ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA200007		22/09/2020

Objet : Avis relatif à une directive commune des ministres de la Justice et de l'Intérieur relative aux mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2 de la loi sur la fonction de police (directive relative à la sécurité de l'information).

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 LPD') en particulier l'article 59 §1, 2e al, l'article 71 et le Titre VII, en particulier l'article 236.

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données* (ci-après la 'LCA').

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

Vu la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (ci-après la 'LPI').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après la '*LED*').

Vu la loi du 25 décembre 2016 *relative au traitement des données des passagers.*

Vu la demande du 17 septembre 2020 du conseiller S. Godin (Secrétariat technique et administratif relatif à la police intégrée auprès du cabinet Justice) au nom du ministre de la Justice et du ministre de la Sécurité et de l'Intérieur, reçue par courrier électronique par l'Organe de contrôle, d'émettre un avis sur la base de la LPD.

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

Émet, le 22 septembre 2020, 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 remanié en profondeur les tâches et 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 dénommée en abrégé 'LAPD') dispose qu'à l'égard des 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. Cela signifie notamment que l'Organe de contrôle est compétent également lorsque les services de police traitent des données à caractère personnel en dehors du cadre des missions de police administrative et judiciaire, par exemple en vue de finalités socioéconomiques ou de traitements relevant de la gestion des ressources humaines. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. Le COC est en outre investi aussi d'une mission d'avis d'office, prévue à l'article 236 §2 de la LPD, et d'une mission de sensibilisation du public, des personnes concernées, des responsables du traitement et des sous-traitants à la matière du droit à la protection de la vie privée et des données, prévue à l'article 240 de la LPD.

2. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet des 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 matière ayant trait à la gestion de l'information policière telle que régie par 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 dénommée « directive Police-Justice » ou *Law Enforcement Directive* (*LED*)).

[3] Article 4, §2, 4e alinéa de la LAPD.

[4] Article 71, §1er, 3e alinéa de la LPD.

[5] Articles 59, §1er, 2e alinéa et 236, §2 de la LPD.

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé '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 dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé 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[6].

4. Enfin, l'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281, §4 de la loi générale sur les douanes et accises du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 modifiant diverses dispositions relatives au traitement des données des passagers.

II. OBJET DE LA DEMANDE

5. L'objet de la demande est formulé en ces termes par les demandeurs :

« Par le présent mail, les cabinets de l'Intérieur et de la Justice souhaitent vous soumettre pour avis 4 projets de directive commune des ministres de la Justice et de l'Intérieur qui viennent compléter l'arsenal juridique en matière de gestion d'information policière opérationnelle. Ces directives trouvent leur fondement juridique dans les articles suivants de la loi sur la fonction de police :

(i) L'article 44/4 §2 (*Directive sur les mesures nécessaires en vue d'assurer la gestion et les mesures de sécurité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2*)

(ii) L'article 44/4 §§ 3 et 5 (*Directive sur l'accès à la BNG, aux banques de données de base, aux banques de données particulières et aux banques de données techniques par les membres du personnel des services de police)*

(iii) L'article 44/4 §§ 4 et 5 (*Directive sur l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique*)

(iv) L'article 44/4 §6 de la LFP (*Directive sur l'interconnexion ou la corrélation des banques de données techniques*)

Nous vous envoyons également pour avis le projet de fiche CO2 de la MFO-3 concernant les mesures à prendre vu le lien de cette fiche avec les interconnexions et corrélations opérées dans des banques de données techniques. Comme vous le savez, deux de ces directives devront être publiées au Moniteur belge, à savoir, (i) la directive sur l'accès à la BNG, aux banques de données de base, aux banques de données particulières et aux banques de données techniques par les membres du

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

personnel et (ii) celle sur l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique[7] ».

Dans l'intérêt de la lisibilité, le COC utilisera les désignations abrégées suivantes pour chacune des directives susmentionnées :

(i) L'article 44/4 §2 (Directive sur les mesures nécessaires en vue d'assurer la gestion et les mesures de sécurité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2) : **« directive relative à la sécurité de l'information »**
(ii) L'article 44/4 §§ 3 et 5 (Directive sur l'accès à la BNG, aux banques de données de base, aux banques de données particulières et aux banques de données techniques par les membres du personnel des services de police) : **« directive relative aux règles d'accès »**
(iii) L'article 44/4 §§ 4 et 5 (Directive sur l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique) : **« directive relative à l'interconnexion »**
(iv) L'article 44/4 §6 de la LFP (Directive sur l'interconnexion ou la corrélation des banques de données techniques) : **« directive relative à l'interconnexion/la corrélation des BDT »**

6. L'Organe de contrôle émettra un avis distinct pour chaque directive et pour le projet de fiche CO2. Il va sans dire que pour une bonne compréhension de la thématique prise dans son ensemble, ces avis doivent être lus conjointement.

