou pour en assurer le suivi. Cela s'applique également pour toute autre information à partir de laquelle l'identité de l'auteur de signalement peut être directement ou indirectement déduite. En leur qualité de « responsables du traitement », les entités juridiques et les autorités compétentes sont, en particulier, tenues de traiter les données à caractère personnel collectées dans le cadre du dispositif d'alerte de façon à en garantir une sécurité appropriée « à l'aide de mesures techniques ou organisationnelles appropriées »[16].

9. Les dispositifs de signalement externe doivent répondre à des exigences similaires à celles exposées plus haut pour le signalement interne, mais plus détaillées. En particulier, l'article 12 de la directive précise ce qu'il faut entendre par canaux « indépendants et autonomes ». L'obligation d'information est, en outre, renforcée en vertu de l'article 13 de la directive. Le retour d'informations doit, quant à lui, intervenir dans un délai raisonnable n'excédant pas trois mois, ou six mois dans des cas dûment justifiés. Cependant, le droit interne peut faire obstacle à un tel retour d'informations, notamment pour des considérations liées au secret professionnel ou au droit à la vie privée. C'est le cas notamment dans le secteur financier[17].

III. Le respect des règles européennes de protection des données

10. Les règles européennes de protection des données occupent une place cardinale dans le régime européen de protection des lanceurs d'alerte[18]. Certaines des exigences mentionnées ci-dessus découlent d'ailleurs en partie du respect de ces règles. On songe aux exigences de confidentialité et de transparence. En particulier, l'article 17 de la directive rappelle que les traitements de données à caractère personnel effectués en vertu de la directive doivent être effectués conformément au RGPD et à la directive « Police & Justice »[19]. Tout échange ou toute transmission d'informations par les institutions, organes ou organismes de l'Union s'effectue conformément au règlement (UE) 2018/1725[20].

Conformément à son rôle d'assistance vis-à-vis du responsable de traitement, le DPO devra à tout le moins dans ce cadre :

- veiller au respect des exigences de transparence imposées tant par le RGPD que par la directive sur les lanceurs d'alerte, notamment par la construction d'une page Internet spécialement dédiée sur le site de l'entité et des campagnes de sensibilisation au sein de l'entité ;
- veiller au respect de l'obligation d'information des personnes concernées (auteur(s) du signalement ou personnes visées par le signalement) par les traitements de données réalisés dans le cadre du dispositif d'alerte, notamment par le biais de la mise à jour de la politique de protection des données à l'égard des travailleurs et des tiers, ainsi que via l'adaptation du registre des activités de traitement ;
- veiller à ce que les procédures mises en place respectent les principes généraux du RGPD (par exemple, en limitant le dispositif aux signalements des actes ou omissions couverts par la loi de transposition, étant entendu que tout signalement doit à tout le moins poursuivre une finalité déterminée, explicite et légitime) et veiller au respect par l'entité du principe d'*accountability* (notamment par le biais d'une documentation appropriée) ;
- aider l'entité à tenir à jour un registre des signalements aux fins notamment de pouvoir répondre aux demandes des personnes concernées quant à leurs droits reconnus en vertu du Chapitre III du RGPD, en particulier le droit d'information et le droit d'accès, dans le respect des obligations d'archivage ;
- lorsque le signalement concerne une fuite de données, rendre un avis à l'entité relatif à la nécessité de notifier la violation à l'APD (et le cas échéant aux personnes concernées en cas de risque élevé pour leurs droits et libertés).

Bien que livrées sous l'empire de l'ancienne directive « vie privée », les orientations fournies par les autorités de contrôle en la matière conservent aujourd'hui toute leur pertinence[21]. Elles permettent de mieux comprendre comment les principes de base applicables aux traitements de données – licéité, loyauté, transparence, finalité, proportionnalité, sécurité, droits de la personne concernée et *accountability* – doivent s'appliquer aux traitements effectués dans le cadre de

[15] Considérant n° 82 de la directive.

[16] Art. 5, § 1er, point f), du RGPD. Cela signifie, par exemple, que les responsables de traitement doivent mettre en place une politique stricte de contrôle des accès (limitation des personnes pouvant accéder aux données, authentification fiable et journalisation des accès : fichiers de logs). Sur le principe d'intégrité et de confidentialité, voy. not. Fr. Dumortier, « Cybersécurité, vie privée, imputabilité, journalisation et log files », *D.C.C.R.*, 2019, n° 1, pp. 204-207.

