

CONTRÔLE GLOBAL

RAPPORT DE SUIVI CONCERNANT LE CONTRÔLE GLOBAL ET LA VISITE EFFECTUÉS AUPRÈS D'UNE ZONE DE POLICE DE LA PROVINCE DE FLANDRE ORIENTALE PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LE CADRE DE SES COMPÉTENCES DE CONTRÔLE ET DE SURVEILLANCE

VERSION PUBLIQUE

Référence : CON19002/1

**ORGANE DE CONTROLE DE
L'INFORMATION POLICIERE**



TABLE DES MATIÈRES

| | |
|---|---|
| 1. INTRODUCTION | 3 |
| 1.1. Les compétences de l'Organe de contrôle | 3 |
| 1.2. Objectifs | 4 |
| 2. LA VISITE DE SUIVI | 4 |
| 4. CONCLUSIONS DE L'ENQUÊTE | 5 |
| 5. CONCLUSION | 6 |

1. INTRODUCTION

1.1. Les compétences de l'Organe de contrôle

1. La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)¹ a réformé l'Organe de contrôle de l'information policière en une autorité de contrôle à part entière, en marge de ses compétences de contrôle existantes en matière de gestion de l'information policière telles que prévues par la loi du 5 août 1992 sur la fonction de police (LFP). L'article 71 §1^{er} et les chapitres II et III de la LPD décrivent les missions et les compétences du COC. Il est dans ce contexte fait référence par ailleurs aux missions de contrôle visées aux articles 44/1 à 44/11/14 inclus de la LFP, relatifs à la gestion de l'information par les services de police. L'Organe de contrôle est ainsi investi d'une mission de surveillance et de contrôle, ce qui signifie qu'en marge de la protection de la vie privée et des données, le COC prête également attention à des éléments comme l'efficacité et l'efficacité de la gestion de l'information et de l'intervention policière. Le COC a dès lors en vertu de la réglementation susmentionnée une compétence générale de surveillance à l'égard de tous les traitements opérationnels et non opérationnels de données (à caractère personnel) par la GPI.

L'Organe de contrôle est compétent pour les services de police², pour l'inspection générale de la police fédérale et de la police locale (AIG)³ et pour l'unité d'information des passagers (BEL-PIU)⁴. La compétence de surveillance de l'Organe de contrôle à l'égard des services de police couvre à la fois les activités de traitement opérationnelles et non opérationnelles.⁵

Pour ce qui est de la mission de contrôle, l'Organe de contrôle est chargé du contrôle du traitement des informations et des données visées à l'article 44/1 de la LFP, y compris celles introduites dans les banques de données visées à l'article 44/2, ainsi que de toute autre mission qui lui est confiée par ou en vertu d'autres lois.

Dans ce cadre, le COC procède aux constatations et peut formuler des questions, des recommandations, des avertissements et/ou des mesures correctrices (au caractère contraignant) en tant que « *ultimum remedium* » si le COC constate des infractions aux lois et règlements.

L'Organe de contrôle est en particulier chargé du contrôle du respect des règles relatives à l'accès direct à la Banque de données nationale générale (BNG) et à sa consultation directe, ainsi que du respect de l'obligation visée à l'article 44/7, 3^e alinéa de la LFP, qui oblige tous les membres des services de police à alimenter cette banque de données.

À travers une inspection du fonctionnement, l'Organe de contrôle vérifie si le contenu de la BNG et la procédure de traitement des données et informations qui y sont conservées sont conformes aux dispositions des articles 44/1 à 44/11/14 de la LFP et à leurs mesures d'exécution.

Dans le cadre de l'utilisation de caméras non visibles, l'Organe de contrôle fonctionne en quelque sorte comme une commission « MAP »⁶. Conformément à l'article 46/6 de la LFP, toute autorisation et prolongation d'utilisation non visible de caméras dans les cas visés à l'article 46/4 doit être notifiée à l'Organe de contrôle sauf lorsque l'utilisation des caméras est réalisée sous le contrôle d'un magistrat. L'Organe de contrôle doit alors examiner si les conditions pour la décision, la prolongation ou l'exécution de cette mesure sont remplies.

L'Organe de contrôle prend en outre connaissance des plaintes et statue sur leur bien-fondé⁷. Les membres de l'Organe de contrôle et les membres du Service d'Enquête (DOSE)⁸ de l'Organe de contrôle disposent à cet égard de compétences d'investigation et peuvent prendre des mesures correctrices⁹.

¹ M.B. 5 septembre 2018. Cette loi contient des dispositions qui donnent exécution au 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), ci-après dénommée « RGPD » et la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après dénommée « directive Police-Justice » ou LED (Law Enforcement Directive)).

