ORGANE DE CONTROLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DD200018		14 avril 2020

Concerne : avis d'office concernant le contenu de la fonction de délégué à la protection des données ou DPO[1]

L'Organe de contrôle de l'information policière (ci-après en abrégé 'COC' ou 'Organe de contrôle').

Vu la 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 (aussi dénommée directive police-justice ou *Law Enforcement Directive*, ci-après *LED*).

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (MB, 5 septembre 2018, abrégée ci-après 'LPD').

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

Vu la loi du 5 août 1992 sur la fonction de police (ci-après 'LFP').

Vu le rapport de Messieurs Frank Schuermans et Koen Gorissen, membres-conseillers de l'organe de contrôle.

Rend le 14 avril 2020 l'avis suivant, de sa propre initiative.

I. Généralités

[1] *Data Protection Officer.*

1. Il y a actuellement un certain manque de clarté et/ou le COC est confronté à des questions relatives au rôle exact du délégué à la protection des données (ci-après *DPO*) au sein des services de police (ci-après 'GPI'[2]). Est exposé ci-après le cadre légal, après quoi suivra un commentaire sur l'expertise du *DPO*, qui est ancré dans ce cadre légal. Ensuite, on se penchera davantage sur les missions du *DPO*, qui sont également établies par la loi.

2. La figure du *DPO* n'est pas nouvelle. Déjà au temps de l'ancienne Directive sur la vie privée 1995/46[3], il était admis que la désignation d'un *DPO* simplifiait le respect de la réglementation en matière de protection des données, ce qui, avec des instruments de justification comme l'analyse d'impact relative à la protection des données (*AIPD*[4]) et le fait d'effectuer ou de permettre des contrôles (internes), vaut d'autant plus dans l'application de la réglementation actuelle.

Le *DPO* n'est pas personnellement responsable en cas de non-respect des dispositions en matière de protection des données. Il s'agit du service de police concerné, en sa qualité de responsable du traitement ou de sous-traitant, qui doit assurer et pouvoir démontrer que le traitement a été effectué conformément aux dispositions respectives. Le respect des règles en matière de protection des données est donc toujours de la responsabilité du service de police lui-même et en particulier de sa direction.

La LPD, reconnaît que le délégué à la protection des données est une figure clé dans le nouveau système de gestion des données et établit les règles relatives à sa désignation, à sa position et à ses missions.

II. <u>Cadre légal</u>

3. Le Titre 2, chapitre 4, section 5 de la LPD[5] couvre le cadre légal pour le *DPO*. Ce dernier est désigné sur base de ses qualités professionnelles et, en particulier, de son expertise sur le plan de la législation, de sa pratique en matière de protection des données et de sa capacité à accomplir les tâches suivantes :

- informer et conseiller les services de police, les fonctionnaires de police et le personnel administratif qui traitent des données personnelles de leurs obligations relatives à la protection des données à caractère personnel ;
- contrôler le respect de la réglementation et des règles internes du responsable du traitement relatives à la protection des données personnelles, en ce compris l'attribution de responsabilités, la sensibilisation et la formation du personnel participant à des opérations de traitement et les audits à ce sujet;
- fournir des avis à la demande concernant l'analyse d'impact relative à la protection des données et veiller à ce qu'une telle analyse d'impact relative à la protection des données comporte au moins ce qui suit :
  1° une description générale des traitements envisagés;
  2° une appréciation des risques pour les droits et libertés des personnes concernées;

[2] Geïntegreerde Politie – Police Intégrée
[3] 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 (*JOCE281, 23 novembre 1995*).
[4] Data Protection Impact Assesment.
[5] Articles 63 à 65

3° les mesures envisagées pour limiter les risques (les mesures de précaution, les mesures de sécurisation et les mécanismes qui sont instaurés pour protéger les données à caractère personnel)

- coopérer avec l'Organe de contrôle en général; plus spécifiquement, le *DPO* fait office de point de contact vis-à-vis de l'Organe de contrôle sur les questions relatives au traitement des données et le *DPO* doit communiquer à propos de toute question dans ce cadre; mais la législation se réfère aussi spécifiquement au *DPO* comme point de contact à propos de la consultation préalable avant que les données à caractère personnel ne soient reprises dans un nouveau fichier lorsque la nature du traitement (nouvelles technologies, mécanismes ou procédures) ou l'analyse d'impact relative à la protection des données indiquent un risque élevé pour les droits et libertés des personnes concernées.

