ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA190013		xx juin 2019

Objet : Avis relatif à un avant-projet de loi relative à l'approche administrative communale et portant création d'une Direction Évaluation de l'Intégrité pour les Pouvoirs publics.

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

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (*M.B.* du 5 septembre 2018, ci-après la "Loi sur la protection des données" ou "LPD"), en particulier l'article 59, § 1er, 2e alinéa, l'article 71 et le Titre 7, en particulier l'article 236.

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier l'article 4, § 2, quatrième alinéa.

Vu la loi du 5 août 1992 *sur la fonction de police* (ci-après la "LFP"), en particulier l'article 44/6.

Vu la notification du Conseil des Ministres du 29 mars 2019 concernant l'avant-projet de loi susmentionné (point 23) par laquelle il a été décidé de soumettre l'avant-projet pour avis notamment à l'Autorité de protection des données.

Vu la demande du 16 mai 2019 de Monsieur Pieter De Crem, Ministre de la Sécurité et de l'Intérieur, adressée à l'Autorité de protection des données afin qu'elle émette un avis sur le projet de loi susmentionné.

Vu la demande de l'Autorité de protection des données (ci-après "l'APD") du 17 mai 2019 adressée à l'Organe de contrôle afin de vérifier si l'Organe de contrôle ne doit pas également émettre un avis sur l'avant-projet de loi susmentionné, vu les dispositions légales mentionnées ci-après.

Vu le rapport de Monsieur Frank Schuermans, membre-conseiller de l'Organe de contrôle.

Émet, le 17 juin 2019, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a profondément modifié les tâches et les missions de l'Organe de contrôle. L'article 4, § 2, quatrième alinéa de la loi organique du 3 décembre 2017 *portant création de l'Autorité de protection des données* (ci-après la "Loi organique APD") dispose que pour les services de police au sens de l'article 2, 2° de la loi du 7 décembre 1998 *organisant un service de police intégré, structuré à deux niveaux*, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle.

2. Cela signifie notamment que l'Organe de contrôle est également compétent lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socio-économiques ou de traitements de ressources humaines. L'Organe de contrôle doit être consulté dans le cadre de la préparation d'une législation ou d'une mesure réglementaire liée au traitement de données à caractère personnel par les services de police de la police intégrée (voir l'article 59, § 1er, 2e alinéa et l'article 236, § 2 de la LPD ainsi que l'article 36.4 du RGPD et l'article 28.2 de la Directive Police et Justice). Dans ce cadre, l'Organe de contrôle a pour mission d'examiner si l'activité de traitement envisagée par les services de police est conforme aux dispositions des Titres 1er (pour les traitements non opérationnels)[3] et 2 (pour les traitements opérationnels) de la LPD[4]. En outre, le COC a également une mission d'avis d'initiative, prévue à l'article 236, § 2 de la LPD, et une mission d'information générale du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans la matière du droit à la protection de la vie privée et des données, prévue à l'article 240 de la LPD.

3. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou de police judiciaire, l'Organe de contrôle émet un avis, soit d'initiative, soit à la demande du gouvernement ou de la Chambre des représentants, d'une autorité administrative ou judiciaire ou d'un service de police concernant toute question relative à la gestion de l'information policière, telle que régie dans la Section 12 du Chapitre 4 de la loi *sur la fonction de police*[5].

---

[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 ou "RGPD").

[2] 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* (ci-après la "Directive Police et Justice").

[3] Article 4, § 2, quatrième alinéa de la Loi organique APD.

[4] Article 71, § 1er, troisième alinéa de la LPD.

[5] Article 59, § 1er, 2e alinéa et article 236, § 2 de la LTD.

4. Enfin, l'Organe de contrôle est également chargé du contrôle de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel telles que visées aux articles 44/1 à 44/11/13 de la loi *sur la fonction de police* et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois vis-à-vis des services de police, de l'Inspection générale de la police fédérale et de la police locale (ci-après l' "AIG"), telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale, et de l'Unité d'information des passagers (ci-après "BelPIU"), telle que visée dans le Chapitre 7 de la loi du 25 décembre 2016.[6]

II. Objet de la demande

5. Pour le cadre général, le contexte et les finalités de l'avant-projet, le COC renvoie à l'avis susmentionné de l'APD ainsi qu'à l'avis n° 75/2018 de l'APD déjà émis le 5 septembre 2018 concernant une précédente (et première) version du projet[7], introduite par le Ministre de la Sécurité et de l'Intérieur de l'époque, Jan Jambon.