[17] Voy. par exemple l'article 10 du règlement de l'Autorité des services et marchés financiers du 5 septembre 2017 précisant les règles de procédure applicables à la réception et au traitement des signalements d'infractions, approuvé par l'arrêté royal du 24 septembre 2017, *M.B.*, 28 septembre 2017.

[18] Voy. not. les considérants nos 14, 82 83, 84 et 85 et les articles 16 et 17 de la directive sur les lanceurs d'alerte. Voy. aussi l'article 32, § 2, point c), du règlement (UE) n° 596/2014 sur les abus de marché ainsi que les considérants nos 41 et 43 de la quatrième directive anti-blanchiment.

[19] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L 119, 4 mai 2016.

[20] Voy. aussi les considérants nos 83, 84 et 85 de la directive.

[21] Voy. spéc. G29, Avis 1/2006 du 1er février 2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, WP 117 ; CPVP, Recommandation n° 01/2006 du 29 novembre 2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *op. cit.*

dispositifs d'alerte[22]. L'application des principes de base aux dispositifs de signalement a été rappelée par l'autorité de protection des données dans un avis récent rendu à propos d'une proposition de loi émanant du PTB tendant à offrir un statut légal et une protection aux lanceurs d'alerte[23].

Ces *guidelines* peuvent également être appliquées, *mutatis mutandis*, à la dénonciation aux autorités de poursuite, soumise, quant à elle, à la directive « Police & Justice ». S'agissant des traitements de données effectués par les institutions, organes ou organismes de l'Union dans le cadre de dispositifs de signalement, il faut noter que le Contrôleur européen de la protection des données (CEPD) a publié des lignes directrices en juillet 2016, lesquelles ont été actualisées en décembre 2019[24]. De l'opinion du Contrôleur européen, ces lignes directrices constituent également « une source précieuse d'inspiration pour les autres organisations ou peuvent venir compléter les orientations fournies par les autorités nationales chargées de la protection des données ».

11. Dans la mesure où les traitements de données personnelles réalisés dans le cadre des dispositifs de signalement présentent assurément un risque élevé pour les droits et libertés des personnes concernées[25], il semblerait utile de faire précéder l'adoption de la loi de transposition d'une analyse générale d'impact relative à la protection des données. Dans un tel cas de figure, une analyse d'impact ne serait plus requise de la part des responsables de traitement, à moins de faire jouer l'article 35, § 10, du RGPD qui permet de l'imposer lorsque cela s'avère nécessaire. Une telle analyse pourrait ici s'avérer nécessaire, tant de la part des entités juridiques que des autorités compétentes. En tout état de cause, l'analyse devra avoir lieu en concertation avec le DPO[26].

IV. La désignation d'un gestionnaire de signalement (*Whistleblower Officer* – WBO)

12. La directive prévoit l'obligation de désigner une personne ou un service impartial compétent pour assurer le suivi des signalements[27]. Il peut s'agir de la même personne ou du même service que celle ou celui qui reçoit les signalements et qui maintiendra la communication avec l'auteur de signalement et, si nécessaire, lui demandera d'autres informations et lui fournira un retour d'informations. Dans le cas du signalement externe, les autorités compétentes doivent expressément désigner les membres du personnel chargés du traitement des signalements et des différentes tâches (information, réception et suivi, retour d'informations)[27]. Les membres du personnel désignés sur cette base doivent recevoir une formation spécifique aux fins du traitement des signalements[29], y compris en matière de règles de protection des données applicables[30].

Le choix de la personne ou du service le plus approprié pour assumer la fonction dépend de la structure de l'entité. La directive précise que « dans les plus petites entités, cette fonction pourrait être une double fonction assumée par un dirigeant d'entreprise bien placé pour rendre compte directement au chef de l'organisation. Il peut s'agir, par exemple, d'un responsable de la conformité ou des ressources humaines [*chief compliance or human resources officer*], d'un responsable de l'intégrité [*integrity officer*], d'un responsable juridique ou d'un responsable de la protection de la vie privée [*legal or privacy officer*], d'un directeur financier [*chief financial officer*], d'un responsable de l'audit interne [*chief audit executive*] ou d'un membre du conseil [*member of the board*]. »[31]

À première vue, on peut penser que la personne la plus appropriée pour recevoir des informations sur les violations relevant du domaine de la protection de la vie privée et des données à caractère personnel devrait être le DPO lorsque la désignation d'une telle personne est obligatoire.

