ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
SPF Intérieur/Services de coordination et d'appui/ Cellule internationale	DA190016		14 octobre 2019

Objet : avis concernant l'Accord entre le Royaume de Belgique et la Géorgie relatif à la collaboration policière

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, § 1er, 2e alinéa, l'article 71, le titre 7 et 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").

Vu la demande du Ministre de la Sécurité et de l'Intérieur, Pieter De Crem, reçue par porteur par l'Organe de contrôle le 5 septembre 2019, d'émettre un avis conformément à la LPD susmentionnée.

Vu l'envoi ultérieur, par e-mail du SPF Intérieur le 1er octobre 2019, du modèle de convention sur lequel l'Accord précité se base, lequel n'avait pas été joint à la demande d'avis initiale et a été réclamé par l'Organe de contrôle.

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

Émet, le 10 octobre 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 LPD.

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. La demande porte sur l'Accord entre le Royaume de Belgique et la République de Géorgie relatif à la collaboration policière.

Pour éviter tout malentendu, l'Organe de contrôle rappelle qu'il ne limite pas nécessairement ses avis à l'article ou aux articles indiqué(s) par un demandeur mais qu'il tient toujours compte dans ses avis de tous les éléments ou dispositions qui relèvent de sa compétence en vertu de la réglementation susmentionnée. En l'occurrence, l'examen réalisé dans le présent avis dépassera le cadre du seul article 11 mentionné par le demandeur.

6. Le demandeur affirme que le texte de l'Accord se base sur ce qu'on appelle la "*convention-type en matière de collaboration policière*" approuvée par le Parlement et qui sert de base jusqu'à présent pour les accords de coopération bilatéraux avec ce qu'on appelle les "pays tiers" (à savoir des pays qui ne sont pas membres de l'Union européenne). Aux yeux de l'Organe de contrôle, l'utilité et la plus-value de ces formes de coopération bilatérale ne nécessitent aucune précision complémentaire et sont incontestables. Malgré l'utilisation d'une "convention-type", l'Organe de contrôle constate qu'il existe assez bien de différences importantes entre les différentes conventions policières conclues (voir ci-après).

7. Le champ d'application matériel (ce qu'on appelle les *"fields of cooperation"*, à savoir les domaines de coopération) est décrit à l'article 2 de manière non exhaustive. L'article 2.2 précise que la coopération entre les parties contractantes concerne la prévention, la détection, la répression des infractions pénales et l'enquête au sujet de ces dernières, et sont ensuite énumérées sans toutefois que la liste des infractions soit exhaustive, étant donné que la coopération concerne "principalement" (*"particularly"*) les faits énoncés.
L'article 2.3 prescrit que les infractions pénales qui ne sont pas définies à l'article 1 (on vise probablement "l'article 2.1") du projet d'accord seront examinées par les autorités compétentes conformément à leur législation nationale respective. Par ailleurs, le contenu concret recouvert par les

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

différentes infractions pénales qui sont énoncées à l'article 2.2, comme la criminalité organisée contre les biens *("organised property crime")*, les délits économiques et financiers *("economic and financial criminal offences")*, et les jeux de hasard illégaux (*"illegal games of chance"*), n'est pas clair, sujet à interprétation et très large. En outre, il est fait abstraction des cas dans lesquels il y a un écart entre la législation nationale respective des deux parties contractantes. On ne détermine pas si on applique la législation de l'état demandeur ou de l'état qui est sollicité en cas de différences quant à la qualification des faits en tant qu' "infractions pénales", et on ne prévoit rien non plus s'apparentant à une procédure de décision. Il faut au moins clarifier ces points et préciser l'interprétation des infractions non définies à l'article 2.2. Lorsque l'on parle par exemple de "criminalité organisée contre les biens", on ne sait pas clairement s'il s'agit de toutes les formes de vol ("theft") comme on les connaît dans le Code pénal belge. La question se pose par exemple de savoir comment il convient d'interpréter le caractère "organisé" de cette criminalité contre les biens. Se base-t-on à cet égard sur la définition des infractions organisées dans la Convention des nations Unies du 15 novembre 2000 contre la criminalité transnationale organisée, telle que mentionnée à l'article 1 ? Ou se réfère-t-on aux critères que l'on retrouve dans le commentaire de la convention type pour la "criminalité organisée" ? Il est important de clarifier les choses à cet égard en adaptant le texte du projet.