III. Discussion

6. Dans le présent avis, le COC limite son examen aux articles qui concernent directement ou indirectement les traitements policiers de données à caractère personnel repris dans le projet ou ayant (pouvant avoir) directement ou indirectement une influence sur le fonctionnement de la police intégrée dans le cadre plus large de la gestion de l'information policière.

7. En l'occurrence, il s'agit tout d'abord de l'article 8 de l'avant-projet qui fait partie de la Section 3 ("*La rédaction de l'avis*") du Chapitre 3 ("*Les missions et le fonctionnement de la DEIPP*") du Titre 2 ("*Création d'une Direction Évaluation de l'Intégrité pour les Pouvoirs publics*"). Mais d'autres articles ont également leur importance (directe ou indirecte). Ainsi, le présent avis concerne également les articles 2, 10, 11, 12, 16, 18, 19 et 20. Dans le présent avis, le COC suit la chronologie de l'avant-projet.

8. Les missions de la DEIPP sont définies à l'article 6 comme étant la fourniture d'avis non contraignants à l'administration locale requérante (toutefois limitée au bourgmestre visé dans le projet d'article 119*ter*, § 7 NLC) quant à l'intégrité d'une personne physique ou d'une personne morale chargée en droit ou en fait d'une exploitation, et ce à des fins de prévention de la criminalité grave et organisée. La DEIPP réalisera donc concrètement une enquête d'intégrité sur demande concernant les personnes physiques ou morales précitées qui souhaitent entrer en considération pour remporter un marché public, une concession ou une subvention déterminé(e)s (voir l'article 3). Cette enquête d'intégrité portera sur le fait (ou les indices de fait), par le demandeur ou le candidat, de s'associer

---

[6] Article 71, § 1er, troisième alinéa *juncto* article 236, § 3 de la LPD.

[7] Avis APD n° 75/2018 du 5 septembre 2018 concernant un avant-projet de loi relatif à l'approche administrative communale, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_75_2018.pdf.

pour commettre, de tenter de commettre, d'aider ou d'inciter quelqu'un à commettre ou le conseiller à cet effet, ou de faciliter l'exécution d'un ou de plusieurs faits punissables énumérés à l'article 2 et qui sont dès lors considérés comme "criminalité grave et organisée".

9. Il convient de s'interroger sur la délimitation des matières qui sont décrites comme "*faits punissables*" (voir le projet d'article 2 et le projet d'article 119*ter* de la NLC). Des notions telles que fraude fiscale et sociale "*grave*" et criminalité environnementale "*grave*" ou criminalité "*grave*" alimentaire et dans le secteur des médicaments restent vagues et volatiles. Pour le COC et on peut craindre que ce sera également le cas des services de police, il n'est d'emblée pas clair de savoir ce qu'il y a lieu d'entendre par là et quelles informations/données à caractère personnel peuvent à présent être communiquées ou non. Si cette notion est déjà utilisée dans le jargon juridique pour la fraude fiscale, ce n'est absolument pas le cas pour les autres domaines de criminalité. Dans leurs banques de données policières, les services de police travaillent soit avec des incriminations pénales, soit avec des dénominations/codages propres qui ne correspondent pas d'emblée aux termes utilisés dans le projet et qui sont qualifiés de "*faits punissables*". Il faut à tout le moins éviter que chaque service de police interprète ces notions différemment pour éviter qu'ils ne transmettent différents types d'informations/de données à caractère personnel (avec également pour conséquence immédiate un traitement inégal des demandeurs). Prenons l'exemple de la "*criminalité environnementale grave*" : les dépôts clandestins en font-ils partie (sous ses diverses formes) ? Peut-on classer sous la notion de "*fraude sociale grave*" le fait de se soustraire aux déclarations DIMONA ? Ou de se soustraire aux obligations de cotisation à la sécurité sociale ? Ou l'occupation d'un (ou de plusieurs ?) travailleurs illégaux, etc.