L'objet de l'avis est une directive commune, ci-après dénommée la directive relative à la sécurité de l'information, dans laquelle les demandeurs déterminent en application de l'article 44/4 §2 de la LFP les mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans la Banque de données nationale (BNG), les banques de données de base, les banques de données particulières et les banques de données techniques. La

---

[7] Traduction libre en néerlandais : "Met deze mail wensen de kabinetten Binnenlandse Zaken en Justitie u 4 ontwerpen van richtlijn, die het juridisch arsenaal met betrekking tot de politionele operationele informatiehuishouding vervolledigen, voor advies voor te leggen. Deze richtlijnen vinden hun rechtsgrondslag in de volgende artikelen van de wet op het politieambt:
(i) Artikel 44/4 §2 (Richtlijn met betrekking tot de maatregelen die nodig zijn om het beheer en de veiligheid van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2)
(ii) Artikel 44/4 §§ 3 en 5 (Richtlijn met betrekking tot de toegang tot de ANG, de basisgegevensbanken, de bijzondere gegevensbanken en de technische door de leden van de politiediensten)
(iii) Artikel 44/4 §§ 4 en 5 (Richtlijn betreffende de koppeling van de gegevensbanken bedoeld in artikel 44/2 onderling of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden)
(iv) Artikel 44/4, § 6 van de WPA (Richtlijn betreffende de koppeling of de correlatie van de technische gegevensbanken)
Wij maken u tevens voor advies het ontwerp van fiche CO2 van de MFO3 betreffende de te nemen maatregelen over, gelet op het verband van deze fiche met de koppelingen en correlaties met de technische gegevensbanken. Zoals u weet dienen twee van deze richtlijnen gepubliceerd te worden in het Belgisch staatsblad, te weten (i) de Richtlijn met betrekking tot de toegang tot de ANG, de basisgegevensbanken, de bijzondere gegevensbanken en de technische door de leden van de politiediensten en (ii) deze met betrekking de koppeling van de gegevensbanken bedoeld in artikel 44/2 onderling of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden."

directive est contraignante pour la police intégrée au même titre que les 4 projets de directive soumis pour avis.

7. La mission d'élaborer cette directive a été imposée aux ministres en charge de la police par la loi du 18 mars 2014[8]. Ensuite, les dispositions de la LFP relatives à la gestion de l'information ont été modifiées/remplacées par la loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière (en abrégé la 'loi de 2019 relative à la gestion de l'information policière') afin de mettre les dispositions relatives à la gestion de l'information en conformité avec la *LED* et le Titre 2 de la LPD. Le contenu de la disposition relative à la mission d'élaborer une directive qui incombe aux ministres en charge de la police est resté pour ainsi dire inchangé, mais a été complété de la condition additionnelle que la directive est contraignante pour la police intégrée[9].

III. DISCUSSION

8. Dans le cadre de la gestion de l'information policière, la police intégrée recourt aux nouvelles technologies de l'information et de la communication. Comme indiqué dans la directive, il convient d'accorder dans ce contexte l'attention requise à la sécurité de l'information étant donné qu'il s'agit d'un aspect essentiel et indissociable de la protection des données à caractère personnel. Il s'agit là d'une obligation légale fondamentale qui est ancrée dans les articles 28, 6°, 50 et 51 de la LPD. L'article 44/4 §2 de la LFP exige à cet égard que les ministres en charge de la police déterminent les mesures nécessaires pour satisfaire à ces exigences légales. Ces obligations légales doivent donc être concrétisées dans la directive.

9. Dans la directive, les mesures de sécurité minimales sont déterminées et subdivisées en 17 aspects (sous-rubriques). Il s'agit d'une sélection d'objectifs des *guidelines* du Centre pour la Cybersécurité (*Baseline Information Security Guidelines*), à savoir :
1) la politique de sécurité de l'information et les plans de sécurité ;
2) l'organisation de la sécurité de l'information ;
3) la sécurité concernant les ressources humaines ;
4) la sensibilisation, la formation et la communication ;
5) la gestion des actifs ;
6) le contrôle d'accès ;
7) la cryptographie ;
8) la sécurité physique ;
9) la sécurité liée aux opérations ;

[8] Article 10 de la loi du 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle.

[9] Et l'ajout des termes « *sans préjudice des compétences propres des autorités judiciaires* » (article 7 de la loi du 22 mai 2019).

10) la sécurité de la communication des informations ;
11) l'acquisition, le développement et la maintenance des systèmes d'information ;
12) les relations avec des tiers (fournisseurs, autorités) ;
13) le recours au cloud ;
14) la gestion des incidents liés à la sécurité de l'information ;
15) les aspects de la sécurité de l'information dans la gestion de la continuité de l'activité ;
16) la veille juridique ;
17) l'évaluation des mesures de sécurité.