Le champ d'application à l'article 2 ne correspond pas tout à fait à l'article 7 qui fixe le champ d'application de l'échange de données. L'échange de données constitue toujours un des éléments centraux de tout accord en matière de coopération policière. À l'article 7.1, il est en effet question d'une assistance aux fins d'enquête sur "des infractions pénales" (*"criminal offences"*). On ne sait pas clairement si la notion d' "infractions pénales" (*"criminal offences"*) est plus large que le champ d'application prévu à l'article 2. En droit belge, on entend en effet par "*infractions pénales*" toutes les infractions (contraventions, délits et crimes) de droit commun ou de droit pénal spécial, qu'elles relèvent ou non de la "*criminalité organisée*".
À l'article 7.2 (échange d'informations d'initiative), on se réfère d'ailleurs à l'article 2 de cet Accord, mais aussi à d'autres menaces pour la sécurité ("Article 2 of this Agreement or of other security threats"). Le choix des termes *"such as"* (cf. art. 7.2) laisse entendre que les faits criminels énoncés à l'article 2 serviraient simplement d'exemple. L'ajout de ces "autres menaces pour la sécurité" implique en outre que la délimitation des infractions pénales visées en devient très vague et large. La formulation en question ne correspond d'ailleurs pas non plus avec le modèle de convention approuvé par le parlement, où l'ajout au champ d'application est limité à la prévention de *"menaces pour l'ordre et la sécurité publics"*. Étant donné qu'à l'article 10.2 a) concernant la désignation d'officiers de liaison, ces autres menaces pour la sécurité (*"other security threats"*) sont également reprises dans le cadre de l'échange de données, alors qu'on ne les retrouve de nouveau pas dans la version du modèle de convention approuvée par le parlement, ces "autres menaces pour la sécurité" doivent être définies (plus) clairement. L'interprétation de ce concept doit aussi être la même pour les deux articles.

Il est recommandé d'analyser à nouveau le projet de texte, non seulement sur la base du principe de légalité en matière pénale mais aussi du point de vue de la protection des données. L'Organe de contrôle souligne que les infractions énoncées à l'article 2.2 ne peuvent pas simplement servir d'exemple, mais qu'elles doivent constituer la délimitation du champ d'application de cet Accord, indépendamment de la question des infractions non définies, cette imprécision devant tout autant être résolue dans la mesure du possible (on peut s'inspirer par exemple de la Décision-cadre Mandat d'arrêt européen[7]) en prévoyant une description plus précise ou une description qui correspond aux textes existants (cf. note de bas de page 7). Par ailleurs, le champ d'application ne peut pas être déterminé à l'aide de la très large définition de l'article 7.1, qui est en tout état de cause en contradiction avec l'article 2. L'Organe de contrôle lit donc l'article 7.1 dans le sens prévu par l'article 2. Il est recommandé de reprendre les modifications nécessaires dans le projet de texte de l'Accord afin de mettre le champ d'application en conformité avec les exigences de protection des données.

Cela signifie que l'Organe de contrôle, dans le cadre de sa fonction de contrôle (voir les articles 44/1 à 44/11/13 inclus de la LFP) et dans le cadre de sa fonction de DPA (article 71 et Titre 7 de la LPD), veillera également à ce que l'échange réciproque de données s'inscrive bel et bien dans le cadre de l'article 2 de l'Accord et qu'il n'y ait donc pas d'échange d'informations avec la Géorgie pour n'importe quelle "infraction".