13. Une telle situation est toutefois susceptible de faire naître un conflit d'intérêts alors que la directive attire l'attention sur la nécessité de garantir l'absence de conflits d'intérêts dans le chef de celui qui exerce la fonction de WBO[32]. Dans ses lignes directrices concernant les délégués à la protection des données, le Groupe de travail « Article 29 » souligne en effet qu'« en règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement »[33]. Dans une décision récente, la Chambre contentieuse de l'Autorité de protection des données a, par ailleurs, précisé que « le cumul, dans le chef d'une même personne physique, de la fonction de responsable de chacun des trois départements en question [*compliance, risk management* et audit interne] distinctement d'une part et de la fonction de délégué à la protection des données d'autre part prive chacun de ces trois départements de toute possibilité de contrôle indépendant par le délégué à la protection des données »[34].

[22] Pour une analyse de la conformité des dispositifs de *whistleblowing* au regard du RGPD, voy. not. A. Lachapelle, « Le lancement d'alerte (*whistleblowing*) à l'ère du règlement général sur la protection des données », in C. De Terwangne et K. Rosier (dir.), *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Bruxelles, Larcier, 2018, pp. 797-836. Voy. aussi A. Lachapelle, « Whistleblowing: Threat or Safeguard for Data Protection in the Digital Era? », *in* J. Herveg (dir.), *Deep diving into data protection. 1979-2019: celebrating 40 years of research on privacy data protection at the CRIDS*, Bruxelles, Larcier, 2021, pp. 129-148.

[23] Avis n° 128/2021 du 28 juillet 2021.

[24] European Data Protection Supervisor (EDPS), *Guidelines on processing personal information within a whistleblowing procedure*, décembre 2019.

[25] Délibération n° 2019-139 du 18 juillet 2019 portant adoption d'un référentiel [par la CNIL] relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles, *J.O.R.F.*, 10 décembre 2019, p. 3.

[26] Art. 35, § 2, du RGPD.

[27] Art. 9, § 1er, point c), de la directive.

[28] Art. 12, § 4, de la directive.

[29] Art. 12, § 5, de la directive.

[30] Considérant n° 74 de la directive.

[31] Considérant n° 56 de la directive.

[32] Considérant n° 56 de la directive.

[33] G29, Lignes directrices concernant les délégués à la protection des données (DPD), 13 décembre 2016, version révisée et adoptée le 5 avril 2017, WP 243 rev.01, p. 19.

[34] Chambre contentieuse (APD), Décision quant au fond 18/2020 du 28 avril 2020 ayant pour objet le rapport d'inspection relatif à la responsabilité des fuites de données et la position du délégué à la protection des données (AH-2019-0013), p. 17.

Dans la mesure où le WBO participe à la détermination des finalités et des moyens des traitements de données à caractère personnel réalisés dans le cadre du système d'alerte de l'entité au sein de laquelle il exerce ses fonctions, il faut donc en déduire qu'une même personne physique ne peut exercer dans le même temps la fonction de WBO et celle de DPO[35]. Le risque de conflit d'intérêts semble, en revanche, levé lorsque la fonction de WBO est exercée par un département. Ceci étant, un potentiel conflit d'intérêts pourrait encore surgir dans l'hypothèse où, par exemple, le département WBO/DPO serait informé de pratiques contraires au RGPD au sein de l'entité ou du non-respect de certaines obligations (absence de notification en cas de fuite de données par exemple) sachant que le DPO a pour mission de veiller à la conformité au RGPD des activités de traitement de l'entité. Dans un tel cas de figure, le lanceur d'alerte aurait tout intérêt à porter son signalement directement en dehors de l'entité, auprès de l'autorité de protection des données (signalement externe). Une telle solution semble, quoi qu'il en soit, privilégiée au vu de l'étendue du champ d'application matériel de la directive – qui va bien au-delà de la protection des données. Ce département devra, le cas échéant, travailler en étroite collaboration avec le DPO, le *Compliance Officer*, l'AML *Compliance Officer*, l'auditeur interne et le Responsable de la Sécurité des Systèmes d'Information (RSSI).

