n°60
[Novembre - Décembre 2017]

www.expertsdelentreprise.com

Le Journal du Management
juridique et réglementaire

Interview de Béatrice Oeuvrard Juriste senior de Microsoft France 3

Nominations 43

EXPERTS DE L'ENTREPRISE

Formations 62

Agenda Juridique — Formations, Conférences, Congrès, Réseaux

DOSSIER 4

DROIT DE L'INFORMATIQUE / NTIC

15ÈME JOURNÉE DE LA PROPRIÉTÉ INTELLECTUELLE ET NUMÉRIQUE 37

INCLUS
- Programme
- Présentation des conférences

LE 2ÈME VILLAGE DE LA LEGALTECH 45

INCLUS
- Programme des ateliers et conférences
- Les 36 exposants

RECOUVREMENT 59

Le recouvrement de créances en Bulgarie

legitéam Editions

QUATRE BONNES RAISONS DE DÉSIGNER UN *DATA PROTECTION OFFICER* EXTERNE

L'application du règlement européen sur la protection des données à caractère personnel (RGPD) prévue le 28 mai 2018 se rapproche à grands pas[1].
Pour autant, le choix de son Data protection *officer* (DPO) ne doit pas être précipité. Car celui-ci aura le rôle déterminant de poser les fondements de l'organisation nouvelle de l'entreprise, qu'il concevra au regard des nouvelles exigences réglementaires.
Ainsi, plus la désignation du DPO sera pertinente, moins le responsable de traitement et le sous-traitant -soit le plus souvent des entreprises- seront exposés aux risques de sanctions particulièrement dissuasives prévues par le RGPD.

En effet, en cas de violation de ses dispositions, le RGPD prévoit un éventail de sanctions de nature administrative, pénale, et civile. La Commission Nationale de l'Informatique et des Libertés (CNIL) aura le pouvoir de prononcer des amendes administratives dont le montant peut s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial de l'entreprise concernée. Elle aura également et notamment la possibilité d'épingler les entreprises, en leur adressant un avertissement public.[2] L'entreprise défaillante devra également répondre civilement des dommages matériels ou moraux causés par la violation du règlement.[3] Enfin, les sanctions pénales seront déterminées par le droit interne.[4]
Dans ces conditions, le responsable de traitement et le sous-traitant devront apporter un soin particulier à la nomination de leur DPO.

Même si cette désignation n'est expressément rendue obligatoire que dans les cas où le traitement de données revêt une certaine ampleur (« à grande échelle »), où la nature des opérations implique un « suivi régulier et systématique », et où les traitements portent sur des données sensibles ou sur des données relatives à des infractions et condamnations pénales, la présence d'un DPO est en toute hypothèse,

Emmanuel Daoud

Flora Plénacoste

vivement encouragée par les membres du G29 ainsi que par la CNIL.[5]

Néanmoins, et malgré la responsabilité importante que le DPO devra assumer (pour résumer : assurer la conformité des pratiques de l'entreprise avec la réglementation applicable en matière de données personnelles), le RGPD contient peu d'informations sur les critères que celui-ci devra satisfaire.
Ainsi, le responsable de traitement peut, de manière indifférente, le désigner parmi le personnel ou choisir un prestataire sur la base d'un contrat de services.[6]

Toutefois, dans la dynamique de mise en conformité qui est la nôtre, nous recommandons clairement la désignation d'un DPO externe à l'entreprise, pour les quatre raisons suivantes.

1. LES DPO EXTERNES : UN CONCENTRÉ DES COMPÉTENCES REQUISES

Le DPO compétent, un oiseau rare en interne

Le RGPD prévoit que le DPO doit être choisi sur la base de « ses qualités professionnelles », en particulier, « de ses connaissances spécialisées du droit et des pratiques en matière de protection des données » ainsi que sur sa « capacité à accomplir les missions ».[7]
Pour résumer, ses missions consisteront à informer, sensibiliser, former, conseiller et contrôler le respect des obligations prévues par le RGPD en menant notamment des audits. Le DPO fera également office d'interlocuteur avec la CNIL. Le DPO devra donc être particulièrement, voire extraordinairement, polyvalent. Il devra comprendre les enjeux juridiques, informatiques, commerciaux et marketing, et être doté d'un sens de la communication, de la médiation, de la diplomatie, et de la pédagogie. Aucun agrément ou diplôme précis n'est exigé. Le groupe de l'article 29 privilégie toutefois une connaissance approfondie de la réglementation.[8]
Autrement dit, les entreprises doivent se mettre en quête d'un oiseau rare.

De fait, en interne, le choix se portera le plus souvent sur une personne issue de la filière juridique, ou informatique (le RSSI par exemple), ce qui n'apparaît pas entièrement satisfaisant au regard des différentes qualités requises. Envisager une formation complémentaire n'est pas une solution, car les offres adéquates et complètes sont encore balbutiantes.

Les cabinets d'avocats sont en capacité de proposer un service conçu « sur mesure »

L'option de désigner un prestataire en qualité de DPO présente sur ce point de nombreux avantages. En effet, certains

1 - *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) (Texte présentant de l'intérêt pour l'EEE)*
2 - *RGPD, cons. 150.*
3 - *RGPD, art. 82*
4 - *RGPD, cons. 149*
5 - *RGPD, art. 37*
6 - *RGPD, art. 37.6*
7 - *RGPD, art. 37.5*
8 - *Article 29 Working Party, Guidelines on Data Protection Officers (DPO), 13 December 2016, WP 243, p. 11 et 14*

d'entre eux, en particulier les cabinets d'avocats, créent des « boutiques » spécialisées mettant à disposition des équipes conçues sur mesure, mêlant des compétences diverses qui répondent exactement aux exigences du métier. Ces groupements forment une synergie de connaissances et de compétences avec laquelle les équipes internes ne pourront que difficilement rivaliser d'ici l'entrée en application du RGPD.