8. L'article 5.1 indique quelles sont les autorités compétentes des parties contractantes ("*competent authorities of the Contracting Parties*"). Pour le Royaume de Belgique, on se réfère en des termes généraux à la Police intégrée belge, structurée à deux niveaux ("*The Belgian Integrated Police, structured at two levels*"). Cela ne permet pas de déduire qui est le responsable du traitement, étant donné que cette description comprend en principe chaque service de police (zone de police ou entité de la police fédérale). Lorsque l'on confronte cela à la désignation claire par la Géorgie du Ministère de l'Intérieur, de la Sûreté de l'État et du Service d'enquêtes du Ministre des Finances en tant qu'autorités compétentes, il est indéniablement nécessaire de prévoir une désignation plus spécifique des autorités compétentes pour le Royaume de Belgique afin que l'identité du responsable du traitement soit connue.

9. Au point IV "Échange d'informations" ("Exchange of information"), l'Accord développe plus en détails l'échange de données. L'article 6 précise qu'il s'agit d'une coopération étroite et permanente ("close and permanent cooperation"), l'article 7 parle entre autres de prévention et de détection d'infractions pénales ("preventing, detecting") et tant l'article 8 que l'article 9 indiquent indirectement que des informations sont fournies sur demande. À cet égard, le COC s'interroge toutefois sur les types d'échanges de données qui relèvent du présent Accord. Il est recommandé que l'Accord précise

---

[7] 2002/584/JAI : Décision-cadre du Conseil du 13 juin 2002 *relative au mandat d'arrêt européen et aux procédures de remise entre États membres - Déclarations de certains États membres sur l'adoption de la décision-cadre.*

s'il s'agit simplement d'un échange d'informations sur demande dans le cadre d'une enquête en cours, ou si un échange de données spontané est également possible sur la base de cet Accord, la partie contractante qui envoie les informations faisant observer que certaines affaires peuvent être pertinentes pour la partie qui les reçoit, sans qu'il soit pour cela nécessaire qu'une enquête soit en cours. La manière dont les données circulent n'est pas claire non plus. Cela se fait-il à des moments fixes dans les deux sens, ou plutôt au cas par cas ? Un échange de données automatique (ou une forme d'échange de données automatique) peut-il (elle) être fondé(e) sur cet Accord ? La manière dont les choses se passent au niveau opérationnel doit être précisée dans le texte de l'Accord afin de garantir que les principes de protection des données seront respectés.

10. L'article 11 traite spécifiquement de la protection des données à caractère personnel. Le transfert de données à caractère personnel dans le cadre de la collaboration policière avec des pays tiers est actuellement régi par les articles 66 à 70 inclus de la LPD. En l'occurrence, à défaut d'une décision d'adéquation pour la Géorgie, le fondement juridique du transfert se trouve à l'article 68, § 1, 1e alinéa de la LPD qui dispose ce qui suit : "*En l'absence de décision d'adéquation, visée à l'article 67 (...), un transfert de données à caractère personnel vers un pays non membre de l'Union européenne ou à une organisation internationale peut avoir lieu lorsque :*
1° des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant ; ou
2° le responsable du traitement a évalué toutes les circonstances du transfert de données à caractère personnel et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.".

Le point 1° serait en l'occurrence d'application sur la base d'un accord de coopération. La question se pose ensuite de savoir si l'article 11, en tant que seul article traitant de la protection des données, prévoit des "garanties appropriées". À la lecture du texte, le COC estime que c'est en principe le cas. Dans ce cadre, le traitement de données à caractère personnel est soumis, à l'article 11.1, respectivement à la législation nationale et aux obligations internationales de chaque partie contractante ("*the processing [...] of personal data are subject tot he respective national legislations and international obligations of each Contracting Party*"), dans le droit belge en vigueur, il s'agit entre autres et avant tout de la LPD du 30 juillet 2018.
À l'article 11.2, les parties contractantes garantissent ensuite un niveau de protection des données à caractère personnel qui correspond aux dispositions de la Convention 108 pour la protection des données, du protocole additionnel du 8 novembre 2001 à la Convention de protection des données précitée, et de la Recommandation R (87) 15 du 17 septembre 1987 du Comité des Ministres du Conseil de l'Europe qui régit l'utilisation de données à caractère personnel à des fins de police.

