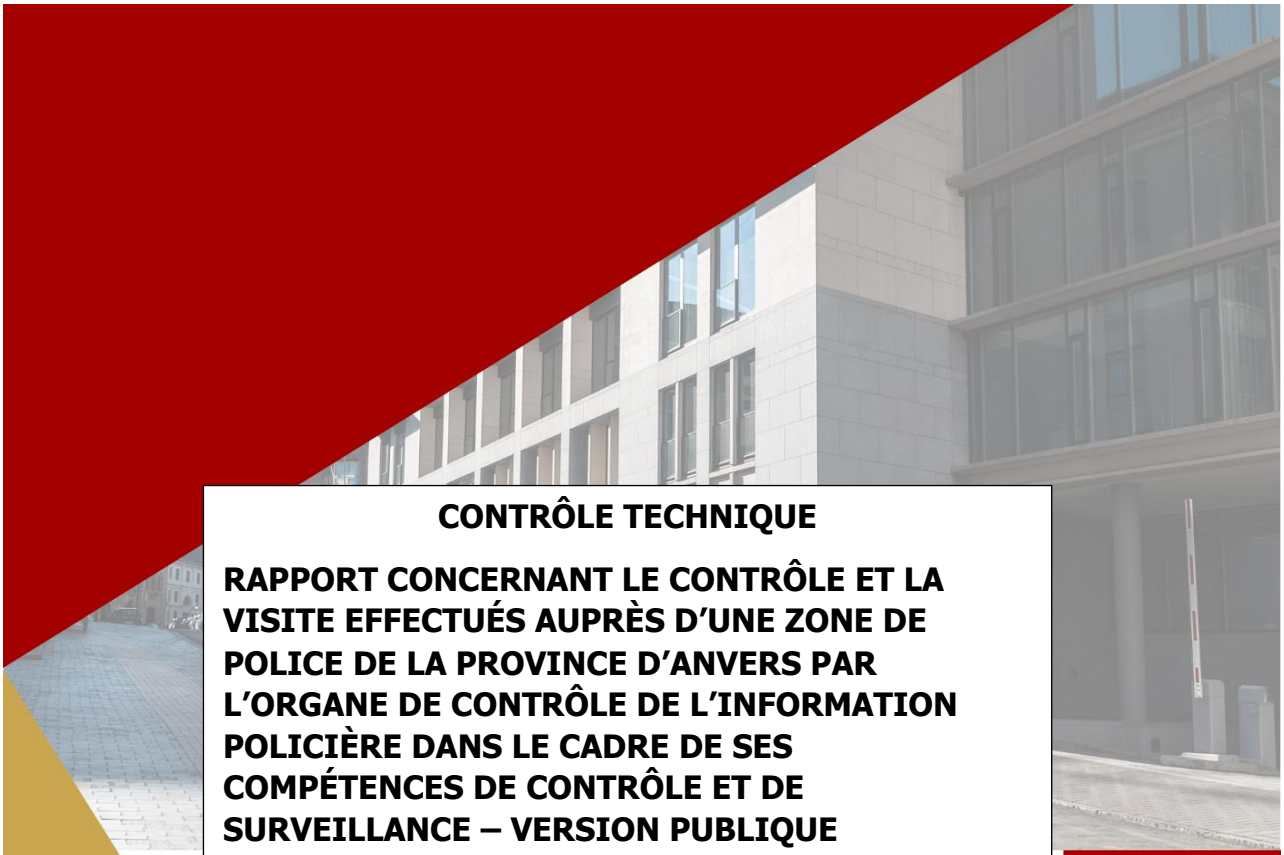


CONTRÔLE TECHNIQUE

RAPPORT CONCERNANT LE CONTRÔLE ET LA VISITE EFFECTUÉS AUPRÈS D'UNE ZONE DE POLICE DE LA PROVINCE D'ANVERS PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LE CADRE DE SES COMPÉTENCES DE CONTRÔLE ET DE SURVEILLANCE – VERSION PUBLIQUE

Référence : CON20007

RAPPORT

Table des matières

RAPPORT

1. INTRODUCTION

1. Vu ses compétences en tant que service de contrôle externe et autorité de contrôle compétente pour les traitements de données par la police intégrée (GPI), l'Organe de contrôle de l'information policière ('l'Organe de contrôle' ou 'COC') a décidé d'effectuer une visite auprès d'une zone de police de la province d'Anvers, dans la région frontalière avec les Pays-Bas (ci-après dénommée 'la ZP de la province d'Anvers') dans le cadre d'un 'contrôle technique'[1]. La présente version publique du rapport[2] a trait aux conclusions de l'enquête menée à l'occasion de ce contrôle.

1.1. Les compétences de l'Organe de contrôle de l'information policière

2. La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)[3] a réformé l'Organe de contrôle de l'information policière ('l'Organe de contrôle' ou 'COC') 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 §1er 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 de l'intervention policière.

L'Organe de contrôle est compétent pour les services de police[4], pour l'inspection générale de la police fédérale et de la police locale (AIG)[5] et pour l'unité d'information des passagers (BEL-PIU)[6]. 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.[7]

---

[1] Le COC établit une distinction entre différentes 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 ;
- **un 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 ;
- **un contrôle technique :** il s'agit d'un contrôle qui se concentre sur la licéité, l'exhaustivité et l'exactitude des enregistrements/traitements effectués dans les banques de données policières ;
- **un contrôle restreint :** ce contrôle porte sur un seul ou sur quelques aspects (partiels) d'un traitement de données policier ou non policier ;
- **un contrôle international :** il s'agit des éventuelles enquêtes internationales auxquelles le COC apporte son concours ;
- **un contrôle spécial :** il s'agit d'un contrôle portant sur des matières particulières, comme les contrôles annuels des banques de données communes terrorisme et extrémisme.

