Au-delà du RGPD - les exigences et attentes de la CNPD concernant la fonction de DPO

Le délégué à la protection des données, communément surnommé «DPO» pour Data protection officer, est un acteur clé du respect des dispositions légales et réglementaires sur la protection des données à caractère personnel.

La nomination d'un DPO au sein d'une organisation, que celle-ci agisse comme responsable du traitement de données ou sous-traitant, est obligatoire dans certains cas (comme pour les organisations traitant des données sensibles à grande échelle ou encore les autorités ou organismes publics n'étant pas des juridictions) et facultative dans les autres cas.

Le Règlement (UE) 2016/679, dit «Règlement général sur la protection des données» ou «RGPD», encadre les fonctions et les missions du DPO. Des lignes directrices du groupe de travail de l'article 29[1] (l'organe européen traitant des questions de vie privée, ancêtre du Comité européen sur la protection des données) viennent préciser et compléter les dispositions du RGPD afin de faire reposer le rôle du DPO sur un socle commun de règles et de guidance à suivre par les organisations européennes et non-européennes soumises au règlement.

Pressentant la nature critique qu'allait avoir le DPO, la Commission nationale pour la protection des données («CNPD»), le régulateur luxembourgeois de la protection des données, a lancé en 2018 une campagne thématique sur la fonction de DPO. Vingt-cinq procédures d'audit «proactives» ont alors été ouvertes à l'encontre d'organisations d'une certaine importance, évaluée en termes de taille, de sensibilité de données traitées et de secteur d'activité. Les organisations visées opéraient tant dans le secteur privé (banques et autres sociétés du secteur financier, assureurs, sociétés commerciales, etc.) que dans le secteur public (administrations, établissements publics, etc.).

Trois ans après l'ouverture des procédures, la CNPD a publié sur son site internet dix-sept décisions issues de la campagne d'audits[2]. Sept d'entre elles ont débouché sur des mesures correctrices, l'amende maximale s'élevant à 18.000 euros. Ces décisions nous permettent de comprendre l'approche en onze «objectifs de contrôle» adoptée par le régulateur (et susceptible d'être suivie dans de futurs audits) ainsi que les exigences ou attentes locales qui dépassent ou qui concrétisent les règles et recommandations européennes. Dans cet article, nous nous concentrerons uniquement sur ces exigences et ces attentes sans détailler les dispositions du RGPD et les lignes directrices européennes pertinentes dont il faut évidemment tenir compte dans chaque analyse de la fonction de DPO au sein d'une organisation.

1) La CNPD s'assure que l'organisme soumis à l'obligation de désigner un DPO l'a bien fait

Lorsqu'une organisation n'est pas dans l'obligation de désigner un DPO en application des critères légaux de l'article 37 du RGPD, tels que ces derniers sont précisés par les lignes directrices européennes précitées sur le DPO, une désignation volontaire d'un DPO et sa notification à la CNPD entraîneront l'application des dispositions légales liées cette fonction. Dans ces cas toutefois, il semble découler d'une décision publiée[3] que les attentes de la CNPD dans la mise en œuvre des conditions liées au rôle de DPO pourraient être moindres lorsque les activités de l'organisation ne présentent pas de risques en termes de traitements de données personnelles (pour des activités d'entretien et de nettoyage par exemple). Cette approche paraît parfaitement fondée au vu de la logique du RGPD centrée autour de la proportionnalité et de la balance des risques.

2) et 3) La CNPD s'assure que l'organisation a publié les coordonnées de son DPO et qu'elle a communiqué ces coordonnées à la CNPD

Ces deux objectifs de contrôle n'appellent pas de développement particulier et découlent directement de l'article 37, paragraphe 7 du RGPD. L'obligation de communiquer les coordonnées du DPO à l'autorité de contrôle est inscrite dans le RGPD. A cet effet, la CNPD a mis en place un formulaire accessible sur son site internet[4].

4) La CNPD s'assure que le DPO dispose d'une expertise et de compétences suffisantes pour s'acquitter efficacement de ses missions

L'article 37, paragraphe 5 du RGPD requiert que le DPO doit avoir des compétences professionnelles suffisantes. Maintenant il est devenu clair à travers de sa pratique décisionnelle que la CNPD s'attend à ce que le DPO ait au minimum **trois années d'expérience professionnelle en matière de protection des données**, les formations et conférences suivies par la personne nommée DPO ne pouvant suffire à combler une quelconque carence à ce titre[5].