En ce qui concerne la Convention n° 108 du Conseil de l'Europe pour la protection des données, on peut faire remarquer que le texte a entre-temps été modernisé (voir https://www.coe.int/fr/web/data-

protection/convention108/modernised) et que la Géorgie, contrairement à la Belgique (signature le 10 octobre 2018), n'a pas encore signé ce texte de protocole d'amendement[8]. Bien que l'entrée en vigueur de ce protocole ne soit pas attendue dans un avenir proche[9], il appartient aux autorités belges de surveiller attentivement la situation et, le cas échéant, de rappeler à la Géorgie la nécessité de signer et de ratifier le protocole susmentionné.

Ceci étant dit, le renvoi, dans le préambule de l'Accord avec la Géorgie, à la Convention pour la protection des données n'englobe pas le protocole additionnel du 8 novembre 2001 à cette convention qui a été signé par la Belgique le 30 avril 2002. Bien que jusqu'à présent, ce protocole additionnel ait bien été ratifié par la Géorgie mais pas par la Belgique[10] et ne constitue dès lors pas un "droit applicable", il a une grande valeur étant donné qu'il ajoute à la Convention pour la protection des données l'obligation d'installer une autorité de contrôle à laquelle des compétences effectives doivent être confiées. Vu l'applicabilité de la LPD belge, le manque de ratification n'est pas juridiquement insurmontable, mais il est à tout le moins recommandé de reprendre ce protocole. À défaut, le protocole ne pourra pas être appliqué au moment de la ratification de l'Accord avec la Géorgie, ce qui n'est pas souhaitable.

En outre, plusieurs obligations complémentaires (reprises aux points 1 à 10 inclus) sont prévues. Le présent projet prévoit des garanties au niveau de :

- L'exactitude des données, une éventuelle correction en cas d'erreurs et une limitation du traitement (article 11.9).
- Le principe de finalité et le principe de spécialité (article 11.3 b).
- La communication ultérieure des données (article 11.6 c, bien qu'on y fasse inutilement référence au § 4).
- Le droit d'information, d'accès, de rectification et d'effacement pour la personne concernée conformément au droit national, le cas échéant exercé par une requête auprès de l'autorité de contrôle (article 11.5).
- La stricte nécessité de traiter des catégories particulières de données (article 11.7).
- L'enregistrement de l'envoi et de la réception de données à caractère personnel (ainsi que d'autres informations) (article 11.6 a).
- Des mesures techniques et organisationnelles (mesures de sécurité de l'information) afin de pouvoir contrôler l'input, l'utilisation, l'accès et la conservation de données à caractère personnel, ainsi que la fiabilité du système (article 11.10).
- L'intervention des autorités de contrôle (articles 11.11 et 11.12).

---

[8] Situation au 28.01.2019, qui peut être consultée à l'adresse suivante : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/223/signatures.

[9] Voir à ce sujet DEBEUCKELAERE, W. et VERMEULEN, G., Codes annotés, Privacy, Larcier, 2018, p. 9

[10] Situation au 09.10.2019 ; consulté à l'adresse suivante : https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/181/signatures?p_auth=IWro5Xq8.

- La responsabilité de dommages découlant d'une violation des droits issus de l'Accord (article 11.12).