[2] Une version publique d'un rapport signifie que celle-ci ne contient pas nécessairement tous les éléments figurant dans le rapport de base qui est adressé à l'un des destinataires. Certains éléments ou passages ont été supprimés ou anonymisés. Il peut y avoir diverses raisons à cet effet, tant des raisons de nature légale que des motifs d'opportunité : la non-divulgation de techniques ou tactiques policières, le secret de l'instruction, le secret professionnel, le fait qu'il ait été remédié à un manquement entre-temps, etc.

[3] 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 (**L**aw **E**nforcement **D**irective)).

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

[5] 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°, d de la LPD).

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

[7] Art. 4 §2, 4ième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

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.

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, 3e 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 »[8]. 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-fondé[9]. Les membres de l'Organe de contrôle et les membres du personnel disposent à cet égard de compétences d'investigation et peuvent prendre des mesures correctrices[10].

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 judiciaire[11].

2. OBJET DU CONTRÔLE ET MÉTHODOLOGIE

3. Le 14 janvier 2021, l'Organe de contrôle a effectué de sa propre initiative un contrôle technique restreint[12] auprès d'une ZP de la province d'Anvers. Ce contrôle ne faisait donc pas suite à une plainte (individuelle) ni à l'existence d'indications (concrètes) d'un non-respect de la législation et de la réglementation par la zone de police visitée.

4. Vu la portée, la nature des données et la forme des traitements dans le cadre de la création de banques de données particulières, le fonctionnement de la BNG, les arrestations judiciaires réalisées par la police et le 'triptyque' y afférent[13], l'utilisation de caméras – et plus particulièrement le recours à la technologie *ANPR*[14] –, il est question lors de tels traitements de données d'une ingérence profonde dans la vie privée. En vue d'une collecte correcte des informations, ces traitements sont soumis à des conditions d'exécution qui sont décrites dans la législation (principalement dans la LFP et la LPD), dans des arrêtés d'exécution et dans des directives (principalement la directive MFO-3 et son vade-mecum). Le COC vérifie si les banques de données particulières ont été créées selon les règles applicables, si la réalisation des arrestations judiciaires et du triptyque est conforme à la réglementation applicable et est correcte, comment se déroule le fonctionnement de la BNG au sein de la zone et comment est envisagée l'utilisation de la technologie *ANPR*.

[8] MAP signifie « méthodes administratives particulières ».
[9] Art. 240, 4° de la LPD.
[10] Art. 244 et 247 de la LPD.
[11] Art. 248 de la LPD.
[12] Un contrôle technique est un examen technique axé principalement sur l'aspect policier opérationnel qui se concentre à chaque fois sur un ou plusieurs thèmes spécifiques comme le contrôle du triptyque, l'alimentation de la BNG, l'accès/la journalisation illicite (voir aussi l'article 236 §3 et l'article 239 de la LPD). Ce type de contrôle est moins axé sur les aspects juridiques ou sur les aspects de la protection des données ou de la protection de la vie privée, sans pour autant les négliger (voir aussi la note de bas de page n° 1).
[13] Le triptyque consiste en le relevé des empreintes digitales et palmaires, la prise de photos et l'établissement du signalement individuel en vue de permettre l'identification d'une personne.
[14] ***A**utomatic **N**umber **P**late **R**ecognition*.

5. Lors d'un contrôle technique, le COC vise à appréhender les processus de fonctionnement de la zone de police dans le cadre de la gestion de l'information policière. Ce contrôle avec visite a été en l'occurrence limité aux thèmes spécifiques suivants :

- Banques de données particulières (BDP)
  - Processus d'alimentation
  - Relation avec les autres banques de données policières
  - Processus d'effacement (vérifications des délais de conservation)
    - Gestion des accès et traçabilité
- Contrôle des journalisations (y compris le motif de la consultation) basé sur un mois de l'année 2020 ;
- BNG : recours à l'option 32[15] et à l'option 35[16] ; recours à la validation centrale : situation et autres points d'attention ;
- Triptyque – arrestations judiciaires ;
- Recours à la technologie *ANPR* et à la banque de données techniques locale.

3. CADRE JURIDIQUE

3.1. Banques de données particulières

6. L'article 44/11/3 de la LFP dispose que la création d'une BDP n'est possible que lorsque l'exercice des missions de police administrative et judiciaire exigent que les services de police structurent les données à caractère personnel et informations visées à l'article 44/1 de la LFP de manière à ce qu'elles puissent être retrouvées directement (il s'agit donc d'une banque de données 'opérationnelle').

7. L'article 44/11/3 susmentionné de la LFP prévoit en outre en son §1er les conditions cumulatives suivantes pour la création d'une BDP :
- dans des circonstances spécifiques ;
- pour l'exercice des missions de police administrative et judiciaire ;
- pour des besoins particuliers.

L'article 44/11/3 de la LFP prévoit par ailleurs en son §2 que la création d'une BDP doit être motivée par au moins un des besoins particuliers suivants :

a) la nécessité de classifier des données à caractère personnel ou informations au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité ;

b) l'impossibilité technique ou fonctionnelle d'alimenter la BNG de tout ou partie des données à caractère personnel et informations traitées dans ces banques de données ;

c) le caractère non pertinent ou excessif de la centralisation dans la BNG de tout ou partie des données à caractère personnel ou des informations, dans le cadre de l'exercice des missions de police administrative et de police judiciaire.