Bien que ces recommandations doivent en effet être considérées comme des meilleures pratiques, elles doivent, comme nous le faisions remarquer plus haut, être élaborées dans des termes plus concrets à l'échelon des services de police.

10. Au titre de remarque générale, on peut aussi s'interroger ici sur le rapport entre cette directive relative à la sécurité de l'information et les directives contenues dans la circulaire MFO-3. Cette dernière sera-t-elle remplacée par la présente directive pour tous les aspects de la sécurité de l'information, ou les deux textes continueront-ils à coexister ? Faire la clarté sur ce point est d'une importance fondamentale avant tout pour la GPI. Le fait que la MFO-3, qui est tout de même la bible de la gestion de l'information policière, n'ait plus été – et de longue date – actualisée en fonction de l'évolution constante du cadre légal est depuis de nombreuses années un problème cuisant. Or, les 4 projets de directive n'y remédient pas. Au contraire, ils posent une question additionnelle, à savoir celle du rapport entre ces 4 projets et les règles contraignantes existantes de la MFO-3. Aucune des 4 directives ne clarifie ce point. L'auteur des projets doit apporter de la clarté à ce sujet.

Ensuite, le COC se demande si la directive offre suffisamment de transparence dans le sillage des droits fondamentaux octroyés par les conventions, tels qu'ils figurent à l'article 8 de la CEDH et aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. À plusieurs endroits de la directive, les dispositions légales pertinentes de la LPD et de la LFP ainsi que les objectifs des recommandations sont repris (pour ainsi dire littéralement) ou paraphrasés sans être élaborés dans des termes plus concrets en fonction du contexte et du niveau (police fédérale ou police locale) de la mise en œuvre. Comme le stipule la directive, il s'agit de *« mesures minimales que les services de police doivent respecter lors de l'élaboration, l'implémentation et l'évaluation de la politique de sécurité de l'information, des plans de sécurité et des procédures et processus qui en découlent »*[10]. Ces *Baseline Information Security Guidelines* sont en elles-mêmes des objectifs généraux qui doivent être concrétisés. Bien que le COC comprenne que certains aspects doivent plutôt, pour des raisons opérationnelles et stratégiques, être élaborés dans des directives internes, la directive publiée devrait tout de même permettre de se faire une meilleure idée de la conformité de la gestion et de la sécurité

[10] Rubrique *« II. INTRODUCTION »*, p. 3.

de l'information des services de police. Comme le stipule la directive, les ministres en charge de la police veulent notamment, à travers les mesures prévues par la directive, *« assurer la sécurité du personnel et des citoyens et renforcer ainsi la confiance de la société à leur égard »*[11]. En conséquence, le COC n'est pas en mesure, dans cet avis, d'évaluer tous les objectifs sur le fond. La concrétisation plus détaillée des objectifs fixés doit dès lors être tenue à la disposition du COC.

11. Les mesures de sécurité minimales sont déterminées dans la directive. La politique de sécurité de l'information est validée par le *« comité de coordination de la police intégrée »*, tel que visé à l'article 8*ter* de la LPI, après avis du *« comité Information et ICT »*. Les plans de sécurité, qui décrivent la politique de sécurité dans des termes concrets, sont par contre validés au niveau de la zone de police ou de l'entité de la police fédérale[12]. Le COC adhère à cette approche différenciée qui définit une politique de sécurité uniforme pour la police intégrée qui est concrétisée à l'échelon local et compte tenu du contexte, en fonction des moyens organisationnels et techniques des services de police.

12. Étant donné que le délégué à la protection des données (DPO[13]) est chargé du suivi de la politique de sécurité de l'information et de la mise en œuvre du (des) plan(s) de sécurité, le COC souligne que le responsable du traitement (opérationnel) doit veiller à ce que le DPO dispose des connaissances et de l'expertise requises dans le domaine du droit à la protection des données à caractère personnel et de la sécurité de l'information, et les entretiennent en suivant les formations (complémentaires) spécialisées. Il s'agit là d'une obligation tout à fait indépendante de l'obligation de sensibilisation, de formation et de communication des membres du personnel des services de police qui est définie dans la directive. Une bonne communication et une bonne entente entre le gestionnaire fonctionnel, le chef de corps ou directeur, les directeurs opérationnels et le DPO sont à cet égard primordiales. Or, l'Organe de contrôle constate dans la pratique que cet aspect se révèle parfois problématique.