En outre, ces faits punissables doivent aussi être commis "*d'une façon organisée*". Ici non plus, on ne donne aucune définition. S'agit-il de l'imputation d' "*organisation criminelle*" telle que prévue dans le Code pénal, s'agit-il plutôt de la définition criminologique employée dans de nombreux documents stratégiques ou vise-t-on encore autre chose par cela ? C'est le flou le plus total. Il convient d'ailleurs de remarquer qu'en vertu du droit belge, nombre de ces "*faits punissables*" ne sont pas du tout des "*infractions*" (bien que ce terme soit utilisé dans le projet d'article 2, 1er alinéa) au sens juridique du terme (et ceux-ci répondent donc à une description de délit avec des éléments constitutifs clairs).

10. Enfin, il doit être clair – aussi pour l'auteur du projet – que par la formulation utilisée ("*infractions*"), il ne puisse pas être question de la transmission (voir plus loin) à la DEIPP par les services de police d'informations de police administrative, telles que visées à l'article 44/5, § 1er[8] de la LFP, qui se trouvent dans la BNG, les banques de données de base ou les banques de données particulières. On ne sait pas clairement si telle est aussi l'intention de l'auteur du projet. On peut en

[8] Les données à caractère personnel qui sont traitées à des fins de police administrative dans les banques de données visées à l'article 44/2, § 1er, deuxième alinéa, 1° et 2°.

douter, d'autant plus que cette restriction ne semble pas s'appliquer aux enquêtes d'intégrité qui sont menées sans avis de la DEIPP par le bourgmestre (les services du bourgmestre). Bien que même dans ces cas, ce n'est pas très clair non plus. Sous la dénomination "*données financières, administratives et les données en matière judiciaire*" du projet d'article 119*quater*, § 1er, e) de la NLC, qui contient la définition des données à caractère personnel qui peuvent être traitées dans le cadre d'une enquête d'intégrité, retrouve-t-on en effet aussi les données de police administrative que les services de police traitent (voir également ci-après) ?

11. Bref, il semble que les problèmes d'application quant à savoir exactement, pour un service de police fournissant des informations (mais cette remarque s'applique aussi *mutatis mutandis* à tous les autres services fournisseurs d'informations), ce qui peut être communiqué, seront légion.

Indépendamment de cela, un problème encore plus important se pose bien entendu en ce qui concerne le respect du principe de légalité, aussi et surtout dans l'intérêt du citoyen/de la personne concernée. Celui-ci/celle-ci doit pouvoir savoir au préalable, avec une prévisibilité raisonnable, quels comportements entrent (peuvent entrer) en considération pour être communiqués à la DEIPP et quelles informations/données à caractère personnel sont reprises (peuvent être reprises) dans son dossier. Pour les "*faits punissables*" précités, cela semble extrêmement problématique (voir également les normes juridiques évoquées au point 15).

12. L'article 8, § 1er énumère les services qui, à la demande de la DEIPP, peuvent transmettre des informations/données à caractère personnel. Il est clair que la DEIPP ne peut que "*requérir*" ces services de transmettre des informations/données à caractère personnel et ne peut les y contraindre. Les services de la police intégrée sont mentionnés comme un des 10 types de services auxquels une telle requête peut être adressée.

La première question qui se pose est de savoir si la police peut transmettre ces informations/données à caractère personnel de manière autonome. Il semble que ce soit l'intention, ce qui donne lieu d'emblée aux remarques suivantes :

1. <u>En ce qui concerne les informations/données à caractère personnel qui sont traitées à des fins de police judiciaire</u>

13. Tout d'abord, il ne semble a priori pas acceptable que les services de police transmettent personnellement ou de manière autonome des informations de police judiciaire. Un accord préalable du ministère public (MP) compétent doit donc être obtenu, vu le cadre légal existant en vigueur auquel le présent avant-projet n'a manifestement pas l'ambition de déroger. On peut faire référence aux articles 21*bis* du Code d'instruction criminelle et 1380 du Code judiciaire ainsi qu'à l'arrêté royal Frais

de justice en matière répressive du 28 décembre 1950 qui confère au MP compétent le monopole pour la communication des informations judiciaires (comme c'est le cas de longue date). Cet accord préalable peut être soit ponctuel (donc par dossier ou au cas par cas), soit structurel (via une circulaire par exemple du Collège du ministère public/Collège des procureurs généraux).

Ceci est conforme au projet d'article 8, § 1er, 2e alinéa qui affirme que "*la communication, l'utilisation et le traitement de ces données se font conformément à la législation qui s'applique pour le service concerné*". Une disposition similaire a été reprise dans le projet d'article 119*quater*, § 1er, 4e alinéa de la NLC.