Les services de police ont ainsi une obligation de justification pour démontrer que le traitement des données répond au titre 2 de la LPD, dans le respect des droits et intérêts légitimes des personnes concernées et des autres intéressés.

III. Expertise, position et missions du DPO

1. Être en relation

4. Le niveau d'expertise du *DPO* doit être en relation à la sensibilité, à la complexité et à la quantité de données que le(s) service(s) dont il est le *DPO* traite(nt).

Ainsi, il faut, par exemple, faire une différence entre l'expertise et le support qu'on peut attendre d'un *DPO* d'une police locale, par rapport à l'expertise et au support qu'on peut attendre du *DPO* qui veille à l'application des traités de police, et plus spécifiquement de l'échange systématique et fréquent de données de police avec des pays tiers (en-dehors de l'UE).

2. Qualités professionnelles

5. Les qualités professionnelles dont doit disposer un *DPO* peuvent, conformément à la réglementation, être réparties en trois volets : (1) connaissance de la législation, (2) connaissance de la pratique et (3) la capacité à remplir les tâches prévues par la loi.

2.1. Connaissance de la législation

6. Disposer de l'expertise nécessaire sur le plan de la législation ne veut pas dire en soi que le *DPO* doit disposer d'un certain diplôme. Une formation régulière adaptée à travers une formation permanente ou une expérience professionnelle antérieure dont il découle clairement qu'il a une grande connaissance de la réglementation nationale ou européenne peut par exemple aussi indiquer une connaissance solide de la législation et de la réglementation sur la protection des données. Ici aussi 'apprendre toute sa vie' est une *condition sine qua non*.

2.2. Connaissance de la pratique

7. Pour pouvoir exercer correctement la fonction de *DPO* au sein d'un service de police, il est important d'avoir une connaissance des flux de données au sein de la structure et de l'organisation de la GPI et d'avoir une vision suffisante des activités de traitement, des

systèmes informatiques et des besoins en informations de la GPI sur le plan de la protection des données et de la sécurisation des données, évidemment orientée vers le service où celui-ci travaille.

Une connaissance pratique solide suppose aussi que le DPO ait quelques années d'expérience. Indiquer un nombre d'années demeure un exercice difficile et un peu arbitraire.

Une expérience minimale de 2 ans comme membre de la GPI est toutefois, pour le COC, une limite minimale recommandée.

2.3. Capacité à remplir les tâches prévues par la loi

8. La capacité à remplir les tâches qui font légalement partie des missions d'un *DPO* ne doit pas seulement se concevoir comme une référence aux capacités personnelles et aux connaissances, mais a aussi trait à la position du *DPO* au sein de l'organisation. L'indépendance de la fonction doit ce faisant être respectée, et donc, une relation d'autorité hiérarchique ne peut avoir d'influence sur le rôle qu'un collaborateur remplit comme *DPO* (cf. infra).

L'intégrité et une éthique professionnelle suffisante n'ont pas seulement un rôle important dans la relation entre le management et le *DPO*. Il s'agit aussi de caractéristiques importantes dans le chef du *DPO*: un collaborateur ayant quelques sanctions disciplinaires ou des évaluations négatives à son palmarès n'est pas la personne appropriée pour ce job.

9. Le *DPO* doit, de par son indépendance, avoir la possibilité de créer une culture et une conscience collective de protection des données au sein du service de police dans lequel il exerce sa fonction de *DPO*. Il ou elle doit avoir la possibilité d'implémenter (d'aider à implémenter) les éléments essentiels de la protection des données, comme les principes de traitement des données, les droits des personnes concernées (il peut s'agir des collaborateurs de police eux-mêmes, mais évidemment avant tout les citoyens), le registre des activités de traitement, le signalement d'une communication à propos d'infractions relatives aux données personnelles, etc …

3. Position du DPO

3.1. Implication

10. Selon la loi, le service de police concerné doit toujours impliquer le *DPO* à temps et correctement dans toutes les questions qui ont trait à la protection des données personnelles.

En pratique, cela veut dire qu'un *DPO* doit toujours être impliqué le plus tôt possible dans les questions qui ont trait à la protection des données. De cette manière, on peut souvent réagir de manière ad hoc, on peut tenir compte à un stade précoce de l'avis du *DPO* et on peut faire application du principe '*privacy by design*'. Il est recommandé de documenter, outre la motivation obligatoire, les motifs pour lesquels l'avis du *DPO* n'est pas suivi.