14. Il n'empêche qu'une telle solution suppose de disposer de ressources suffisantes en interne, ce qui est rarement le cas des « petites entités » pour lesquelles la directive semble autoriser l'exercice conjoint des fonctions de DPO et de WBO. Une solution moins coûteuse que la création d'un département exprès et moins risquée en termes de conflits d'intérêts serait d'externaliser la fonction de WBO vers des tiers, qui seraient alors autorisés à recevoir des signalements de violations pour le compte d'entités juridiques des secteurs privé et public[36]. Dans ce cas, la directive précise que les tiers sélectionnés doivent offrir « des garanties appropriées de respect de l'indépendance, de la confidentialité, de la protection des données et du secret »[37]. Elle mentionne, en outre, que le signalement pourrait être confié à des fournisseurs de plateformes de signalement, des conseils externes, des auditeurs, des représentants syndicaux ou des représentants des travailleurs. En pratique, on peut néanmoins douter qu'un conseiller externe offre les qualités attendues en termes de disponibilité et d'écoute. Eu égard à notre tradition juridique, la place des représentants syndicaux et des représentants des travailleurs mérite clairement d'être étudiée, sans occulter le risque patent d'une bipolarisation employeur/employé[38].

Conclusion

15. Largement passée inaperçue, la directive sur les lanceurs d'alerte mérite plus que jamais l'attention des DPO. Alors qu'une loi de transposition devrait être adoptée d'ici la fin de l'année civile, les DPO devraient d'ores et déjà accompagner les entreprises et les administrations soucieuses de se mettre en conformité en mettant en place des canaux et des procédures de signalement. Le DPO doit être associé du début à la fin du processus. En effet, la légitimité et l'efficacité des dispositifs d'alerte dépend en partie du respect des règles européennes de protection des données. L'exigence de confidentialité occupe, à cet égard, une place essentielle. En pratique, celle-ci ne pourra être pleinement respectée qu'à la condition de prendre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. La tâche n'est pas simple tandis que les cyberattaques se multiplient à mesure que le numérique gagne du terrain dans notre cercle privé, social et professionnel. Si certains en doutaient encore, la résilience des réseaux et systèmes d'information est devenue une préoccupation majeure de laquelle dépend la réussite d'un grand nombre de politiques et de réglementations, parmi lesquelles figure assurément la directive sur les lanceurs d'alerte.

■ *Amélie Lachapelle*

Chargée d'enseignement à l'UNamur
Responsable de la cellule CSS
(Criminalité, Sécurité et Surveillance
à l'ère numérique) – CRIDS/NaDI
Coordinatrice pédagogique du baccalauréat
en droit à horaire décalé à l'UNamur

[35] Voy. A. Lachapelle, « Data Protection Enforcement in the Era of the Directive on whistleblowers: towards a collective approach? », *in* E. Kosta et R. Leenes (éd.), *Research handbook on EU data protection*, Cheltenham, Edward Elgar Publishing, 2021, à paraître.

[36] Le fournisseur de services doit offrir les mêmes garanties que le gestionnaire de signalements lui-même, notamment en termes de compétence, de confidentialité, de sécurité et d'indépendance. Il doit aussi s'engager contractuellement au respect des principes relatifs à la protection des données, et en particulier des obligations de confidentialité et de sécurité. Voy. not. A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale : de la complaisance à la vigilance*, Bruxelles, Larcier, 2021, n° 1210.

[37] Considérant n° 54 de la directive.

[38] Sur le rôle que pourraient jouer les syndicats dans le déploiement de dispositifs d'alerte, voy. spéc. A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale : de la complaisance à la vigilance*, *op. cit.*, 2021, n^{os} 697 et 876.

DPO news DROIT, TECHNOLOGIE ET MANAGEMENT

ABONNEMENT

ANTHEMIS, Place Albert I, 9 à 1300 Limal
Tél. 010/42.02.90 - Fax. 010/40.21.84
abonnement@anthemis.be - www.anthemis.be
Éditeurs responsables : Marc-Olivier Lifrange et Elisabeth Courtens
Secrétariat de rédaction : Justine Minot
justine.minot@anthemis.be
Maquette et mise en page par Matthieu Lepoutre
© 2021 Anthemis s.a. ISSN : 2593-7979

5 numéros par an

Abonnement
- annuel papier et électronique* : 167 € HTVA (port inclus pour la Belgique),
- annuel électronique* : 133 € HTVA

Les abonnements sont renouvelés automatiquement, sauf résiliation expresse avant l'échéance.

** Les codes d'accès au site sont communiqués par mail à l'abonné.*
Important : une adresse mail, un nom et un prénom doivent nous être fournis à cette fin.

ANTHEMIS