14. Ensuite, il est encore précisé que "*en tout état de cause, le service interrogé par la DEIPP est autorisé à refuser de fournir les informations demandées par la DEIPP s'il a argumenté la décision de façon suffisante et pertinente*". Une phrase similaire a été insérée dans le projet d'article 119*quater*, § 1er, 4e alinéa de la NLC pour la communication de données (à caractère personnel) par la Police intégrée dans le cadre de l'exécution de l'enquête d'intégrité du projet d'article 119*ter* de la NLC (bien qu'il y soit question en néerlandais de "*voldoende*" plutôt qu' "*afdoende*

La condition selon laquelle le refus de communiquer entièrement ou partiellement des données à la DEIPP doit être "*argumenté de manière suffisante et pertinente*" n'est pas acceptable. Tout d'abord, la question se pose de savoir qui effectuera l'évaluation du caractère suffisant et pertinent. La DEIPP ne peut pas procéder à cette évaluation étant donné que les informations/données à caractère personnel ne proviennent pas d'elle. Seul le fournisseur des informations/données à caractère personnel peut réaliser cette évaluation de manière utile. En outre, les règles normales d'autorité et de contrôle ainsi que les systèmes hiérarchiques jouent également un rôle. En ce qui concerne les informations judiciaires, cette évaluation est effectuée par le MP ou par la police sous l'autorité du MP qui a la direction et le contrôle des enquêtes en matière pénale. Il s'agit donc d'un ajout inutile qui ne fait que semer la confusion. Par ailleurs, si les services de police ne souhaitent pas communiquer des informations/données à caractère personnel (ou certaines d'entre elles), on peut supposer qu'il y a de bonnes raisons à cela : ne pas (encore) vouloir divulguer la phase secrète de l'enquête (pour par ex. ne pas vider de leur sens certaines méthodes de recherche), vouloir protéger certaines sources, un ordre en ce sens du MP, etc. Le but ne peut pas être que les services de police qui fournissent des informations aient à se justifier vis-à-vis de la DEIPP. C'est aussi imposer une charge de travail inutile à la police qui doit ainsi faire face à des problèmes de capacité chroniques. L'élément de phrase "*s'il a argumenté la décision de façon suffisante et pertinente*" ou toute la phrase doit dès lors être supprimé(e).

15. Le COC fait remarquer que l'arrêté royal délibéré en Conseil des ministres qui fixera les modalités de la nature des données, la demande et la communication des données, y compris la désignation

d'un point de contact, si aucun membre du personnel n'était détaché, doit être soumis à l'avis de l'Organe de contrôle en vertu de l'article 59, § 1er, 2e alinéa de la LPD.

L'Organe de contrôle rappelle toutefois qu'en vertu de l'article 8 de la CEDH et de l'article 22 de la Constitution, toute ingérence d'une autorité publique dans le droit au respect de la vie privée (ce qui comprend la protection des données à caractère personnel) doit être prescrite dans une "*disposition légale suffisamment précise*" qui répond à un besoin social impérieux et qui est proportionnelle à la finalité poursuivie. Une telle disposition légale précise doit définir les éléments essentiels des traitements de données à caractère personnel allant de pair avec l'ingérence de l'autorité publique[9]. Dans ce cadre, il s'agit au moins :

a) des finalités déterminées, explicites et légitimes ;
b) des (catégories de) données à caractère personnel qui sont pertinentes et non excessives ;
c) du délai de conservation maximal des données à caractère personnel enregistrées ;
d) de la désignation du responsable du traitement.

Le présent projet ne régit en tout cas pas du tout ou du moins pas suffisamment la condition reprise sous le point b), ce qui n'est pas acceptable. Ainsi, en ce qui concerne la condition reprise au point b), on ne sait pas clairement quelles catégories d'informations peuvent être communiquées :