Dès qu'une infraction aux données ou un autre incident se produit dans le cadre du traitement des données, le *DPO* doit immédiatement être consulté.

11. L'Organe de contrôle insiste non seulement sur l'implication, c.à.d. que la direction du corps et les dirigeants opérationnels doivent toujours impliquer le *DPO* à temps, mais aussi que cette direction du corps soutienne suffisamment le *DPO* dans le champ de tensions qu'il y aura toujours entre les désidératas des fonctionnaires de police opérationnels et les nécessités de la protection des données.

3.2. Moyens utilisés

12. Le service de police concerné est légalement tenu de mettre à disposition du *DPO* les moyens nécessaires à l'accomplissement de ses missions et de lui donner accès aux données personnelles et aux traitements. Il s'agit ici du soutien que le management apporte au *DPO*: selon la taille d'une zone de police, et les traitements de données qui s'y déroulent, un *DPO* doit consacrer plus ou moins de temps à ses tâches de *DPO* et celles-ci doivent avoir la priorité requise. On pense par exemple à la préparation et à l'introduction à temps des *DPIA* préalables auprès de l'Organe de contrôle. Avec le nombre croissant de cas dans lesquels les nouvelles technologies sont utilisées dans une zone de police en rapport avec le traitement de données à caractère personnel (l'utilisation de *drones*, de *bodycams*, etc.), cela peut potentiellement prendre plus de temps dans l'agenda du *DPO*. Le management doit donner au *DPO* l'espace nécessaire dans ses tâches pour effectuer ces tâches correctement.

13. Outre la répartition du temps, un soutien adéquat de la part du management à l'égard de la fonction de *DPO* nécessite aussi l'infrastructure nécessaire, les facilités et l'accès aux flux de données dont les services de police font usage.

Concrètement, il est à recommander absolument que le *DPO* ait lui-même directement accès à la B.N.G. et aux autres bases de données policières pertinentes et ne soit pas à chaque fois dépendant pour ce faire d'autres services ou collaborateurs de police.

14. A l'égard de tous les collaborateurs au sein d'un service de police pour lequel un *DPO* accomplit ses tâches, le management doit être transparent dans la désignation du *DPO* et quant à la portée de sa fonction. Les collaborateurs doivent avoir la possibilité de communiquer (directement ou indirectement) avec le *DPO* à propos des questions relatives au traitement des données et inversement, le *DPO* doit nécessairement avoir accès, non

seulement au plus haut dirigeant de l'entité de police, mais aussi à un support essentiel, recevoir de l'assistance et des informations de divers services pertinents comme RH, IT, sécurité, etc …

De cette manière, on évite que des fonctionnaires de police individuels ou des collaborateurs CALOG interrogent directement l'Organe de contrôle ou demande un avis sans aucune forme de filtre. Les collaborateurs doivent être convaincus que les canaux internes doivent d'abord être interrogés, canaux dans lesquels le *DPO* joue un rôle crucial. Ce n'est que lorsqu'on ne trouve pas de solution satisfaisante en interne, de préférence via le canal du *DPO*, que le COC est interrogé.

15. Selon la taille du service de police, il est possible que plus d'une personne soit désignée pour remplir les tâches de *DPO*. Chaque personne qui remplit de telles tâches doit aussi se voir offrir la possibilité par le management de suivre les nouveaux développements sur le plan de la protection des données et doit pouvoir et devoir suivre des formations dans ce cadre pour maintenir l'expertise à un niveau élevé.

En principe, le *DPO* doit avoir d'autant plus de moyens à disposition qu'augmentent la complexité et la sensibilité du traitement de données.

3.3. Indépendance

16. Conformément à l'article 64, alinéa 3 de la LPD, un service de police doit veiller à ce que le *DPO* ne reçoive pas d'instructions relatives à l'accomplissement de ses tâches comme *DPO* en vue d'assurer au *DPO* une autonomie suffisante.

Concrètement, cette indépendance concerne non seulement le résultat à obtenir ou obtenu, mais aussi la manière dont est traitée une plainte, la question de savoir si le *DPO* peut prendre contact avec l'Organe de contrôle, dans le cadre ou non d'une demande d'information ou pour effectuer un signalement.