² Tels que définis à l'article 2, 2^o de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (art. 26, 7^o, a de la LPD).

³ Telle que définie à l'article 2 de la loi du 15 mai 2007 sur l'Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police (art. 27, 7^o, d de la LPD).

⁴ Telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers (art. 26, 7^o, f de la LPD), également désignée en tant que 'BEL-PIU' (*Belgian Passenger Information Unit*).

⁵ Art. 4 §2, 4^e alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

⁶ MAP signifie « méthodes administratives particulières ».

⁷ Art. 240, 4^o de la LPD.

⁸ Dienst Onderzoeken / Service d'Enquête.

⁹ Art. 244 et 247 de la LPD.

Un recours juridictionnel peut être introduit dans les trente jours contre certaines décisions de l'Organe de contrôle devant la Cour d'appel du domicile ou du siège du demandeur qui traite l'affaire selon les formes du référé conformément aux articles 1038, 1040 et 1041 du Code judiciaire¹⁰.

1.2. Objectifs

2. La surveillance vise d'une part à se faire une idée de l'application du cadre légal relatif au traitement de données à caractère personnel et d'autre part à attirer l'attention de l'entité contrôlée sur la sécurité de l'information. La compétence de contrôle est quant à elle plutôt axée sur le respect des processus de travail et des procédures. Les deux compétences ont néanmoins comme point commun que des données à caractère personnel sont traitées.

La surveillance porte sur les aspects organisationnels, à savoir les différentes étapes du processus et leur timing. Il est vérifié dans ce contexte si les activités de traitement satisfont au cadre légal du RGPD, de la LPD et de la LFP ainsi qu'aux exigences en matière de sécurité de l'information en ce qui concerne la structure, les processus de traitement et les systèmes.

Lorsque des mesures correctrices sont imposées et/ou des recommandations formulées dans le sillage d'une visite, l'Organe de contrôle en assure le suivi. Le suivi des mesures correctrices, des requêtes et des recommandations qui sont respectivement imposées et formulées dans le sillage d'une visite porte sur le compte rendu, à l'Organe de contrôle, de l'état d'avancement de la mise en œuvre (selon les délais imposés par le rapport).

Une visite de suivi a pour objectif de vérifier dans quelle mesure les aspects introduits ou adaptés en fonction des mesures correctrices, requêtes et/ou recommandations formulées sont effectivement mis en œuvre dans la pratique.

Une enquête de suivi n'est pas systématiquement réalisée après une visite. La décision d'y procéder ou non est prise au cas par cas et de manière autonome par l'Organe de contrôle sur la base des constatations spécifiques de la visite initiale et des mesures correctrices, requêtes et/ou recommandations en découlant, en fonction des circonstances spécifiques, de l'évolution dans le temps et dans l'espace de la thématique ou de certains de ses aspects spécifiques.

2. LA VISITE DE SUIVI

3. Le 8 juillet 2021, l'Organe de contrôle a effectué une visite de suivi auprès d'une zone de police locale de la province de Flandre orientale (ci-après dénommée « la ZP Flor »). Cette visite de suivi faisait suite à une visite initiale effectuée le 20 juin 2019 par l'Organe de contrôle auprès de cette zone de police. Le contrôle initial effectué auprès de la zone de police locale de la province de Flandre orientale était une visite spontanée qui s'inscrivait dans le cadre d'un contrôle dit global¹¹. La visite ne faisait donc pas suite à une plainte (individuelle) ni ne découlait de l'existence d'indications (concrètes) d'un non-respect, par la zone de police visitée, de la législation et de la réglementation. Il avait été opté pour un contrôle global dans la largeur, ce qui signifie que le contrôle portait sur plusieurs thèmes sans approfondir trop chacun des différents thèmes abordés. Le contrôle consacrait une attention particulière à l'application du cadre juridique de la protection des données.

La visite portait sur cinq thèmes :

- 1) l'utilisation de caméras ;
- 2) le contrôle de la gestion des données et informations contenues dans la BNG ;
- 3) les banques de données particulières ;
- 4) les systèmes de contrôle du personnel ;

¹⁰ Art. 248 de la LPD.

¹¹ Le COC distingue plusieurs formes de contrôles ou de surveillance. Le COC procède soit à un :

- **Contrôle global** : il s'agit d'un contrôle qui s'assortit d'une ou plusieurs visites approfondies sur place et d'une portée très large.
- **Contrôle thématique** : comme le nom l'indique, il s'agit d'une enquête menée sur un thème déterminé et qui peut inclure à la fois de la *desk research* et des visites sur place.
- **Contrôle technique** : ces contrôles se concentrent principalement sur la licéité, l'exhaustivité et l'exactitude des enregistrements et traitements effectués dans les banques de données policières.
- **Contrôle restreint** : ces contrôles portent sur un seul ou sur quelques aspects (partiels) d'un traitement de données policier ou non policier.
- **Contrôle international** : il s'agit des éventuelles enquêtes internationales auxquelles le COC apporte son concours.
- **Contrôle spécial** : il s'agit d'enquêtes et de contrôles portant sur des matières particulières, comme les contrôles annuels des banques de données communes terrorisme et extrémisme.