[15] L'option 32 désigne dans le jargon policier la réalisation d'un téléchargement de données spécifiques de la BNG vers la zone de police qui les demande. Le recours à cette option est journalisé, ce qui permet d'en assurer un suivi par unité. L'option 32 est principalement utilisée pour le téléchargement des données provenant de la BNG (mesures à prendre au niveau national à l'égard de véhicules et de numéros d'immatriculation), du *SIS* (mesures à prendre au niveau international à l'égard de véhicules, ne remontant pas à plus de deux ans), du GOCA (véhicules probablement pas en règle de contrôle technique) et de Veridas (véhicules probablement pas assurés). Ces données peuvent être utilisées pour la corrélation dans les banques de données techniques en vue de la mise en œuvre de la politique d'action définie par le groupe de travail Police-Justice-Intérieur, qui doit se traduire au niveau de l'arrondissement par une politique d'intervention. L'option 32 inclut également des données provenant de la BNG et de la DIV à partir desquelles les données des numéros d'immatriculation captés par la technologie *ANPR* peuvent être enrichies. Pour la BNG, il s'agit de l'enrichissement au moyen de l'indication que le véhicule ou le numéro d'immatriculation est lié ou non à une personne connue dans la BNG ; pour la DIV, il s'agit de l'enrichissement au moyen de l'indication que le titulaire du véhicule est connu ou non dans la BNG.

[16] On entend par l'option 35 le transfert normal de données à partir d'ISLP vers la Banque de données Nationale Générale (BNG).

9. Les finalités et conditions de la création d'une banque de données particulière sont donc clairement définies dans la loi. Ces dispositions légales constituent donc le fondement sur lequel le COC se base pour considérer une certaine banque de données comme une BDP. Le responsable du traitement doit, avant de reprendre cette banque de données dans le registre national des traitements (REGPOL) ou dans un registre local, passer ces critères en revue, les cocher et les expliciter ou les commenter comme il se doit.

8. Conformément aux articles 58 et 59 de la LPD, les services de police doivent demander au préalable l'avis du COC :

- lors de la réalisation d'une analyse d'impact relative à la protection des données (AIPD ou *DPIA*)[17] lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques (art. 58) ;
- lorsque l'AIPD indique que le traitement présente un risque élevé et que le responsable du traitement ne prend pas de mesures pour atténuer le risque ; ou lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées (art. 59 §1er, 1° et 2°).

9. La GPI ne peut donc pas retenir les arguments suivants pour créer une banque de données particulière :

- la charge de travail induite par l'encodage, l'alimentation et le transfert des données à la BNG ;
- le manque de connaissance de l'utilisation de la BNG ou d'une banque de données de base ;
- le manque (prétendu) de convivialité de la BNG ou d'une banque de données de base.

3.2. Journalisation de la BNG

10. La police est tenue de conserver des fichiers de journalisation[18]. Un fichier de journalisation est par excellence un instrument permettant de contrôler la preuve de la licéité ou de l'illicéité du traitement et de garantir l'intégrité et la protection des données[19]. À cet égard, les fichiers de journalisation sont également importants dans le cadre des procédures disciplinaires internes ou des enquêtes administratives. Les chiffres du conseil disciplinaire de la GPI démontrent que la consultation illicite est le délit disciplinaire le plus fréquemment commis. Les fichiers de journalisation sont par conséquent importants pour le contrôle tant proactif que réactif, et ce tant au niveau interne qu'externe. Cette importance est également démontrée par la récente décision du comité de direction de la police fédérale de rendre techniquement obligatoire la mention du motif de la consultation[20].

3.3. Fonctionnement de la BNG

11. Les données policières et judiciaires sont particulièrement sensibles. Elles ne peuvent être traitées que dans le cadre de missions de police judiciaire ou administrative, et uniquement conformément aux prescriptions légales (LFP, LPD, MFO-3[21], Code d'instruction criminelle, secret professionnel, secret de l'instruction, etc.). Une application rigoureuse des règles d'encodage et de ventilation conformément aux dispositions légales de la LPD[22] et de la LFP[23] d'une part, et aux dispositions réglementaires de la MFO-3 et du vade-mecum y afférent[24] d'autre part, est d'une importance primordiale.

3.4. Triptyque

[17] *DPIA* étant l'acronyme anglais signifiant ***D**ata **P**rotection **I**mpact **A**ssessment.*
[18] Article 56 §1er de la LPD mettant en œuvre l'article 25 de la directive Police-Justice.
[19] Art. 56 §2 de la LPD.
[20] Comité de direction du 21 septembre 2020, point 3, numéro d'émission CG/2020/4855.
[21] La Directive commune MFO-3 des Ministres de la Justice et de l'Intérieur *'relative à la gestion de l'information de police judiciaire et de police administrative'*.
[22] En particulier le Titre 2.
[23] En particulier les articles 44/1 à 44/11 inclus.
[24] Le Vade-mecum de la Police judiciaire décrit en détail les règles d'encodage à observer lors des enregistrements dans la BNG.

12. La réglementation sur la réalisation du triptyque trouve son origine dans la directive contraignante commune MFO-3 des Ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative.

13. La réalisation du triptyque est essentielle dans le cadre de l'objectif qui vise à amener les bonnes informations au bon endroit et au bon moment en vue d'un exercice plus efficace des missions de police judiciaire et administrative.

Le triptyque judiciaire est réalisé dans le cadre de l'identification de personnes et se compose de 3 volets :

a. les empreintes digitales et palmaires ;
b. les photos ;
c. le signalement individuel de la personne.

14. Le triptyque est réalisé dans le cadre des missions de police judiciaire et, le cas échéant, dans le cadre de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers.

15. On entend dans ce contexte par 'personne' :

- l'auteur, le coauteur, le complice ou le suspect (catégorie « SUSPECT ») ;
- la personne qui ne dispose pas d'un titre de séjour légal ou qui n'est pas en possession de documents permettant son identification, à l'exception des mineurs étrangers non accompagnés (MENA) et des demandeurs d'asile (catégorie « SUSPECT ») ;
- la victime, la personne préjudiciée, le témoin ou le(s) membre(s) des services de police ou de secours présent(s) sur le lieu des faits (catégorie « NON SUSPECT »). Un corps sans vie est toujours considéré comme relevant de la catégorie « non suspect » (lors du relevé des empreintes digitales et palmaires) ;
- la personne disparue (prise de photos) ;
- la personne disparue ou la personne faisant l'objet d'une mesure à prendre (établissement du signalement individuel).