- des informations judiciaires ou administratives ou les deux ;
- uniquement des informations relatives à des faits concrets ou également ce qu'on appelle des "informations douces" ; lorsqu'on relit les critères pouvant conduire à la non-délivrance, à la suspension ou à l'abrogation d'un permis ou à la fermeture d'un établissement sur la base de l'enquête d'intégrité qui a été menée, on doit conclure que le but est peut-être de prendre en considération n'importe quel type d'informations (aussi les faits non concrets, aussi des informations non validées, etc.) (voir le projet d'article 119*ter*, § 6 de la NLC qui parle de "*présomptions raisonnables*", "*que l'établissement sera exploité*", "*le rapport entre l'exploitant et les faits punissables*", "*exercer de façon indirecte des fonctions de direction*", "*occupe ou occupera de facto une position dominante vis-à-vis de l'exploitant*", qui sont tous des termes relatifs à des faits, des allégations, des circonstances ou des informations doux (douces) et/ou non validé(e)s) ;
- des informations provenant uniquement de sources nationales ou également de sources internationales (banques de donnée d'Europol, données d'Interpol, etc.) ;
- des informations sous embargo (soit un embargo légal imposé par le MP, soit un code d'utilisateur limité comme le prévoit la MFO-3) ;

[9] Voir DEGRAVE, E., "L'e-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle", Collection du CRIDS, Larcier, Bruxelles, 2014, p. 161 e.s.(voir par ex. : CEDH, arrêt Rotaru c. Roumanie, 4 mai 2000). Voir également notamment les arrêts suivants de la Cour constitutionnelle : arrêt n° 44/2015 du 23 avril 2015 (p. 63), l'arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et l'arrêt n° 29/2018 du 15 mars 2018 (p. 26).

- quid de toutes les informations/données à caractère personnel qui ne concernent pas le demandeur ou "*les personnes chargées en droit ou en fait de l'exploitation*" (voir le projet d'article 119*ter*, § 5 de la NLC), comme des membres de la famille, des amis, des connaissances, des témoins, des victimes, ... ces données se retrouveront-elles aussi dans le dossier de la DEIPP ou dans le dossier administratif final ? La police doit-elle sécuriser ces données avant de les communiquer ? En son article 31, la LPD impose aux services de police, dans la mesure du possible, d'établir une distinction entre les différentes catégories de personnes (auteurs, victimes, témoins, dénonciateurs, ...). L'article 10, § 2 du projet dispose que l'avis de la DEIPP ne peut pas mentionner des données qui pourraient notamment porter préjudice à la protection de la vie privée de tiers. Il s'agit d'emblée d'un aspect important mais la question est de savoir si cela prévient tout risque que des données à caractère personnel portant préjudice à la vie privée des tiers susmentionnés se retrouvent dans le dossier de la DEIPP ou dans celui de l'autorité administrative qui prend la décision. À la lecture de l'article 12 qui contient une description du contenu du dossier de traitement de l'avis, cela ne semble pas être le cas, étant donné que le point 3 mentionne "*les demandes de données conformément à l'article 8 et les données qui ont ainsi été communiquées* (soulignement propre), *ainsi que le service ou l'autorité qui les ont fournies*".
- etc.

Dans un souci d'exhaustivité, l'Organe de contrôle attire encore l'attention, dans ce contexte, sur l'article 6.3 du RGPD qui s'appliquera à la DEIPP, et qui prescrit également, lu conjointement avec l'article 8 de la CEDH et l'article 22 de la Constitution, que toute réglementation qui encadre le traitement de données à caractère personnel doit en principe mentionner les éléments essentiels suivants de ce traitement :

- la finalité du traitement[10] ;
- les types ou catégories de données à caractère personnel à traiter ; ces données doivent en outre être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ("minimisation des données")[11] ;
- les personnes concernées ;
- les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ;
- les durées de conservation[12] ;
- ainsi que la désignation du responsable du traitement.

---

[10] Voir l'article 5.1.b) du RGPD.

[11] Voir l'article 5.1.c) du RGPD.

[12] Voir l'article 5.1.e) du RGPD.

La désignation des (catégories de) données à caractère personnel qui sont pertinentes et non excessives et qui peuvent être transmises à la DEIPP par les services qui les ont fournies doit donc être régie dans le projet et ne peut pas être traitée dans un arrêté royal (voir également ci-après au point 24).