5) La CNPD s'assure que les missions et les tâches du DPO n'entraînent pas de conflit d'intérêts

En vertu de l'article 38, paragraphe 6 du RGPD, les autres missions et tâches d'un DPO ne peuvent pas entraîner de conflit d'intérêts. Dans sa pratique décisionnelle la CNPD précise qu'elle s'attend à ce que l'organisation contrôlée ait réalisé une analyse quant à l'existence d'un éventuel conflit d'intérêts. La CNPD liste à ce titre une série de bonnes pratiques à adopter (comme celle d'établir des règles internes visant à éviter des conflits d'intérêts) en fonction des activités, de la taille et la structure de l'organisation[6].

Dans certaines décisions, la CNPD reprend les exemples d'incompatibilité avec les fonctions du DPO énumérées sur la page du site web de l'autorité consacrée au DPO (et notamment avec les fonctions de ***CEO***, ***COO***, ***CIO***, ***CFO***, ***HRD***, etc.)[7].

Dans un cas particulier, le régulateur a estimé que les fonctions de DPO et de ***Chief Compliance Officer*** **(CCO)** ne pouvaient être combinées en raison du risque de conflit d'intérêts. Afin d'écarter ce risque, il aurait fallu établir que la personne ne participait pas à la détermination des finalités et des moyens des traitements de données mis en œuvre dans le cadre des activités opérationnelles AML/KYC[8], preuve qui n'était pas rapportée en l'espèce selon la CNPD.

6) La CNPD s'assure que le DPO dispose de ressources suffisantes pour s'acquitter efficacement de ses missions

Pour les organisations d'une certaine taille (sans que la CNPD ne donne des critères précis à cet égard), la CNPD s'attend à **au moins un employé ETP (équivalent temps plein)** pour l'équipe en charge de la protection des données[9].

7) La CNPD s'assure que le DPO est en mesure d'exercer ses missions avec un degré suffisant d'autonomie au sein de son organisation

En vertu de l'article 38, paragraphe 3 du RGPD, le DPO ne peut pas recevoir des instructions quant à l'accomplissement de ses missions et fait directement rapport au niveau le plus élevé de la direction. Lorsque l'organisation traite un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé, la CNPD s'attend à ce que le **DPO soit rattaché au plus haut niveau de la direction de l'organisation** afin de garantir au maximum son autonomie[10]. L'existence effective de discussions et de réunions informelles avec la direction ne permettrait, selon la CNPD, pas d'établir à elle seule le rapport direct du DPO au niveau le plus élevé de la direction. La CNPD semble toutefois laisser la porte ouverte à un système où le DPO, sans être rattaché au plus haut niveau de la direction, pourrait utiliser des mesures (pourvu qu'elles soient documentées) permettant de contourner les niveaux hiérarchiques intermédiaires dès qu'il/elle l'estime nécessaire.

8) La CNPD s'assure que l'organisation a mis en place des mesures pour que le DPO soit associé à toutes les questions relatives à la protection des données

Lorsque l'organisation traite un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé, la CNPD considère[11] que la **participation formalisée et systématique du DPO aux réunions pertinentes** est utile pour prouver que le DPO est associé à toutes les questions relatives à la protection des données, comme le requiert l'article 38, paragraphe 1er du RGPD. Les «réunions pertinentes» seraient celles des comités jugés utiles ou pertinents au regard de la protection des données. Suivant les organisations, il pourrait s'agir des comités de direction, de coordination de projets, de nouveaux produits et/ou des comités sécurité. La CNPD a également fait connaître ses attentes concrètes dans un cas où une organisation avait nommé un DPO au niveau du groupe de sociétés pour couvrir les besoins en conformité RGPD de ce groupe y compris de son l'entité luxembourgeoise[12].

9) La CNPD s'assure que le DPO remplit sa mission d'information et de conseil auprès du responsable du traitement et des employés

Un ***reporting*** **formel** des activités du DPO auprès de la direction, sur base d'une fréquence définie est, selon la CNPD[13], une mesure utile pour prouver l'accomplissement de la mission d'information du DPO envers le responsable du traitement en vertu l'article 39, paragraphe 1er, point a) du RGPD, surtout lorsque le responsable traite un nombre substantiel de données dont le degré de sensibilité peut être élevé.