16. Il est **obligatoire** de relever les empreintes digitales d'un suspect lorsque cette personne est âgée de plus de 14 ans et :

- soit est entendue et mise sur la base d'informations confirmées (prouvées) en relation avec un fait concret, ou fait l'objet de présomptions sérieuses de la part des services de police ;
- soit est privée de sa liberté (à partir du moment où, pour les besoins de l'enquête, la personne concernée n'est plus libre d'aller et venir comme elle veut) ;
- soit est mise à la disposition des instances judiciaires ou de l'Office des Étrangers ;
- soit doit être enfermée dans un établissement pénitentiaire en vertu d'un ordre judiciaire ou d'une décision judiciaire.

17. Pour les mineurs d'âge âgés de moins de 14 ans, le magistrat en charge du dossier doit en outre avoir donné son autorisation en vue de la réalisation de l'identification judiciaire en trois volets. Cette autorisation doit être consignée dans le procès-verbal.

18. En cas de séjour illégal, le triptyque judiciaire **DOIT** toujours être réalisé. La contrainte strictement nécessaire peut être exercée pour le relevé des empreintes digitales (cf. art. 37 de la LFP). Les modalités pratiques de la réalisation du triptyque sont décrites dans les fiches B03, B04 et B05 de la directive MFO-3.

3.5. Arrestations judiciaires

19. Les règles régissant la réalisation des arrestations judiciaires figurent dans la législation suivante :

- L'article 15 de la LFP dispose que dans l'exercice de leurs missions de police judiciaire, les services de police ont pour tâche de rechercher les crimes, les délits et les contraventions, d'en rassembler les preuves, d'en donner connaissance aux autorités compétentes, d'en saisir, arrêter et mettre à la disposition de l'autorité compétente les auteurs, de la manière et dans les formes déterminées par la loi ;
- L'article 32 de la LFP fait mention de la durée de l'arrestation ;

- La loi du 20 juillet 1990 relative à la détention préventive trouve également application (cf. art. 1er : arrestation, art. 3 : mandat d'amener et art. 16 : mandat d'arrêt).

3.6. Surveillance par caméra

20. Depuis la loi du 21 mars 2018 modifiant la LFP, la décision d'installer des caméras dans les espaces publics ne peut plus être prise que par une autorité publique, comme la commune[25]. Lorsque la police recourt à la surveillance par caméra, les dispositions de la LFP s'appliquent, sauf si l'utilisation de caméras est régie par une autre législation[26].

3.6.1. Responsable du traitement

21. Le droit de la protection des données réserve un rôle important au 'responsable du traitement'. Le responsable du traitement est « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel* »[27]. En ce qui concerne les activités de traitement dans le cadre des missions de police administrative et judiciaire, le responsable du traitement est défini par la LPD comme « *l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens de ce traitement sont déterminés par la loi, le décret ou l'ordonnance, le responsable du traitement est l'entité désignée comme responsable du traitement par ou en vertu de cette loi, ce décret ou cette ordonnance* ».[28] On entend par « *autorités compétentes* » « *a) 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* »[29].

22. Bien que la LFP attribue à certains endroits un rôle (spécifique) au responsable du traitement, ce n'est pas le cas pour l'utilisation de caméras. Comme nous le disions plus haut, le responsable du traitement est un acteur essentiel dans le traitement de données à caractère personnel. Il doit en effet prouver que les données à caractère personnel sont traitées conformément au cadre légal. Il est aussi, ou son préposé ou mandataire, la personne à l'égard de laquelle d'éventuelles mesures correctrices peuvent être imposées, ou qui peut faire l'objet d'une sanction pénale[30].

Le chef de corps est le responsable du traitement pour la conservation des images des caméras dans une banque de données technique locale[31]. Le chef de corps est également le responsable du traitement pour les banques de données particulières[32].

3.6.2. Exigences procédurales

23. Avant qu'un service de police ne puisse introduire la surveillance par caméra sur le territoire d'une commune, il a besoin de l'autorisation de principe du Conseil communal[33]. Aucune autorisation n'est toutefois requise pour l'utilisation de caméras dans des lieux fermés dont la police est elle-même le gestionnaire, comme un commissariat de police[34]. Il est important de souligner que si l'autorisation du Conseil communal a déjà été obtenue avant la modification de loi du

---

[25] Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, M.B. 16 avril 2018.
[26] Comme le contrôle de trajet, qui relève de l'application de la loi du 16 mars 1968 relative à la police de la circulation routière (Doc. Parl. *Chambre* 2017-2018, n° 54-2855/001, 9).
[27] Art. 4. 7) du RGPD.
[28] Art. 26, 8° de la LPD.
[29] Art. 26, 7° de la LPD.
[30] Voir les articles 221 et 222 de la LPD. Concrètement, l'Organe de contrôle peut prendre notamment les mesures suivantes (art. 25.2 du RGPD) :
- donner un avertissement ;
- donner une réprimande ;
- ordonner de mettre dans un certain délai le traitement en conformité avec le cadre légal ;
- imposer une limitation ou une interdiction temporaire ou définitive du traitement.
[31] Art. 44/11/3*sexies* §1er, 2e alinéa de la LFP.
[32] Art. 44/4 §1er, troisième alinéa de la LFP.
[33] Art. 25/4 §1er, 1° de la LFP.
[34] Exposé des motifs de cette loi, p. 21 (Doc. Parl. *Chambre* 2017-2018, n° 54-2855/001).

21 mars 2018 en application de la loi relative aux caméras, l'autorisation du Conseil communal ne devra pas être obtenue à nouveau[35]. Cette autorisation obtenue initialement reste donc valable. Cette même autorisation ne pourra toutefois pas être utilisée pour l'utilisation de nouveaux types de caméras introduits par la loi du 21 mars 2018. La LFP impose notamment des conditions spécifiques pour l'utilisation de caméras fixes mobiles sur laquelle le Conseil communal doit se prononcer[36]. Dans ce cas, une nouvelle autorisation ou une autorisation complémentaire du Conseil communal doit donc être obtenue.