17. Cette indépendance vaut peu importe la forme d'emploi selon laquelle le *DPO* est engagé. Ainsi, il est inadmissible, d'un point de vue de l'intégrité, qu'un membre du personnel CALOG, qui travaillerait sous un contrat à durée déterminée, soit désigné comme *DPO*, la 'collaboration' ou la 'souplesse' dans la qualité de *DPO* pouvant être un moyen de pression pour prolonger son emploi ou pour y mettre fin. Le *DPO* doit pouvoir, en toute liberté et indépendance, sans risque pour son emploi et sans aucun inconvénient, donner des avis qui vont à l'encontre du point de vue du management. Plus encore, en ligne avec ce qui a été formulé comme directive au niveau européen pour les *DPO* par le 'groupe protection des données article 29', dans un contrat d'emploi d'un collaborateur chargé de tâches de *DPO*, un licenciement du collaborateur concerné pour ses activités comme *DPO* (mais pas le défaut d'activités) devrait être exclu[6].

Vu le fait qu'un DPO auprès de la GPI doit être un membre du personnel de la police (cf. plus loin), la plupart des formes d'emploi seront toutefois de nature statutaire, en sorte qu'il soit essentiel que le DPO ne puisse subir aucun inconvénient suite à l'exercice de sa fonction.

[6] Voir https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 p. 15.

18. De même, d'autres moyens de pression (plus subtils ou non) depuis le management que ceux qui concernent l'emploi ou la carrière du *DPO* ne sont pas admissibles ou permis. Retenir ou reporter une promotion, une demande de mobilité ou un changement de fonction, retirer des avantages dont bénéficient d'autres collaborateurs, faire dépendre l'évaluation du *DPO* de la concordance entre son avis et le point de vue du management ou menacer d'un de ces moyens de pression est évidemment à proscrire.

L'indépendance du *DPO* n'implique nullement que celui-ci dispose de plus de pouvoir de décision que ces tâches légales ne l'exigent: la police et sa direction demeurent, comme responsable du traitement, tenus au respect des principes du traitement, comme la nécessité, la proportionnalité et la finalité et doivent pouvoir démontrer que ces principes sont respectés, conformément à l'article 29 §5 LPD. Plus précisément, le pouvoir de décision repose toujours sur le management du(des) service(s) de police concerné(s) lui-même, mais le *DPO* ne peut être empêché de formuler son avis, qui déroge à cette décision, et d'en faire rapport au chef de corps/à la direction du corps lorsque le *DPO* estime que la décision que le management du service de police a prise est contraire à la réglementation en matière de traitement et de protection des données.

Idéalement, le *DPO* rédige également un rapport annuel de ses activités, avec son avis différent ou non à propos des diverses questions qui ont été traitées ou décidées par le management durant l'année dans le champ d'application du traitement des données. Ce rapport devrait aussi être transmis directement au chef de corps et mis à la disposition de l'Organe de contrôle.

3.4. Conflits d'intérêts

19. Le collaborateur qui travaille comme *DPO* dans un ou plusieurs services de police peut également remplir d'autres tâches que purement celles de *DPO*, à l'exclusion de fonctions de management ou de fonctions dans lesquelles le *DPO* doit également aider à déterminer les objectifs et les moyens pour le traitement des données. Il appartient au responsable du traitement du service de police et non au DPO de veiller à ce que ses tâches et obligations ne comportent pas de conflit d'intérêts[7].

La description des tâches du *DPO* doit être suffisamment précisée et détaillée pour pouvoir détecter et éviter les conflits d'intérêts.

3.5. *Statut*

20. L'article 144 de la Loi sur la Police Intégrée dispose: "*Chaque responsable du traitement et au moins chaque zone de police, le commissariat général, chaque direction générale et chaque direction de la police fédérale désigne un ou plusieurs membres du personnel [8] de la police en tant que délégué à la protection des données, conformément à l'article 37 du règlement général sur la protection des données et à l'article 63 de la loi relative à la protection des données".*

[7] Cfr. article 64 *in fine* LPD
[8] C'est nous qui soulignons.

Il est donc clair, en ce qui concerne la GPI, que le DPO doit être soit un membre du cadre opérationnel, soit un membre du cadre CALOG. Il n'est pas permis de laisser la fonction de DPO à un prestataire de services externe (genre consultant, expert privé, etc …).