11. En ce qui concerne le délai de conservation, l'article 11.3 dispose que les données à caractère personnel seront conservées pour une durée ne dépassant pas celle qui est nécessaire aux finalités de traitement envisagées, sous une forme qui permet l'identification des personnes concernées ("*no longer than necessary for the purposes for which they are processed*"). On retrouve une même formulation au paragraphe 1 de l'article 11.8 au sujet des données à caractère personnel reçues par les autorités compétentes, en application de l'Accord. Si cela est clair pour la Belgique, étant donné que les délais de conservation sont mentionnés dans la LFP, l'Organe de contrôle estime que cela n'est absolument pas clair pour le droit géorgien. Les explications à ce sujet doivent au moins fournir suffisamment d'informations ; il est cependant recommandé de se référer dans le texte de l'accord à un *minimum minimorum* qui vaut pour les deux parties contractantes, étant donné que la législation nationale peut être modifiée ou abrogée unilatéralement. Concrètement, par exemple dans le cas de données à caractère personnel de suspects belges qui sont transmises à la Géorgie, on ne sait pas clairement combien de temps ces données y seront (pourront y être) conservées.
Selon le projet de paragraphe 2 de l'article 11.8, la nécessité de poursuivre la conservation sera évaluée au plus tard trois ans après l'envoi des données ("*The need for continued storage shall be reviewed no later than 3 years after transmission*"). D'après le projet de texte, une telle évaluation peut être répétée après une nouvelle période de trois ans. On y ajoute : "si c'est encore nécessaire à l'exécution de leurs tâches" (*"if that is still necessary for the performance of its tasks"*). Pour le bon ordre, le COC note que cette dernière phrase ne concerne pas l'évaluation proprement dite ("review") mais bien la conservation des données à caractère personnel ("storing the personal data").
Étant donné que les délais de la LFP[11] s'appliquent ici (l'article 11.1 déclare en effet la législation nationale d'application) et que le traitement de données à caractère personnel comprend également les données qui sont traitées dans le cadre de la coopération policière internationale en matière pénale[12], il est important d'y adapter le texte de l'Accord. En ce sens, il est nécessaire de clarifier les délais maximaux applicables pour la ventilation des données échangées.

Au niveau de l'effacement des données, la formulation utilisée dans l'Accord de police avec le Monténégro est plus claire. L'article 3.d), c. affirme que les données à caractère personnel reçues seront effacées, détruites ou corrigées si "*les données ne sont plus nécessaires à l'exécution de la mission pour laquelle elles ont été transférées à l'origine, à moins que l'utilisation de ces données à d'autres fins ne soit clairement autorisée*". L'article 11.3.d), 3e astérisque de la convention policière avec la Macédoine prévoit aussi une suppression des données lorsqu'elles "*n'étaient plus nécessaires pour l'exécution de la mission pour laquelle elles avaient été transférées, à moins qu'une autorisation*

[11] Article 44/9 de la LFP
[12] Article 44/5, § 5 de la LFP

explicite n'ait été délivrée en vue de l'utilisation de ces données à d'autres fins". L'article 11.3.e) affirme même que "*la Partie contractante en charge du transfert des données* [doit informer] *l'autre Partie contractante du délai de conservation conformément à la législation nationale de l'État ou au droit international*" et aussi : "*Indépendamment du délai de conservation, les données à caractère personnel ne peuvent être conservées plus longtemps que nécessaire dans le cadre des objectifs fixés. La Partie contractante en charge du transfert doit être informée de la suppression des données soumises à la transmission, ainsi que des motifs de cette suppression".* Le COC estime que la convention policière avec la Macédoine est beaucoup plus claire au niveau des délais de conservation et offre une plus grande protection juridique. Il encourage dès lors le Gouvernement à utiliser ces formulations à l'avenir.

12. En ce qui concerne l'adaptation ou la suppression de données inexactes, l'article 11.9 prescrit que l'autorité compétente qui a des raisons de penser que les données envoyées vers (paragraphe 1) ou reçues (paragraphe 2) de l'autre autorité compétente sont incorrectes, ne sont pas exactes, sont désuètes ou n'auraient pas dû être envoyées, en informe l'autre autorité compétente. L'autorité compétente en question adapte les données à caractère personnel ou les supprime. La manière dont cette disposition est formulée actuellement laisse toutefois une trop grande marge d'appréciation : l'adaptation de données incorrectes ou inexactes doit se faire immédiatement et avoir un caractère contraignant, ce qui ne ressort pas actuellement de la formulation tant du premier que du deuxième paragraphe de l'article de l'accord. Une adaptation du texte en ce sens est ici nécessaire.
D'ailleurs, les autorités compétentes des deux parties contractantes disposent des données précitées et l'article de l'accord doit dès lors imposer aux deux parties contractantes l'obligation d'adapter ou d'effacer ces données.