10) La CNPD s'assure que le DPO exerce un contrôle adéquat du traitement des données au sein de son organisation

Dans une décision impliquant des traitements de données touchant potentiellement un nombre important d'individus[14], la CNPD a exigé un certain formalisme du contrôle effectivement mené par le DPO. Etablir un **«plan de contrôle en matière de protection des données»** peut servir à satisfaire cette exigence qui découle de l'article 39, paragraphe 1er, point b) du RGPD en vertu duquel une des missions principales du DPO est de «contrôler le respect» du RGPD.

11) La CNPD s'assure que le DPO assiste le responsable du traitement dans la réalisation des analyses d'impact en cas de nouveaux traitements de données

Les décisions publiées par la CNPD n'ont pas traité cet objectif de contrôle qui découle de l'article 39, paragraphe 1er, point c) du RGPD et est aussi lié à celui, plus global, d'associer le DPO aux questions relatives à la protection des données.

Conclusion

Il convient de souligner que certaines décisions de la CNPD sont encore susceptibles de recours par les organisations sanctionnées et que, par conséquent, certains ajustements des attentes et exigences du régulateur ne peuvent être exclus. Nous constatons que de nombreuses exigences de la CNPD décrites ci-dessus ont été appliquées à des organisations traitant «*un nombre substantiel de données dont le degré de sensibilité peut être relativement élevé*» (selon l'expression utilisée par le régulateur). Comme des organisations obligées de nommer un DPO cocheront souvent cette case, il semble prudent de partir du principe que ces exigences locales s'appliqueront à ces organisations, même si certaines d'entre elles peuvent sembler aller (trop) loin pour les organisations concernées.

Enfin, il y a lieu de noter que la nécessité pour les organisations de documenter, les décisions prises, les analyses menées ou les *process* mis en place en lien avec le DPO, revient constamment dans les décisions de la CNPD. Le manque de documentation est d'ailleurs dans plusieurs décisions une raison de sanctionner alors même que, dans les faits, les conditions légales (liées au *reporting* du DPO à la direction ou autres) paraissaient effectivement remplies. Ainsi, il ne peut qu'être recommandé de mettre sur papier et de tenir à jour les décisions et actions principales liées à la fonction de DPO et de pouvoir aisément identifier et présenter ces documents en cas d'audit de la CNPD.

Vincent WELLENS (picture),
barreaux de Luxembourg et de Bruxelles,
IP & Technology Law Partner, NautaDutilh

Lindsay KORYTKO,
barreau de Luxembourg IP & Technology Law Partner, NautaDutilh

avec l'aide de Maxime DUFOUR, stagiaire NautaDutilh

1) Lignes directrices concernant les délégués à la protection des données (DPD). Adoptées le 5 avril 2017 (WP 243 rev.01) Accessible sur https://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf
2) https://cnpd.public.lu/fr/decisions-sanctions.html
3) Délibération n° 25FR/2021 du 1 er juillet 2021.
4) Accessible via https://cnpd.public.lu/fr/actualites/national/2018/05/formulaire-declaration-dpo.html
5) Délibération n° 10FR/2021 du 26 mars 2021 et Délibération n° 23FR/2021 du 29 juin 2021.
6) Délibération N° 19FR/2021 du 31 mai 2021 (p. 5).
7) https://cnpd.public.lu/fr/professionnels/dpo.html
8) Délibération N° 19FR/2021 du 31 mai 2021.
9) Délibération N° 18FR/2021 du 31 mai 2021 et Délibération n° 30FR/2021 du 4 août 2021.
10) Délibération n° 23FR/2021 du 29 juin 2021.
11) Délibération n° 23FR/2021 du 29 juin 2021 et Délibération n° 20FR/2021 du 11 juin 2021.
12) Délibération n° 18FR/2021 du 31 mai 2021. Pour une analyse de cette décision, nous vous renvoyons à notre newsletter disponible via https://www.e-nautadutilh.com/95/4486/landing-pages/the-cnpd-publishes-several-decisions-following-investigations.asp?sid=blankform
13) Délibération n° 29FR/2021 du 4 août 2021.
14) Délibération n° 30FR/2021 du 4 août 2021.