2. Missions du DPO

1. Informer et conseiller le management et le personnel quant à leurs obligations relatives à la protection des données à caractère personnel.

21. Concrètement, un *DPO* doit tout d'abord orienter les informations fournies et les avis sur les questions qui comportent un risque plus élevé pour la protection des données. Une telle approche aide les *DPO* à conseiller le(s) service(s) de police concerné(s) à propos de la méthode qu'on doit utiliser pour effectuer une analyse d'impact relative à la protection des données, à propos des choses qui doivent être examinées lors d'un contrôle de la protection interne des données, mais aussi à propos des formations internes qui doivent être données aux collaborateurs et au management et à propos des activités de traitements auxquels plus/le plus de temps et de moyens doivent être consacrés.

2. Vérifier le respect de la réglementation et des règles de police internes relatives à la protection des données personnelles

22. Dans le cadre de la surveillance du respect de la règlementation, le *DPO* doit pouvoir rassembler des informations pour identifier les activités de traitement, analyser leur respect et, le cas échéant, faire des recommandations.

Cette surveillance concerne entre autres la politique du(des) service(s) de police concerné(s) pour lesquels le DPO travaille (comme *DPO*). Concrètement, cela implique qu'un *DPO* dirige l'attribution des responsabilités, la sensibilisation et la formation du personnel concerné par le traitement et les audits à ce sujet. Ainsi, un *DPO* peut parfaitement faire des recommandations à propos des mesures prises pour veiller à ce que seules soient traitées les données personnelles qui sont nécessaires pour les objectifs de traitement de police, ce qui implique qu'il/elle doit évidemment être informé(e) afin de pouvoir accomplir ses tâches comme *DPO* correctement. Le *DPO* doit pouvoir vérifier la quantité de données personnelles collectées, la manière dont elles sont traitées, la période durant laquelle elles sont conservées et leur accessibilité.

3. Rôle relatif à l'analyse d'impact relative à la protection des données (*DPIA*)[9]

23. Une des missions légales d'un *DPO* est de fournir, à la demande, un avis relatif à l'analyse d'impact relative à la protection des données (*DPIA*). Ce faisant, le *DPO* doit veiller à l'exécution d'une telle appréciation conformément aux dispositions légales applicables.

La loi définit quand une analyse d'impact relative à la protection des données doit être effectuée[10].

24. Le contenu concret de ces conditions légales est plus amplement exposé ci-dessous:

[9] Data Protection Impact Assesment.
[10] Article 59 LPD

- Lorsqu'une sorte de traitement implique vraisemblablement un risque élevé pour les droits et libertés des personnes physiques

Si un tel risque élevé est vraisemblable, il faut apprécier sur base de la nature (sensible), de la portée, du contexte ou des finalités du traitement. De même, les garanties qui sont disponibles pour la protection des données personnelles ont ici leur importance.

Concrètement, il faut tenir compte de la question de savoir comment des traitements à grande échelle sont accomplis, ou s'il s'agit de quantités importantes de données à caractère personnel, à quel niveau (local, régional, national ou supranational) les traitements ont lieu et quelle est l'importance du nombre de personnes concernées qui pourraient subir des conséquences (préjudiciables) suite aux traitements.

La nature sensible d'un traitement peut entre autres se rapporter, p.ex. à une appréciation systématique et étendue d'aspects personnels des personnes physiques qui est basée sur le profilage de données, ou du traitement de catégories particulières de données à caractère personnel, de données biométriques ou de données relatives à des condamnations pénales ou des faits punissables.

Les données de police seront donc généralement, en pratique, par nature sensibles.

Il importe en outre que la(les) zone(s) de police ou les services reconnaisse(nt) les risques en la matière et explique(nt) quelles sont les limites apportées aux droits et libertés des personnes physiques. Certainement lorsque des personnes physiques pourront moins facilement exercer leurs droits, il importe que le service de police concerné motive suffisamment pourquoi le traitement des données personnelles prime sur ces limitations ou éventuellement même sur une impossibilité d'exercer certains droits.

En d'autres termes, il s'agit ici d'une auto-évaluation sur le plan de la protection des données que les services de police concernés doivent effectuer de la manière la plus complète possible, compte tenu de tous les intéressés et de leurs intérêts légitimes.