5) la sécurité de l'information : l'organisation, la politique et la gestion des TIC.

Partant d'une approche générique, ce contrôle s'est concentré sur la gestion de l'information des données policières, sur la protection des données dans le cadre des finalités tant opérationnelles (LFP) que non opérationnelles (RGPD), sur la sécurité de l'information et sur le rôle actif du délégué à la protection des données (en anglais *DPO* pour « *data protection officer* »).

5. Pour résumer, le rapport de contrôle du 7 janvier 2020 concluait¹² qu'un nombre minime d'aspects des thèmes contrôlés étaient (entièrement) conformes à la législation. Un certain nombre de manquements à l'égard des dispositions légales avaient d'autre part été constatés. Pour ce qui est des aspects dominant clairement le thème de la protection des données, il s'était avéré que la ZP Flor ne disposait pas des connaissances spécifiques requises pour apporter une réponse adéquate dans certaines matières sensibles. En dépit de l'engagement manifeste des membres du personnel désignés à consentir dans ce domaine les efforts nécessaires, il se révélait impossible de consacrer suffisamment de temps, en marge des tâches policières journalières, à des formations spécialisées. Ce constat ne pouvait pas être entièrement compensé par l'assistance du DPO telle qu'elle pouvait être fournie concrètement à ce moment.

Le constat général qui précède reflétait l'ampleur des manquements concrets constatés. Bien qu'un certain nombre de directives aient été élaborées à l'échelle du corps sur le thème de la sécurité de l'information, la zone de police ne disposait pas d'un plan général de sécurité et de continuité de l'information reposant sur le risque à partir duquel l'organisation, et en particulier le service TIC, aurait pu distiller ses propres mesures. Une telle approche reposant sur le risque aurait permis d'évaluer, formaliser et documenter les mesures prises. Le service TIC de la zone de police prévoyait une série d'initiatives de sécurisation de l'information et de la communication, mais le contrôle périodique (interne/externe) du bon fonctionnement et de l'exhaustivité de ces initiatives n'était pas exercé de manière structurelle et formelle.

Le DPO devait aussi être davantage impliqué dans le suivi, l'adaptation et la mise en œuvre de la politique de sécurité de l'information et de protection des données. Une approche structurelle et un suivi périodique étaient à cet égard indiqués.

6. Quinze recommandations avaient dès lors été formulées pour contribuer à améliorer l'efficacité et l'effectivité du traitement des données (à caractère personnel) réalisé par la zone de police de la province de Flandre orientale. Les manquements constatés à l'égard des dispositions légales avaient en outre contraint l'Organe de contrôle à prendre six mesures correctrices auxquelles la zone de police de la province de Flandre orientale devait donner suite dans un délai bien défini afin de régulariser la situation.

3. CONCLUSIONS DE L'ENQUÊTE

7. Comme exposé ci-avant, l'objectif de la visite de suivi est de vérifier si l'état d'avancement rapporté est mis en œuvre de manière effective et dynamique par la zone de police et porte ses fruits.

8. L'Organe de contrôle a pu constater que le chef de corps apporte activement son concours pour faire de la sécurité de l'information et de la protection des données des processus efficaces. Cela implique notamment que les tâches et responsabilités sont attribuées à certaines personnes afin de donner forme à l'organisation (virtuelle) de la sécurisation au sein de la zone de police.

9. Le compte rendu peut être qualifié de parfait, non seulement grâce à la cohérence du compte rendu en lui-même, mais surtout parce que la zone de police a consenti des efforts financiers et organisationnels particuliers pour maximaliser l'assistance offerte au DPO pour tous les aspects des manquements ou lacunes constaté(e)s lors du contrôle. Le DPO peut dans ce contexte compter sur le soutien d'un vaste groupe de travail qui a été mis en place au sein de la zone de police, de sorte que la politique peut être effectivement mise en œuvre dans la pratique. Cette stratégie porte manifestement ses fruits.

10. Lors de la visite de suivi, l'Organe de contrôle a soumis au DPO et au groupe de travail plusieurs cas pratiques (réels) sur lesquels la zone de police avait déjà anticipé ou pour lesquels les instruments de politique (règlements et code de conduite) atteignent une certaine maturité.