2. L'EXTERNALISATION DU DPO : UNE CONDITION *SINE QUA NON* DE SON INDÉPENDANCE, ET DONC DE SON EFFICACITÉ

Le conflit inexorable entre l'exigence d'indépendance du DPO et une désignation en interne

Le DPO doit pouvoir exercer ses fonctions et missions « en toute indépendance »[9].
A ce titre, le DPO ne doit recevoir « aucune instruction en ce qui concerne l'exercice des missions »[10]
Cependant, en pratique, l'on conçoit mal comment un salarié, dépendant économiquement de la société qui l'emploie, soumis à un lien de subordination à l'égard de sa hiérarchie, pourrait jouir d'une telle indépendance vis-à-vis de sa direction. Le rapport Braibant au Premier ministre mettait déjà en évidence cette contradiction[11].

La difficulté paraît plus nette encore lorsqu'on s'aperçoit que le RGPD donne au DPO interne la possibilité d'exécuter d'autres missions et tâches, à la seule condition qu'elles « n'entraînent pas de conflit d'intérêts »[12]. En d'autres termes, le DPO peut cumuler d'autres fonctions dans l'entreprise, à condition que celles-ci ne le conduisent pas à déterminer les finalités et les moyens d'un traitement de données, ce qui le placerait en position de « juge et partie ».
En pratique, le risque de conflit d'intérêts est prégnant, voire évident, pour les DPO internes exerçant à mi-temps en tant que responsable du service informatique par exemple.

Ces situations schizophréniques engendrent un conflit d'intérêts difficilement surmontable, ayant pour effet d'empêcher le DPO de mener à bien ses missions correctement et par conséquent d'exposer l'entreprise qui l'a désigné aux risques de sanctions prévues par le RGPD.

Le pendant de l'indépendance est une gestion effective des risques

Certes, le RGPD prévoit que le DPO « ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions », ce qui peut être interprété comme la volonté de protection de celui-ci[13]. Cependant cette impunité semble bien théorique. Car en pratique, un DPO qui cumulerait une autre fonction pourrait toujours se voir sanctionner en sa seconde qualité. Ces sanctions pourraient donc être prononcées sans entrave significative, puisque le DPO ne bénéficie pas du statut de salarié protégé.

L'efficacité du travail du DPO semble ainsi être conditionnée par la désignation d'un prestataire externe.
Le principe étant celui de l'indépendance du DPO, l'avocat est un candidat tout désigné. L'indépendance est en effet inscrite dans le serment de l'avocat, et constitue par conséquent son ADN dans sa pratique quotidienne.[14][15]

Certes, cette désignation externe implique que le DPO ne soit pas présent dans les locaux, ce qui demande une certaine rigueur en termes d'organisation et de gestion, en particulier pour les entreprises de grande taille. La CNIL préconise dans ce cas d'organiser la relation de manière opérationnelle en formalisant des circuits de transmission d'informations, en désignant des points de contact privilégiés au sein de l'entreprise, en planifiant régulièrement des réunions. Cette difficulté n'en est donc pas une.

3. L'AVOCAT DPO, LA GARANTIE D'UN SECRET ET D'UNE CONFIDENTIALITÉ ABSOLUS

Si le DPO interne est bien soumis au secret professionnel ainsi qu'à une obligation de confidentialité, il n'est pas pour autant pas tenu à une interdiction de dénoncer le responsable de traitement auprès de la CNIL en cas de difficulté dans l'exercice de ses missions.[16]

Par contre, les règles déontologiques de l'avocat interdisent formellement à celui-ci de dénoncer son client à la CNIL. Il ne peut que mettre un terme à sa mission s'il estime ne pas pouvoir l'exercer correctement.[17]
Le secret professionnel de l'avocat est en effet d'ordre public. Il est général, absolu et illimité dans le temps.[18] Outre les sanctions disciplinaires, la violation de cette obligation est un délit, susceptible d'entraîner des sanctions pénales. [19]
Le responsable de traitement ou le sous-traitant pourra donc se sentir parfaitement libre de lui confier des dossiers sensibles.

4. EXTERNALISER LE DPO PERMET UNE MEILLEURE GESTION DES COÛTS

Enfin, en cas d'externalisation, le coût des prestations reste sous contrôle. L'intervention du prestataire peut être modulée en fonction de sa charge de travail. Ainsi, si la mise en conformité avec le RGPD impliquera dans un premier temps une disponibilité importante du DPO externe, ses interventions pourront ensuite être nettement diminuées dans le temps.

**

En définitive, les garanties déontologiques de l'avocat, sa flexibilité d'intervention, sa compétence juridique ainsi que sa faculté de s'entourer de personnes aux profils complémentaires, sont autant d'atouts qui doivent conduire les responsables de traitement et les sous-traitants à le désigner en qualité de DPO.

Emmanuel Daoud, avocat au barreau de Paris, cabinet Vigo, membre du réseau GESICA
Flora Plénacoste, avocate au barreau de Paris, cabinet Vigo, membre du réseau GESICA

Vigo CABINET D'AVOCATS

9 - RGPD, cons. 68
10 - RGPD, art. 38.3
11 - Braibant G., Rapport au Premier ministre sur la transposition en droit français de la directive n°95/46, mars 1998, Doc. Fr.
12 - RGPD, art. 38.6
13 - RGPD, art. 38.3
14 - RIN, art. 1.3
15 - RIN art. 6.1; Code pénal art. 226-13
16 - RGPD, art. 38.5
17 - RIN, art. 6.3.3
18 - RIN art.2.1
19 - RIN, art. 1.4