Acronis Cyberthreats Report

Les cybercriminels se recentrent sur les PME

Malgré la perception qu'elles seraient trop petites pour être visées, les PME sont de plus en plus vulnérables du fait d'attaques de type «supply-chain» et du recours à l'automatisation de ceux qui diffusent des ransomwares. Acronis, le leader mondial de la cyberprotection, publie son nouveau rapport de milieu d'année 2021 Acronis Cyberthreats Report, qui fait le point sur les cybermenaces. Ce rapport prévient que les PME sont particulièrement exposées aux attaques constatées pendant le premier semestre.

En effet, durant ce semestre, 4 entreprises sur 5 ont expérimenté une compromission de cybersécurité due à une vulnérabilité touchant l'écosystème de leurs fournisseurs tiers. Le coût moyen d'une compromission de données a alors atteint 3,56 millions de dollars et le versement moyen en cas d'attaque de ransomware a progressé de 33% pour dépasser les 100.000 dollars. Si ces montants sont lourds pour n'importe quelle entreprise, ils risquent de sonner le glas de la plupart des PME, ce qu'Acronis craint pour le second semestre 2021.

«Si l'intensification des attaques vaut pour les entreprises de toute taille, on tend à négliger l'impact sur les plus petites entreprises», explique Candid Wüest, vice-président de Cyber Protection Research chez Acronis. «Contrairement aux grands groupes, les PME n'ont pas l'argent, les ressources ni les experts en interne pour contrer les menaces actuelles. C'est pourquoi elles se tournent vers des fournisseurs de services IT, mais il suffit que ceux-ci soient compromis pour que les PME se retrouvent à la merci des cybercriminels.»

Les attaques de la chaîne d'approvisionnement des fournisseurs de services managés (MSP) permettent d'avoir accès aux opérations des MSP et à l'ensemble de leurs clients. Comme nous l'avons vu avec la compromission SolarWinds l'an dernier et l'attaque Kaseya VSA plus tôt en 2021, une attaque qui aboutit peut compromettre des centaines ou des milliers de PME. Candid Wüest a expliqué, lors de l'événement Black Hat 2021 aux États-Unis, en quoi les attaques de type «supply-chain» contre les fournisseurs de services IT sont une menace pour les PME, dans une session intitulée Ransomware Attacks Against MSPs – A Nightmare for SMBs.

Zoom sur les résultats du rapport

Outre les attaques d'envergure qui ont fait la une ces six derniers mois et les préoccupations d'Acronis concernant l'impact sur les MSP et les petites entreprises, l'édition du 1er semestre 2021 d'Acronis Cyberthreats Report souligne que :
- **Les attaques de phishing foisonnent**. Les e-mails de phishing qui procèdent de techniques d'ingénierie sociale pour amener les utilisateurs à cliquer sur des liens ou des pièces jointes infectés ont progressé de 62% entre le 1er et le 2nd trimestre. Cette progression est inquiétante étant donné que 94% des malwares sont transmis par e-mail. Pendant la même période, Acronis a bloqué plus de 393.000 URL de phishing et malveillantes visant ses clients, empêchant ainsi les cybercriminels d'avoir accès à des données sensibles et d'injecter des malwares dans le système de clients.
- **L'exfiltration des données se poursuit**. En 2020, plus de 1.300 victimes de ransomwares ont déploré la divulgation publique de données suite à une attaque, dans une tentative de monétisation des cybercriminels. Pendant le premier semestre 2021, plus de 1.100 fuites de données ont donné lieu à divulgation, soit une augmentation de 70% cette année.
- **Les télétravailleurs demeurent une cible privilégiée**. Du fait de la généralisation du télétravail en raison de la pandémie de COVID-19, deux tiers des télétravailleurs utilisent leurs équipements professionnels pour leurs activités personnelles et leurs appareils personnels pour leurs activités professionnelles. Ceux-ci sont donc particulièrement visés et Acronis a observé le doublement des cyberattaques, avec une augmentation de 300% des attaques par force brute contre des machines distantes via RDP.

Le rapport Acronis Cyberthreats Report Mid-year 2021 peut être téléchargé sur https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Protect-Cyberthreats-Report-Mid-year-2021-EN-US.pdf