3.6.3. Délai de conservation des images

26. Les images des caméras peuvent être conservées au maximum pendant 1 an[37]. La loi ne stipule pas de délai minimum. En ce qui concerne les images des caméras classiques, la LFP ne précise pas sur quel support de données les images doivent être enregistrées. Il est dès lors indiqué que le chef de corps précise dans le registre des traitements de données à caractère personnel tel que visé à l'article 55 de la LPD (voir le point 3.3.8) sur quel support de données les images sont enregistrées. L'Organe de contrôle doit avoir accès à ce support de données.

3.6.4. Banques de données techniques

27. Un régime spécifique s'applique pour l'utilisation de caméras *ANPR*. Il s'agit de « *caméras intelligentes* », à savoir des « *caméras qui comprennent également des composantes ainsi que des logiciels qui, couplés ou non à des registres ou à des fichiers, peuvent traiter de manière autonome ou non les images recueillies* »[38]. Lorsque la surveillance par caméra *ANPR* est appliquée, les images doivent être enregistrées dans une « *banque de données technique* »[39], étant entendu que les données à caractère personnel et informations sont également transmises à la banque de données technique nationale[40]. Les images peuvent être conservées au maximum pendant un an et il n'est pas fixé de délai minimum[41].

La banque de données technique contient les données suivantes, si elles apparaissent sur les images des caméras[42] :
1) la date, le moment et l'endroit précis du passage de la plaque d'immatriculation ;
2) les caractéristiques du véhicule lié à cette plaque ;
3) une photo de la plaque d'immatriculation à l'avant du véhicule et le cas échéant, à l'arrière ;
4) une photo du véhicule ;
5) le cas échéant, une photo du conducteur et des passagers ;
6) les données de journalisation des traitements.

Ces données doivent donc être enregistrées dans la banque de données technique pour autant que ces données apparaissent sur les images *ANPR*.

28. Les principes relatifs aux interconnexions et corrélations des banques de données techniques avec les banques de données visées à l'article 44/2 §§ 1er et 2 de la LFP 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 conformément à l'article 44/4 §6 de la LFP sont régis par la directive interconnexions et corrélations[43]. Les interconnexions et corrélations doivent notamment tenir compte :

- des critères de temps, d'espace et de fréquence tels que visés à l'article 44/4 §6 de la LFP ;

[35] Art. 88 de la loi du 21 mars 2018 et exposé des motifs de cette loi, p. 113-114 (Doc. Parl. *Chambre* 2017-2018, n° 54-2855/001).
[36] Art. 25/4 §2, 2e alinéa de la LFP.
[37] Art. 25/6, 44/11/3*decies* §2, premier alinéa, et 46/12, premier alinéa de la LFP.
[38] Art. 25/2 §1er, 3°, *juncto* art. 44/2 §3, troisième alinéa de la LFP.
[39] Art. 44/2 §3, premier alinéa de la LFP.
[40] Art. 44/11/3*sexies* de la LFP.
[41] Art. 44/11/3*decies* §2, premier alinéa de la LFP.
[42] Art. 44/11/3*decies* §1er de la LFP.
[43] Directive commune contraignante des Ministres de la Justice et de l'Intérieur relative à la détermination des mesures adéquates, pertinentes et non excessives relatives à l'interconnexion ou la corrélation des banques de données techniques suite à l'utilisation de caméras ou de systèmes intelligents de reconnaissance automatique de plaques d'immatriculation, visées à l'article 44/2, §3 de la loi sur la fonction de police, avec les banques de données visées à l'article 44/2, §§ 1er et 2 LFP, 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, M.B. 28 janvier 2021.

- de l'enregistrement dans le registre des traitements REGPOL des autorisations requises ;
- de la nécessité d'adopter une procédure transparente et auditable lorsque les unités de police utilisent des listes ou des extraits en dehors des standards nationaux qu'ils interconnectent avec les *ANPR* locaux et l'*ANPR* national en vue d'établir des comparaisons ;
- de la nécessité en cas de *hit* (corrélation positive) de suivre la politique d'action nationale et une politique d'intervention ciblée ;
- de la nécessité de retourner vers la source authentique en cas d'un *hit* sur une plaque d'immatriculation, détecté à l'aide de listes ou d'extraits injectés dans une banque de données technique locale ou nationale, sauf si la corrélation se fait en temps réel avec la source authentique.

3.6.5. Accès aux images

29. L'accès aux images dépend de la finalité et est réglé de la même manière pour la surveillance par caméra ordinaire et pour l'utilisation de caméras *ANPR*. Dans les deux cas, les images peuvent être conservées au maximum pendant 12 mois. En ce qui concerne les missions de police administrative, l'accès est limité au premier mois à partir de l'enregistrement des images. Pour les missions de police judiciaire, les images sont accessibles pendant l'entièreté du délai de conservation, étant entendu que l'intervention du Procureur du Roi est requise après l'expiration du premier mois[44]. L'accès doit être motivé sur le plan opérationnel et nécessaire pour l'exercice d'une mission précise[45], ce qui revient à dire que l'accès aux images n'est autorisé que pour les personnes qui ont besoin de ces données à caractère personnel et informations et en présence d'un intérêt opérationnel concret[46].