13. L'objectif *« 3) la sécurité concernant les ressources humaines »* inclut la politique et les procédures en matière de recrutement, d'occupation et de résiliation ou modification du contrat de travail. Il convient de faire remarquer que ces aspects peuvent avoir trait à des traitements relevant de l'application du RGPD et du Titre 1er de la LPD. Cela peut prêter à confusion étant donné que la directive met en œuvre l'article 44/4 §2 de la LFP et a donc en principe exclusivement trait aux traitements opérationnels, à savoir des traitements qui ne relèvent pas du RGPD mais qui cadrent dans les missions de police administrative et judiciaire (*LED* et Titre II de la LPD). C'est le cas aussi des objectifs *« la gestion des actifs »* (sous-rubrique 5), *« l'acquisition, le développement et la maintenance des systèmes d'information »* (sous-rubrique 11) et *« les relations avec des tiers (fournisseurs, autorités) »* (sous-rubrique 12), qui ne sont pas nécessairement (entièrement) en

[11] Rubrique *« II. INTRODUCTION »*, p. 2.

[12] À savoir respectivement le chef de corps et le comité de direction de la police fédérale.

[13] *Data Protection Officer*.

rapport avec des traitements opérationnels. Si ces objectifs ont trait également à des traitements relevant du RGPD, l'auteur de la directive doit apporter de la clarté sur ce point, au moins en complétant en ce sens l'intitulé de la directive et en motivant et précisant ce point dans l'introduction de la directive.

14. Pour les règles relatives à l'accès aux données à caractère personnel et aux informations contenues dans les banques de données policières, la directive fait référence à une autre directive telle que visée à l'article 44/4 §3 de la LFP (la directive relative aux règles d'accès). Bien que le COC puisse comprendre cette distinction, on peut dans ce contexte se demander ce que l'on entend par les *« autres actifs ICT essentiels »*[14]. Si ce terme vise aussi des systèmes ou applications ne présentant aucun rapport avec des traitements opérationnels, l'auteur de la directive est prié de le préciser.

15. La directive s'attarde aussi brièvement, et dans des termes généraux, sur la cryptographie, l'utilisation des services dans le cloud et l'obligation de prendre en la matière les mesures de sécurité appropriées. Le COC attire dans ce contexte l'attention sur l'étude réalisée par le Contrôleur européen de la protection des données (EDPS), qui met en lumière quelques points problématiques dans la rédaction des contrats afférents à la prestation de services et aux produits de *Microsoft* fournis aux institutions de l'UE[15]. Des manquements ont notamment été constatés dans la convention de traitement, à savoir l'absence d'instructions claires à l'intention du sous-traitant et de contrôle sur les sous-traitants des sous-traitants auxquels *Microsoft* fait appel, le manque de droits d'audit pertinents pour le responsable du traitement, l'absence de garantie et de contrôle quant au lieu du traitement, les transferts internationaux des données et le risque de divulgation illicite des données, et enfin l'intégration de solutions techniques adéquates pour empêcher un flux non autorisé de données en direction de *Microsoft*. Autant de points cruciaux méritant toute l'attention, donc, et sous-entendant des risques importants et réels concernant la confidentialité effective, la disponibilité et l'intégrité des données policières (données à caractère personnel et informations). L'Organe de contrôle appelle dans ce contexte la GPI en général, et la DRI[16] de la police fédérale en particulier, à faire preuve d'une grande vigilance.

16. Sous la rubrique 10, la *« sécurité de la communication des informations »*, il est indiqué que des directives ministérielles distinctes ont été émises à cet égard. Le COC ignore de quelles directives ministérielles il est question, et elles n'ont pas non plus été soumises à l'Organe de contrôle pour avis.

17. Pour terminer, le COC ne comprend pas la portée de la dernière rubrique de la directive, intitulée *« IV. La méthodologie »*. Il est fait référence dans des termes généraux à « *la méthodologie* » sans

---

[14] La directive, p. 7 (*« 6) le contrôle d'accès »*).

[15] EDPS, "*Outcome of own-initiative investigations into EU institutions' use of Microsoft products and services* 2 juillet 2020, https://edps.europa.eu/data-protection/our-work/publications/papers/outcome-own-initiative-investigation-eu-institutions_en.

[16] Direction de l'information policière et des moyens ICT.

préciser concrètement en quoi celle-ci consiste, si ce n'est qu'elle doit s'appuyer sur la méthodologie prévue dans les *Baseline Information Security Guidelines* du Centre pour la Cybersécurité Belgique. Il convient de faire remarquer que ces *guidelines* n'avancent – ni ne concrétisent, comme nous le faisions remarquer au point 9 – aucune méthodologie spécifique. Il est par conséquent demandé à l'auteur de la directive d'apporter davantage de clarté à ce sujet.

18. Pour le reste, le COC n'a pas de remarques spécifiques à formuler.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

requiert le demandeur de donner suite aux remarques reprises aux points 10 à 17 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 22 septembre 2020.

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