11. En ce qui concerne l'aspect de la protection des données, des démarches importantes ont été entreprises sur le plan de la sensibilisation, de la formation, de la prise de conscience et des droits des personnes concernées (les membres du personnel). C'est également le cas en ce qui concerne les banques de données qui sont accessibles à la zone de police et les traitements découlant de la surveillance par caméra. La surveillance par caméra a été entièrement inventoriée et fait l'objet d'une gestion consciencieuse.

¹² Pour un exposé détaillé des conclusions, il est fait référence au rapport de visite et de contrôle du 7 janvier 2020.

12. Un instrument de politique très efficace a été mis au point pour attribuer de manière différenciée les droits d'accès et profils pour les banques de données et en assurer un suivi minutieux. Les critères sur la base desquels les droits sont attribués en fonction des profils correspondants ont été objectivés et définis de manière logique en prenant comme point de référence l'effectif du personnel. Le principe appliqué lors de la détermination des droits d'accès en fonction des rôles est celui du « pourquoi ? », au lieu de celui du « pourquoi pas ? ».

13. Notamment à cet égard, la zone de police procède régulièrement à des contrôles périodiques de la licéité des consultations des banques de données auxquelles la zone de police a accès. Ce monitoring fait systématiquement l'objet d'un compte rendu auquel il est le cas échéant donné suite. Bien que la zone de police lance de cette manière un signal très important au personnel, l'Organe de contrôle insiste pour que ce monitoring périodique ne soit pas limité au cas par cas à une certaine banque de données, mais englobe au contraire plusieurs banques de données (opérationnelles).

14. Sur le plan de la gestion de l'information, la validation centrale de la BNG fait l'objet d'un suivi consciencieux dans le cadre duquel la zone de police parvient à maintenir le nombre de rejet à 30 lignes en moyenne, alors que ce nombre était beaucoup plus élevé lors de la visite effectuée en 2019.

15. La zone de police a élaboré à l'échelle du corps des directives sur le thème de la sécurité de l'information et dispose désormais d'une politique et d'un plan de sécurité de l'information reposant sur le risque à partir duquel l'organisation, et en particulier le service TIC, peut distiller ses propres mesures. Une telle approche reposant sur le risque permet d'évaluer, formaliser et documenter les mesures prises. Le service TIC de la zone de police prévoit une série d'initiatives de sécurisation de l'information et de la communication et procède périodiquement à un contrôle (interne/externe) du bon fonctionnement et de l'exhaustivité de ces initiatives.

16. L'adaptation et la mise en œuvre de la politique de sécurité de l'information et de protection des données se sont clairement intensifiées. À travers des évaluations de la maturité et un plan d'action, la zone de police a initié un processus itératif visant à surveiller en permanence les risques en matière de sécurité de l'information et de protection des données et à les actualiser au besoin. La zone de police a procédé à une première itération de ce processus et a mis en œuvre à cette occasion une première série de mesures destinées à réduire les risques identifiés et à satisfaire aux recommandations formulées dans le rapport initial du COC. La zone de police semble donc avoir mis en place une approche structurelle et un suivi périodique lui offrant les armes idéales pour continuer à l'avenir à faire face aux risques résiduels en matière de sécurité de l'information. La sécurité de l'information n'est en effet pas une activité unique (projet), mais bien un processus d'amélioration continu et itératif.

4. CONCLUSION

17. Il ressort de ce qui précède que toutes les mesures correctrices ont été mises en œuvre. Pour ce qui est des recommandations, 80 % d'entre elles ont été mises en œuvre ou en sont à un stade très avancé de leur réalisation.

18. Pour ce qui est des aspects dominant clairement le thème de la protection des données, il s'avère que la zone de police de la province de Flandre orientale nourrit l'ambition d'apporter une réponse dans certaines matières sensibles.

19. En ce qui concerne la protection des données et la sécurité de l'information, un processus a clairement été mis en place pour gérer et surveiller les risques. Bien que quelques démarches doivent encore être finalisées, en particulier sur le plan de la sécurité de l'information, les efforts fournis jusqu'à présent sont impressionnants.

PAR CES MOTIFS,

L'Organe de contrôle de l'information policière,

Conclut que la zone de police de Flandre orientale fait montre pour tous les thèmes épinglés lors du contrôle global initial de connaissances étendues et d'une application effective de toutes les recommandations et mesures correctrices dans le fonctionnement journalier de la zone de police.

Considère par conséquent le contrôle global auprès de la zone de police de la province de Flandre orientale comme entièrement clôturé.

Ainsi décidé par l'Organe de contrôle de l'information policière le 14 septembre 2021.

Pour l'Organe de contrôle,

Koen Gorissen
Membre-conseiller
(SIGNÉ)

Frank Schuermans
Membre-conseiller
(SIGNÉ)

Philippe Arnould
Président
(SIGNÉ)