16. En outre, l'attention de l'auteur du projet est attirée sur l'article 44/11/9, § 2 de la LFP, récemment modifié par le projet de loi déjà approuvé par le Parlement modifiant diverses dispositions en ce qui concerne la gestion de l'information policière (ci-après le Projet Gestion de l'Information policière 2019), qui est libellé comme suit :
"*§ 2. Selon les modalités déterminées par les directives des ministres de l'Intérieur et de la Justice, chacun dans le cadre de ses compétences, elles* (les données à caractère personnel policières et les informations, ndlr.) *peuvent également être communiquées aux autorités publiques belges, organes ou organismes publics ou d'intérêt public chargés par la loi de l'application de la loi pénale ou qui ont des missions légales de sécurité publique lorsque ceux-ci en ont besoin pour l'exécution de leurs missions légales. La liste de ces autorités, organes ou organismes est arrêtée par les ministres de l'Intérieur et de la Justice sur la base d'une proposition du Comité information et ICT visé à l'article 8sexies de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux. L'avis de l'Organe de Contrôle concernant cette proposition est sollicité.* (soulignement propre)"

La première question qui se pose est de savoir quel est le lien entre l'article 8, § 1er, a) ainsi que le projet d'article 119*quater*, § 1er, e) de la NLC et l'article 44/11/9, § 2 modifié de la LFP. La DEIPP est incontestablement une autorité publique belge, un organe ou organisme public ou d'intérêt public mais la question est de savoir si elle a aussi des "*missions légales de sécurité publique*". Cela ne semble pas si évident, étant donné que la DEIPP a uniquement une mission d'avis non contraignant. En outre, la DEIPP doit être reprise dans la liste des organismes par les deux ministres de tutelle sur proposition du nouveau "Comité Information et ICT" visé à l'article 8*sexies* de la Loi sur la Police Intégrée (LPI), proposition au sujet de laquelle l'Organe de contrôle doit également rendre son propre avis.

Quel est le lien entre ce cadre légal relatif à la communication d'informations policières à des "Law Enforcement Agencies" tierces de l'article 44/11/,9, § 2 de la LFP et le présent avant-projet, en ce qui concerne la DEIPP ? Le présent avant-projet doit-il être perçu comme une dérogation aux règles de la LFP ? L'Organe de contrôle lit également dans le projet d'article 119*quater*, § 1er, 4e alinéa que "*La communication, l'utilisation et le traitement de ces données se font conformément à la législation qui s'applique au servie concerné*". En d'autres termes, les règles de la LFP semblent donc primer.

L'auteur doit apporter de la clarté à ce sujet.

2. En ce qui concerne les informations/données à caractère personnel qui sont traitées à des fins de police administrative

17. L'Organe de contrôle rappelle ici ce qui a été précisé au point 10 et la constatation selon laquelle il n'est absolument pas permis aux services de police de transmettre des informations/données à caractère personnel de police administrative à la DEIPP. Il doit en effet s'agir d'informations/de données à caractère personnel relatives à des "*infractions*" ou à leurs participants (dans le sens qui est donné à "participation" à l'article 2, *in fine*). L'auteur du projet doit faire la clarté à cet égard. Ce qui est mentionné aux points 14 et suivants s'applique à titre subsidiaire aussi ici, *mutatis mutandis*, ainsi que ce qui est précisé au point 15.

18. L'article 11, *in fine*, prévoit que la DEIPP tient des fichiers de journalisation qui sont conservés pendant trois ans. Un délai similaire est prévu pour les traitements de données à caractère personnel réalisés par le bourgmestre (les services du bourgmestre) lors de l'exécution de ce qu'on appelle l'enquête d'intégrité (voir le projet d'article 119*quater*, § 4, 2e alinéa de la NLC).

Il est également essentiel pour les services de police (et tous les autres services fournisseurs d'informations) que soient tenus des fichiers de journalisation des traitements d'informations/de données à caractère personnel provenant des services de police fournisseurs. En cas de violation de la sécurité ou de data breach, il est essentiel de pouvoir retracer la source de la violation, a fortiori vu le type de données que la DEIPP reçoit de la police. À cet égard, un délai de 3 ans est trop court. Le COC fait remarquer que la LFP prévoit actuellement des délais de 30, 15 ou 10 ans pour les fichiers de journalisation des banques de données policières (voir la Loi Gestion de l'information policière 2019, le nouveau § 3 de l'article 44/9 et le nouvel alinéa de l'article 44/10, § 1er en ce que concerne la BNG (30 ans) ; le nouveau § 8 de l'article 44/11/2 en ce qui concerne les banques de données de base (15 ans avec une possibilité de prolongation jusqu'à 20 ans) et le nouveau § 4 de l'article 44/11/3 en ce qui concerne les banques de données particulières (10 ans avec possibilité de prolongation jusqu'à 20 ans)). On peut partir du principe que la plupart des informations qui seront transmises de la police vers la DEIPP ou le bourgmestre (les services du bourgmestre) proviendront de la BNG ou des banques de données de base. Un délai de 30 ans tel qu'applicable pour la BNG est dès lors préférable, au moins un délai de 15 ans.