3.6.6. Utilisation de caméras visibles et non visibles

30. Les caméras visibles sont des caméras dont l'utilisation est annoncée par des pictogrammes, les caméras montées à bord de véhicules de police, de navires de police, d'aéronefs de police, ou de tout autre moyen de transport de police, identifiables comme tels, ou portés par des fonctionnaires de police identifiables comme tels[47]. Dans des circonstances exceptionnelles, la police peut recourir secrètement à des caméras (utilisation non visible de caméras). La caméra peut dans ce contexte être portée par le fonctionnaire de police ou être montée à bord d'un véhicule de police anonyme. Il est question d'un véhicule de police anonyme lorsque le véhicule de police n'est pas identifiable comme tel. Dans ce cas, il est donc question d'une utilisation « *non visible* » de caméras[48]. Le recours à des caméras non visibles est strictement réglementé et limité à quatre situations, à savoir :
1) dans des circonstances particulières, notamment lors d'attroupements, en vue du recueil de l'information de police administrative concernant des personnes radicalisées ou des *terrorist fighters* et sur un moyen de transport de police, non identifiable comme tel, pour la lecture automatique de plaques d'immatriculation, en vue de détecter des véhicules signalés (art. 46/4 de la LFP) ;
2) pour la préparation d'actions de police judiciaire et afin de garantir l'ordre public lors de ces actions (art. 46/7 et 46/8 de la LFP) ;
3) dans le cadre de l'exécution de missions spécialisées de protection de personnes (art. 44/9 de la LFP) et
4) dans le cadre de l'exécution de missions de transfert de personnes détenues ou arrêtées (art. 46/11 de la LFP).

Sauf lorsque l'utilisation non visible des caméras est réalisée sous le contrôle d'un magistrat, cette forme d'utilisation de caméras doit toutefois être notifiée au préalable à l'Organe de contrôle. Cette notification préalable doit permettre à l'Organe de contrôle d'évaluer la licéité de la décision[49].

3.6.7. Analyse d'impact relative à la protection des données (AIPD ou *DPIA* pour *Data Protection Impact Assessment*)

[44] Art. 25/7 §1er, 1er et 2e alinéas et 44/11/3*decies* §3, deuxième alinéa de la LFP.
[45] Art. 44/11/3*decies* §3, 1er alinéa de la LFP.
[46] Exposé des motifs de cette loi, p. 29 (Doc. Parl. *Chambre* 2017-2018, n° 54-2855/001).
[47] Art. 25/2 §2 de la LFP.
[48] Art. 46/4 et suivants de la LFP.
[49] Art. 46/6 et 46/10 de la LFP.

31. Depuis la loi du 21 mars 2018, il est obligatoire de procéder, préalablement au recours à la surveillance par caméra, à une analyse d'impact et de risques évaluant l'aspect de la protection de la vie privée par rapport au niveau opérationnel de l'utilisation des caméras[50]. Cet exercice doit également être réalisé avant la création d'une banque de données technique (locale)[51]. L'assistance du délégué à la protection des données est demandée dans ce contexte[52].

Pour autant que les conditions de la LDP pour une AIPD et les conditions pour une analyse de risques et d'impact relative à l'utilisation de caméras et/ou relative à la création de banques de données techniques dans le cadre de la LFP soient respectées, les deux analyses peuvent être compilées en un seul document. Étant donné qu'une AIPD dans le cadre de la LPD requiert une analyse plus large que ce que prescrit la LFP, nous précisons que si les deux analyses sont réalisées ensemble, cette analyse doit couvrir conformément à la LPD tous les systèmes et procédures pertinents des activités de traitement. En marge du respect de la LPD et de la LFP, les mesures de précaution opérationnelles et les mesures de sécurité (prises pour limiter les risques pour les données à caractère personnel à protéger) doivent également être décrites.

3.6.8. Surveillance par caméra des bâtiments et bureaux de police et cellules de police

32. La surveillance par caméra des bâtiments et bureaux de police et cellules de police relève de la LFP[53]. C'est également le cas de la surveillance par caméra du hall d'entrée ou de l'accueil du commissariat de police. La vidéosurveillance[54] dans les lieux de détention contribue à la protection et à la garantie du bien-être des personnes qui ont été privées de leur liberté et contribue en outre à un meilleur respect des droits de la défense visés à l'article 6 de la CEDH[55]. Cette vidéosurveillance n'est cependant envisageable que comme un élément venant s'ajouter à un ensemble de mesures, comme le contrôle physique régulier des personnes détenues, une politique de prévention du suicide, un système de dénonciation efficace pour les victimes d'actes illicites dans des cellules, de séparation, d'isolement, de l'application de sanctions disciplinaires ou encore la présence d'un avocat pendant l'audition par la police[56]. Le bâtiment ou poste de police doit être équipé d'une signalisation claire de la vidéosurveillance, de manière à ce que la personne détenue dans l'une des cellules en ait été explicitement informée. Les enregistrements de la détention doivent rester intégraux (aucun effacement partiel) et être conservés pendant une période permettant d'introduire une plainte dans un délai raisonnable.

Étant donné que ces images ne sont pas nécessairement conservées pour les missions de police administrative ou judiciaire, mais aussi à des fins préventives d'administration de la preuve (pour la police ou pour la personne concernée, selon le cas), la procédure d'accès indirect à ces images par l'intermédiaire du COC ne trouve pas application et la personne concernée peut conformément à la LPD et au RGPD accéder directement aux images de sa détention.

Lors de la projection des images des différentes cellules sur les moniteurs installés au commissariat, la police doit prendre un certain nombre de mesures de sécurité et d'accès rigoureuses : l'accès doit être limité selon le principe « need to know ». Il convient d'éviter un accès général aux images (par exemple sur des moniteurs installés dans un local où les membres du personnel vont et viennent, ou à l'accueil).