Une analyse d'impact relative à la protection des données ne se limite d'ailleurs pas à un seul projet, mais peut concerner de nombreux objectifs et niveaux, p.ex. lorsque divers services de police veulent créer une application de traitement ou une plateforme commune, ou lorsque plusieurs zones de police ou services prévoient d'instaurer une application ou un environnement de traitement commun comme outil multifonctionnel, de sorte que les risques sur le plan de la protection des données, liés à de tels traitements, augmenteront plus rapidement et nécessiteront plus d'attention.

- Avec une attention particulière pour l'utilisation de nouvelles technologies

On pense ici, par exemple, à l'utilisation de *bodycams* ou de *drones*, surtout lorsque ceux-ci sont équipés de software qui n'a pas été utilisé ou testé antérieurement.

Il faut observer ici l'état de la technologie, le caractère courant de la technologie existante, les nouvelles possibilités d'utilisation qui sont ajoutées au *software* existant, etc. Lorsqu'il s'agit, p.ex. d'un projet pilote dans lequel une technologie déjà existante est utilisée pour la première fois dans un service de police, sans que l'impact pour la protection des données n'ait été délimité par le passé, il est recommandé de présenter une analyse d'impact relative à la

protection des données pour avis au *DPO* pour effectuer l'appréciation la plus qualitative et avertie possible.

- Préalablement au traitement des données

Pour que l'analyse d'impact relative à la protection des données soit fonctionnelle, elle doit avoir lieu à temps. Il ne suffit pas qu'une analyse d'impact relative à la protection des données ait déjà été effectuée dans le cadre de l'établissement d'un fondement juridique pour qu'ensuite on n'effectue pas d'évaluation des effets pour les activités de traitement qui reposent sur ce fondement juridique. De même, une copie de cette appréciation ne suffit pas, puisqu'elle doit être orientée vers les caractéristiques spécifiques et les conséquences de l'activité de traitement ainsi que sur leur implémentation pratique.

25. Pour que le *DPO* puisse soutenir le(s) service(s) de police concerné(s) dans l'établissement d'une analyse d'impact relative à la protection des données, il faut le cas échéant que la demande d'avis ait lieu à temps. Le temps nécessaire pour fournir un avis doit de préférence être déterminé en tenant compte des divers aspects d'une telle analyse, à savoir une analyse des mesures prises, des garanties et mécanismes pour la protection des données à caractère personnel, et on doit également démontrer que la législation sur la protection des données est respectée. Les analyses d'impact doivent couvrir les systèmes et procédures pertinents des activités de traitements, mais pas les cas individuels.

26. La question de savoir si le management demande le cas échéant l'avis du *DPO* ne peut en aucun cas dépendre d'une appréciation d'opportunité relative au lancement de l'activité de traitement ou des points de vue discordants qui pourraient découler de l'avis. Il s'agit ici évidemment d'une compétence discrétionnaire du management, mais il doit néanmoins respecter la règle que le *DPO* est impliqué correctement dans toutes les questions qui sont en rapport avec la protection des données personnelles, même s'il n'estimait pas nécessaire de demander un avis au *DPO*.

4. Agir comme point de contact et collaborer avec l'Organe de Contrôle

27. Cette tâche est étroitement liée à l'indépendance dont un *DPO* doit bénéficier à l'égard du(des) service(s) de police pour le(s)quel(s) il est actif en sa qualité de *DPO*: le(s) service(s) de police concerné(s) ne peu(t)(vent) pas apprécier ou influencer si le *DPO* prend contact avec l'Organe de Contrôle. Il s'agit alors principalement de situations dans lesquelles le *DPO*, de par son expertise sur le plan de la protection des données, estime qu'il peut être utile ou nécessaire d'informer l'Organe de Contrôle, ou de demander un avis, ou de donner une réponse définitive sur les circonstances qui pourraient impacter la protection des données et/ou les droits des personnes physiques.

De même, dans le cadre du signalement et de la documentation d'infractions relatives aux données à caractères personnel ou d'infractions à la sécurité, des conséquences de ceci et des mesures de correction prises, le *DPO* joue un rôle important dans la communication vers l'Organe de Contrôle.

Si le service de police désigne un (nouveau) *DPO,* il doit, en sa qualité de responsable du traitement, communiquer à l'Organe de Contrôle les coordonnées du *DPO* afin de concrétiser une bonne collaboration et de satisfaire à son obligation légale[11].