19. L'article 12 comprend une énumération du contenu du dossier d'avis de la DEIPP. La première question fondamentale qui se pose est de savoir si ce dossier peut être accessible pour le demandeur ou une autre partie intéressée. Il est évidemment essentiel que les services de police le sachent. D'après le 2e alinéa du § 1er, ce dossier "*de traitement de l'avis n'est disponible ou ne peut être consulté que par les membres désignés par le directeur de la DEIPP, en fonction de la nécessité d'en prendre connaissance*". Il faut donc partir du principe que la Loi sur la Publicité de l'administration du 11 avril 1994 ne s'applique pas ici ou plutôt que le présent avant-projet déroge à cette loi. Si c'est le cas, la

question se pose de savoir s'il n'est pas préférable d'également reprendre dans la loi susmentionnée proprement dite l'exception visée dans la présente loi. L'alinéa susmentionné est rédigé de manière si affirmative qu'on ne sait pas non plus clairement si la police ou le parquet peuvent consulter le dossier précité (au besoin, sous la contrainte). Cette disposition touche-t-elle par exemple aux compétences pénales en matière de saisie de la police et du MP ? L'auteur du projet est prié de préciser cet aspect. Il semble recommandé d'également déclarer applicable le 2e alinéa du § 2 au § 1er de manière à ce que non seulement le dossier archivé mais aussi le dossier "vivant" puisse également être consulté par les autorités judiciaires (le cas échéant, sous la contrainte).

20. La clause de confidentialité du projet d'article 16 ne peut pas non plus s'appliquer à l'égard des autorités de contrôle. Ainsi, il est clair qu'un membre détaché des services de police, qui est ainsi devenu membre du personnel de la DEIPP, ne peut ou ne pourrait pas invoquer ce secret dans le cadre d'enquêtes et de contrôles menés par l'Organe de contrôle. Cela s'applique d'ailleurs aux autres autorités de contrôle : l'Autorité de protection des données, le Comité R et le Comité P. Cet article doit donc être amendé comme suit : "*En dehors des cas où ils sont convoqués pour témoigner en droit en matière pénale ou devant un commission d'enquête parlementaire ou à l'égard de l'autorité de contrôle compétente, le directeur, les agents détachés et les magistrats de liaison ainsi que les membres du personnel de la DEIPP sont liés par le secret professionnel et ne peuvent communiquer à aucune personne ou autorité des données dont ils ont eu connaissance dans le cadre de l'exercice de leurs compétences, en vertu de la présente loi. Le secret doit être maintenu même lorsqu'ils ont quitté la DEIPP ou ont cessé leur collaboration*".

21. Le § 4 du projet d'article 119*ter* de la NLC dispose que le bourgmestre désigne les membres du personnel chargés de l'enquête d'intégrité qui est prévue. Le projet de § 12 prévoit que le Roi "*détermine les modalités minimales de l'analyse de risques et les conditions relatives aux membres du personnel chargés de l'enquête d'intégrité*". Le COC se demande si les membres de la police locale sont aussi visés par cette disposition. Si c'est le but, il est préférable de le préciser explicitement, au moins dans l'Exposé des motifs. Il est en effet important que les zones de police sachent qu'elles peuvent être chargées de cette enquête d'intégrité, vu l'impact sur leur capacité opérationnelle, d'autant plus qu'un délai très court de 30 jours est prévu pour boucler cette enquête (abstraction faite de la possibilité de prolonger ce délai une fois de 30 jours). Cela signifie effectivement que de telles enquêtes d'intégrité devront recevoir la priorité absolue avec toutes les conséquences qui en découlent sur l'exécution des autres missions de police de base par la police locale (comme les missions locales de recherche, le travail de quartier local, etc.) Il appartient à l'auteur du projet de reconsidérer ce délai particulièrement strict, en sachant qu'une telle enquête concerne ou peut également concerner la personne physique ou morale qui sera chargée non seulement en droit mais aussi en fait de l'exploitation. Rien que la recherche de la personne qui sera chargée en fait de l'exploitation peut requérir une enquête approfondie et donc du temps. L'Organe de contrôle estime que le délai prévu de 30 jours n'est pas réaliste et risque de donner lieu à des erreurs, des négligences et des échecs.