13. En ce qui concerne les mesures techniques et organisationnelles précitées de l'article 11.10, il convient de souligner, en l'absence d'un projet d'Exposé des motifs (qui doit toutefois normalement faire partie des documents soumis à l'avis du COC), que ces mesures doivent permettre que les données à caractère personnel ne soient par défaut pas mises à disposition d'un nombre illimité de personnes physiques sans intervention de la personne physique. Ces mesures visent à garantir la sécurité des données à caractère personnel de manière à ce qu'elles soient protégées notamment contre un traitement non autorisé ou illicite (ce qui inclut notamment un accès non autorisé, une destruction accidentelle ou illicite, une publicité et des dégâts d'origine accidentelle).

14. Aux articles 11.11 et 11.12 du projet d'accord, des imprécisions subsistent quant au rôle et à l'intervention des autorités de contrôle. Tout d'abord, l'Accord évoque le fait de prévoir des autorités publiques indépendantes, responsables de la surveillance du traitement de données à caractère personnel en vertu du présent Accord ("*independent public authorities to be responsible for monitoring the processing of personal data on the basis of this Agreement*"), afin de protéger les droits et libertés

fondamentaux des personnes physiques concernées. En outre, les autorités de contrôle respectives collaboreront à cet effet. Toutefois, l'article 11.12 revient ensuite sur le droit de porter plainte auprès de cette autorité de contrôle, en se référant à l'article 11.11, qui reste cependant totalement muet sur un droit de porter plainte. Il est recommandé à cet égard de concrétiser davantage ce droit de porter plainte à l'article 11.11. Il serait d'ailleurs opportun que la Belgique et la Géorgie se communiquent réciproquement quelles autorités ou quels organes sont responsables de cette surveillance.

15. En ce qui concerne l'article 11.6 d), il va de soi qu'en droit belge, la police intégrée ne peut en principe jamais donner une autorisation de manière indépendante d'utiliser des données à caractère personnel qui relèvent du présent Accord pour d'autres finalités, mais qu'elle doit disposer à cet effet de l'autorisation des autorités compétentes, comme le ministère public.

16. L'article 12 concerne l'échange de données via un officier de liaison. On peut toutefois interpréter cet article de différentes manières. La phrase indiquant que les dispositions de l'Accord ne s'appliqueront pas sauf si l'officier de liaison communique ces données à la partie contractante auprès de laquelle il a été détaché ("*this Agreement shal not apply unless the law enforcement representative communicates such data to the Contracting Party to which they are seconded*") ne signifie nullement que les dispositions en matière de protection des données peuvent être écartées pour autant qu'un échange de données ait lieu hors du détachement mais dans le cadre du champ d'application du présent Accord. À cet égard, le COC souligne que le rôle de l'officier de liaison dans l'échange de données ne peut aucunement porter atteinte à la responsabilité des parties contractantes en matière de protection des données à caractère personnel. La plus-value de cette phrase échappe au COC. Que l'échange de données ait lieu directement ou via un officier de liaison, les dispositions de cet Accord et la loi belge doivent être appliquées.

17. Conformément à l'article 14.1, toute partie contractante peut refuser une assistance lorsqu'il apparaît que cela pourrait être contraire à la législation nationale ("*Each Contracting Party may refuse assistance if it turns out to be against its national legislation*"). Le COC souligne que cette disposition de l'accord concerne aussi les violations flagrantes des principes de protection des données à caractère personnel, en se référant à la législation énoncée ci-avant qui concrétise ces principes.

18. L'article 19.2 prescrit la manière dont une partie contractante peut résilier cet Accord. La fin de cet Accord doit également marquer la fin du traitement des données qui sont enregistrées/échangées en vertu ou en exécution de cet Accord. Il est non seulement recommandé de modifier le texte en ce sens, mais il est aussi souhaitable qu'une notification proprement dite de la fin de l'Accord le rappelle également.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

demande qu'il soit tenu compte des remarques susmentionnées ;

demande qu'il soit donné suite aux prescriptions formulées aux points 7 à 18 inclus.

Avis approuvé par l'Organe de contrôle de l'information policière le 14 octobre 2019.

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

Frank SCHUERMANS
Lid van het COC
Membre du COC