3.6.9. Registre

33. Le recours à la surveillance par caméra doit être tenu à jour dans un registre (local)[57] mentionnant le type de caméras et leur emplacement. Il n'existe toutefois pas encore d'arrêté royal détaillant le contenu du registre. L'Organe

[50] Art. 25/4 §2 de la LFP.
[51] Art. 44/11/3*octies* de la LFP.
[52] Art. 65, 3° *juncto* 58 de la LPD.
[53] Voir aussi l'arrêté royal du 14 septembre 2007 relatif aux normes minimales, à l'implantation et à l'usage des lieux de détention utilisés par les services de police, et en particulier l'article 10.
[54] Recommandation 06/11 de l'ancienne Commission de protection de la vie privée ou CPVP – actuellement l'Autorité de protection des données ou APD – sur l'installation et l'utilisation de caméras de surveillance dans les lieux de détention et dans d'autres lieux du commissariat.
[55] Convention européenne des droits de l'homme.
[56] Voir à ce sujet « Les normes du CPT – Chapitres des rapports généraux du CPT consacrés à des questions de fond » (document CPT/Inf/E (2002) 1 – Rév. 2009), disponible sur le site www.cpt.coe.int/en/docsstandards.htm.
[57] Art. 25/8 de la LFP.

de contrôle préconise néanmoins, dans l'intérêt de l'efficacité de ses compétences de contrôle, que le service de police crée de sa propre initiative, dans l'attente de l'arrêté d'exécution, un registre mentionnant chaque utilisation (d'un type) de caméras, y compris l'utilisation non visible de caméras. L'Organe de contrôle (et d'ailleurs aussi et avant tout la zone de police elle-même) pourra ainsi se faire une idée du recours à la surveillance par caméra sur le territoire de la commune relevant de la compétence du service de police. Dans le même temps, le recours à la surveillance par caméra pourra ainsi être comparé au registre des activités de traitement. Étant donné que l'enregistrement d'images induit un traitement de données à caractère personnel, ce traitement doit également être consigné dans le registre des traitements[58]. Les deux registres sont ou doivent être disponibles pour l'Organe de contrôle.

4. CONCLUSIONS DE L'ENQUÊTE

…

5. CONCLUSION – RECOMMANDATIONS, REQUÊTES ET MESURES CORRECTRICES

76. Après l'annonce du contrôle, la ZP de la province d'Anvers a mis de manière transparente la documentation requise à disposition et a répondu dans le délai imparti aux questions qui avaient été posées en guise de préparation. Le COC souligne une fois de plus le caractère réfléchi du fonctionnement recourant aux banques de données particulières dans le contexte d'un système de police intelligent axé sur l'information qui doit tenir compte de l'implantation spécifique de la zone de police au sein d'une région frontalière, des limitations des moyens et canaux mis à disposition au niveau central ainsi que de la situation du cadre réglementaire devant répondre à cette spécificité, mais doit agir, tout comme la zone de police, à la lumière de ce cadre réglementaire.

77. Le fonctionnement de la BNG est réfléchi également, même si le COC constate à cet égard que l'attribution systématique du profil le plus élevé possible revêt un caractère excessif. La coordination des instructions judiciaires par le biais de la BNG laisse également encore matière à amélioration.

78. La conception du traitement humain des personnes détenues mérite d'être recommandée. L'approche de l'analyse de traces témoigne également des méthodes innovantes de la ZP de la province d'Anvers.

79. La volonté d'innovation est en outre démontrée par le rôle de pionnier que la zone de police a joué sur le plan de la technologie *ANPR*. La zone devra dans ce domaine continuer à miser sur l'intégration de son propre fonctionnement et du fonctionnement national dès que ce dernier aura suffisamment évolué.

PAR CES MOTIFS,

L'Organe de contrôle,

Émet les <u>recommandations</u> suivantes,

1) <u>Recommandation</u>

Le COC recommande à la ZP de la province d'Anvers de transmettre à la police fédérale, de préférence par l'intermédiaire de la CPPL, les remarques aux utilisateurs concernant le registre REGPOL.

2) <u>Recommandation</u>

Conformément au document de politique intitulé 'Code de conduite ICT et sécurité de l'information', le COC recommande à la ZP de la province d'Anvers d'évaluer périodiquement la BDP existante à la lumière des évolutions des banques de

[58] Art. 55 de la LPD.

données de base, de la BNG et de la législation et de la réglementation en vue de l'intégration dans les applications de ICT existantes, en particulier en ce qui concerne les évolutions de FOCUS et de Questis.

3) Recommandation

Le COC recommande à la ZP de la province d'Anvers de mettre à profit la réalisation du triptyque judiciaire pour vérifier la qualité de l'encodage dans la BNG de la personne faisant l'objet de la réalisation du triptyque, et ce en ce qui concerne le signalement individuel, la photo et les empreintes digitales, et de procéder le cas échéant à la fusion de l'entité s'il apparaît que celle-ci a été encodée à plusieurs reprises dans la BNG.

Le COC constate en outre que la ZP de la province d'Anvers est disposée, en ce qui concerne l'analyse de traces, à réfléchir à de nouvelles méthodes et techniques et encourage la zone de police à poursuivre sur cette voie, mais toujours dans le respect du cadre législatif en vigueur.

4) Recommandation

Le COC recommande à la ZP de la province d'Anvers de suivre de près les évolutions techniques de la banque de données technique nationale afin soit de s'acquitter de l'obligation de transférer les données à la banque de données technique nationale, soit d'évaluer quand une utilisation exclusive de la banque de données technique nationale sera possible d'un point de vue technique et opérationnel.

5) Recommandation

Le COC recommande à la ZP de la province d'Anvers de veiller à spécifier un motif de consultation clair, conformément aux règles formulées et au plan de suivi.

6) Recommandation

Le COC recommande à la ZP de la province d'Anvers de vérifier si les processus de traitement des exportations de la banque de données technique locale ne peuvent pas être réalisés par le biais de la banque de données de base GES. Le COC recommande en outre à la ZP de vérifier si l'enquête sur la base de laquelle l'exportation a été réalisée relève des dispositions de la fiche C13 de la directive MFO-3 et doit par conséquent être notifiée par le biais d'un formulaire DOS.