28. Enfin, on peut se référer aux compétences de l'Organisme de Contrôle, dans l'exercice desquelles le *DPO*, comme point de contact, doit fournir à la demande son entière collaboration au COC, et ceci en relation, mais de manière indépendante, avec le(s) service(s) de police pour le(s)quel(s) il/elle est actif(ve).

Enfin, nous rappelons ici (cf. numéro 14) qu'il faut éviter que des fonctionnaires de police individuels ou des collaborateurs CALOG interrogent directement l'Organe de Contrôle sans aucune forme de filtre. Les collaborateurs doivent interroger de manière prioritaire les canaux internes, parmi lesquels le *DPO*. Ce n'est que lorsqu'aucune solution satisfaisante n'est trouvée en interne que le COC est interrogé par le canal du *DPO*.

Le *DPO* est donc également l'interlocuteur privilégié du COC.

IV. Conclusion

29. Bien que la figure du *DPO* ne soit pas nouvelle, la fonction a été ancrée davantage et plus fortement d'un point de vue légal dans la LPD, ce qui souligne également l'importance de la fonction et des tâches qu'un *DPO* exerce au sein de la GPI.

En partant de la *LED*, le législateur belge a mis l'accent sur la nécessité d'une expertise dans le chef du *DPO* sur le plan de la protection des données. Son expertise doit être en rapport avec la complexité du traitement de données qu'il rencontre sur son lieu de travail, et ses qualités professionnelles doivent concerner tant la législation concernée que la structure et l'organisation de la GPI et les flux de données de police, mais aussi les aptitudes personnelles et une éthique professionnelle de haut niveau.

30. Il est d'une importance primordiale quant à la position du *DPO* : chaque service de police doit trouver un équilibre entre une implication suffisante du *DPO* dans toutes les matières concernant le traitement des données à caractère personnel, prévoir les moyens nécessaires pour permettre au *DPO* d'accomplir correctement ses tâches et l'indépendance qui doit être celle d'un *DPO* dans l'exercice de ses tâches. Surtout la relation d'autorité et le contenu matériel et interne des tâches qui reposent éventuellement encore sur le *DPO*, outre cette fonction, sont des points d'attention sensibles pour atteindre cet équilibre délicat et éviter les conflits d'intérêts. Mais aussi l'infrastructure, le temps consacré et l'accès nécessaire à toutes les données et bases de données (de police) concernées sont importants.

31. Enfin, une bonne compréhension des tâches du *DPO* est nécessaire pour avoir une image correcte de la fonction. A cette fin, le management doit prévoir le support nécessaire. Le *DPO* doit informer et conseiller tant le management que les collaborateurs de police de toutes les questions qui concernent le traitement des données à caractère personnel et il/elle veille au respect de la réglementation et des règles de police internes. Son rôle dans l'établissement d'une analyse d'impact relative à la protection des données (*DPIA*) dépend en partie de la politique que le management a élaborée à ce sujet, mais il faut toutefois recommander, en

[11] Cf. article 63, 4e alinéa LPD.

cas de questions sensibles ou de risques élevés, de toujours faire appel à l'expertise du *DPO*. Certainement lorsqu'il s'agit de nouvelles technologies ou de matières complexes, l'avis du *DPO* peut contribuer à une meilleure évaluation de la probabilité des risques et/ou à une meilleure vision de la part du management en matière de traitement des données.

Enfin, la bonne collaboration et communication avec l'Organe de Contrôle est également une tâche importante pour le *DPO,* puisqu'il/elle sera toujours le premier point de contact et qu'il n'y ait pas de crainte à avoir pour faire des signalements pertinents à propos de problèmes de protection des données ou d'infractions à ce sujet.

Il importe que lors de chaque changement de *DPO*, ceci soit immédiatement communiqué à l'Organe de Contrôle.

Par ces motifs,

l'Organe de Contrôle de l'information policière,

rend de sa propre initiative le présent avis

Donne, conformément à l'article 237, deuxième, troisième et quatrième alinéa de la LPD, cet avis d'office:

- aux Ministres de la Sécurité et de l'Intérieur et de la Justice
- au Collège des procureurs généraux
- au Commissaire général de la police fédérale
- à la Commission Permanente de la Police Locale

Avis de propre initiative approuvé par l'Organe de contrôle de l'information policière le 14 avril 2020

Pour l'Organe de Contrôle,

Le président,

(sign.) Philippe ARNOULD