22. En ce qui concerne le projet d'article 119*quater*, § 1er, e) de la NLC, l'Organe de contrôle renvoie *mutatis mutandis* à ce qui a été précisé ci-dessus aux points 14 et suivants. Ici non plus, il n'y a pas la moindre précision quant aux catégories de données que les services de police peuvent transmettre au bourgmestre (aux services du bourgmestre) dans le cadre de l'enquête d'intégrité. En l'occurrence, c'est encore plus problématique car, dans l'hypothèse où aucun avis n'est demandé à la DEIPP, ce qui n'a pas été rendu obligatoire, il n'y a donc aucune intervention d'un "trusted third party" (tiers de confiance), ce qu'est la DEIPP, et toutes les informations policières sensibles possibles de nature judiciaire et/ou administrative peuvent directement arriver chez le bourgmestre, sans le moindre filtre. Dans ce cadre, le bourgmestre est le chef de la police locale qui se trouve sous son autorité (articles 11 et 42 de la Loi sur la Police intégrée) de sorte qu'il n'est pas si évident, pour une police locale, de refuser certaines informations au bourgmestre ou de les filtrer.

En ce qui concerne les données judiciaires, il est en outre prévu qu' "*Au sein du conseil zonal de sécurité, un protocole est conclu au sujet des enquêtes d'intégrité dans lesquelles des données judiciaires peuvent être utilisées. Ce protocole contient au moins une description du champ d'application matériel et territorial, ainsi que les modalités de communication et d'utilisation des informations*". Que se passe-t-il si aucun protocole n'est conclu ? Un protocole ou de préférence un accord ne peut en effet pas être forcé. Il semble dès lors que dans cette hypothèse, aucune information judiciaire ou information policière de nature judiciaire ne peut être communiquée, par les services de police non plus. Il appartient à l'auteur du projet de distinguer cette hypothèse.

23. Ensuite, l'avant-dernier alinéa du § 1er du projet d'article 119*quater* de la NLC affirme que "*Les données utilisées visées aux points a) jusque e) inclus ne peuvent être traitées qu'au cours d'une période de cinq ans préalable à l'enquête d'intégrité.*" L'Organe de contrôle comprend ce passage dans le sens où les services de police ne peuvent communiquer que des informations et des données à caractère personnel ne datant pas de plus de 5 ans avant le début de l'enquête d'intégrité. Cela signifie tout d'abord que la date exacte de début d'une enquête d'intégrité doit être déterminée. On peut partir du principe que ce début se situe le jour de la notification à l'intéressé (voir le projet d'article 119*ter*, § 4, 3e alinéa de la NLC). Cela signifie que les services de police (et tous les autres services fournisseurs d'informations) devront recevoir cette date du bourgmestre (des services du bourgmestre) qui mènera (mèneront) l'enquête d'intégrité. Ainsi, la police ne peut pas communiquer des informations/données à caractère personnel datant de plus de 5 ans. Cette limitation visant à ne pouvoir retourner dans le temps que jusqu'à 5 ans s'applique également au flux d'informations émanant de la police vers la DEIPP (voir le projet d'article 8, § 1er, a)).

24. Le § 2 du projet d'article 119*quater* tente de décrire les catégories de données à caractère personnel qui seront traitées dans le cadre d'une telle enquête d'intégrité. Comme précisé au point 22, cela reste toutefois très vague : la catégorie la plus importante, faisant l'objet essentiel du présent

projet, est en effet le point e), ce qui est défini comme étant "*Les données financières, administratives et les données en matière judiciaire pour autant que ces données à caractère personnel émanent des instances visées au paragraphe 1er.*" Cette énumération est si large qu'elle ne répond pas aux normes juridiques fondamentales précitées telles que contenues dans la CEDH, le RGPD ou la Constitution.

Dans un souci d'exhaustivité, il faut encore faire remarquer que la version néerlandaise du 5e paragraphe doit être revue.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

requiert le demandeur de donner suite aux remarques reprises aux points 9 à 24 inclus ;

demande pour le reste qu'il soit tenu compte des remarques susmentionnées reprises aux autres points ;

Avis approuvé par l'Organe de contrôle de l'information policière le 17 juin 2019.

Pour l'Organe de contrôle,
Le Président,
(sé.) Philippe ARNOULD