Prie la zone de police de la province d'Anvers,

1) Requête

Le COC prie la ZP de la province d'Anvers de faire un usage complet et correct du registre REGPOL et de compléter au moins les paramètres 'BDD_type', 'Orga_trait', 'GPI_Unit' et 'DPO' conformément à la réalité.

2) Requête

Conformément au document de politique intitulé 'Code de conduite ICT et sécurité de l'information', le COC prie la ZP d'appliquer de manière cohérente le passage 9.4 relatif au monitoring des fichiers de journalisation et de sensibiliser et responsabiliser le personnel en la matière. La politique prévue peut être mise en œuvre de manière concrète à travers une politique proactive reposant sur un système de contrôles a posteriori de la motivation des consultations réalisées afin d'en vérifier la licéité et la légalité. Le COC prie la zone de police de réaliser des contrôles systématiques et proactifs concernant l'utilisation et/ou la consultation des banques de données policières, plus précisément en procédant chaque mois ou chaque trimestre à des contrôles par échantillonnage sur la base de journalisations. Le COC demande à ce que les résultats des contrôles soient tenus à sa disposition.

3) Requête

Le COC prie la ZP de la province d'Anvers d'évaluer les enquêtes (d'information ou judiciaires) réalisées en fonction des paramètres de notification tels que prévus dans la fiche C13 de la directive MFO-3 et de procéder systématiquement à l'établissement d'un formulaire DOS lorsque les conditions sont remplies.

4) Requête

Le COC prie la ZP de la province d'Anvers de faire le nécessaire pour l'enregistrement dans le registre des traitements de la police (REGPOL) des autorisations requises en cas de comparaisons des numéros d'immatriculation lues par les caméras *Automatic Number Plate Recognition* (*ANPR*) avec des numéros d'immatriculation repris dans des listes ou extraits des banques de données utilisées conformément à la directive ministérielle interconnexions et corrélations.

prie la zone de police de la province d'Anvers de faire le point sur ces recommandations et requêtes dans les 12 mois de la réception du présent rapport ;

ordonne les mesures correctrices suivantes à l'égard de la zone de police de la province d'Anvers (ZP),

Vu les articles 221 §1er et 247, 2°, 4°, 5° et 6° de la LPD,

1) Mesure correctrice[59]

Le COC ordonne à la ZP de la province d'Anvers de mettre un terme pour le 31 octobre 2021 au plus tard à tous les accès de personnes autres que les membres de la propre zone de police à une BDP pour laquelle le chef de corps de la ZP de la province d'Anvers est le responsable du traitement, ou d'offrir des garanties à cet égard jusqu'à la publication des directives ministérielles en la matière et d'en informer le COC (info@organedecontrole.be). Il devra être mis un terme aux échanges de *listes noires* par le biais de la BDP «points d'attention» dans le mois de la réception du présent rapport étant donné qu'il existe une alternative au sein de la GPI.

2) Mesure correctrice[60]

Le COC ordonne à la ZP de la province d'Anvers de mettre immédiatement un terme aux interconnexions et corrélations entre les banques de données particulières et les autres banques de données avec effet immédiat et d'en informer le COC dans un délai de 1 mois à compter de la réception du présent rapport.

3) Mesure correctrice[61]

Le COC ordonne à la ZP de la province d'Anvers soit de mettre un terme à l'échange d'informations d'office avec le DRIO par le biais de la BDP «points d'attention», soit de le mettre de manière démontrable en conformité avec l'article 2/7 de la loi de 2004 sur l'entraide judiciaire de la manière indiquée plus haut et d'en informer le COC pour le 31 octobre 2021 au plus tard.

4) Mesure correctrice

Le COC met en garde contre le non-respect du principe de proportionnalité et de finalité dans le cadre de ce 'push' automatisé et d'office à destination des Pays-Bas par le biais de la BDP des points d'attention, et appelle la ZP de la province d'Anvers à réaliser à ce sujet un exercice approfondi.

5) Mesure correctrice

Le COC ordonne à la ZP de la province d'Anvers de mentionner les traitements recourant à cet instrument UFED comme une banque de données particulière dans le registre REGPOL et d'en informer le COC dans un délai de 1 mois à compter de la réception du présent rapport.

[59] La ZP de la province d'Anvers a introduit le 2 juillet 2021 un recours contre cette mesure correctrice auprès de la Cour d'appel d'Anvers conformément à l'article 248 §2 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. En raison de la levée de la mesure corrective susmentionnée par le COC (cf. rapport de suivi 1), cet appel est devenu sans objet.
[60] La ZP de la province d'Anvers a introduit le 2 juillet 2021 un recours contre cette mesure correctrice auprès de la Cour d'appel d'Anvers conformément à l'article 248 §2 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. En raison de la levée de la mesure corrective susmentionnée par le COC (cf. rapport de suivi 1), cet appel est devenu sans objet.
[61] La ZP de la province d'Anvers a introduit le 2 juillet 2021 un recours contre cette mesure correctrice auprès de la Cour d'appel d'Anvers conformément à l'article 248 §2 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

6) Mesure correctrice

Le COC ordonne à la ZP de la province d'Anvers d'attribuer le profil 'exploitation avancée' de manière différenciée et de faire part de la situation au COC dans un délai de 3 mois à compter de la réception du présent rapport.

7) Mesure correctrice

Le COC ordonne à la ZP de la province d'Anvers, conformément aux articles 44/11/3*octies* de la LFP et 59 de la LPD, d'établir un projet de création d'une banque de données technique locale faisant mention des finalités et des modalités de traitement, y compris une analyse d'impact et de risques relative à la protection de la vie privée et au niveau opérationnel, notamment en ce qui concerne les catégories de données à caractère personnel traitées, la proportionnalité des moyens utilisés, les objectifs opérationnels à atteindre et le délai de conservation des données nécessaire pour atteindre ces objectifs. Vu la charge de travail induite par un tel effort, un premier point de la situation est attendu dans un délai de six mois à compter de la réception du présent rapport.

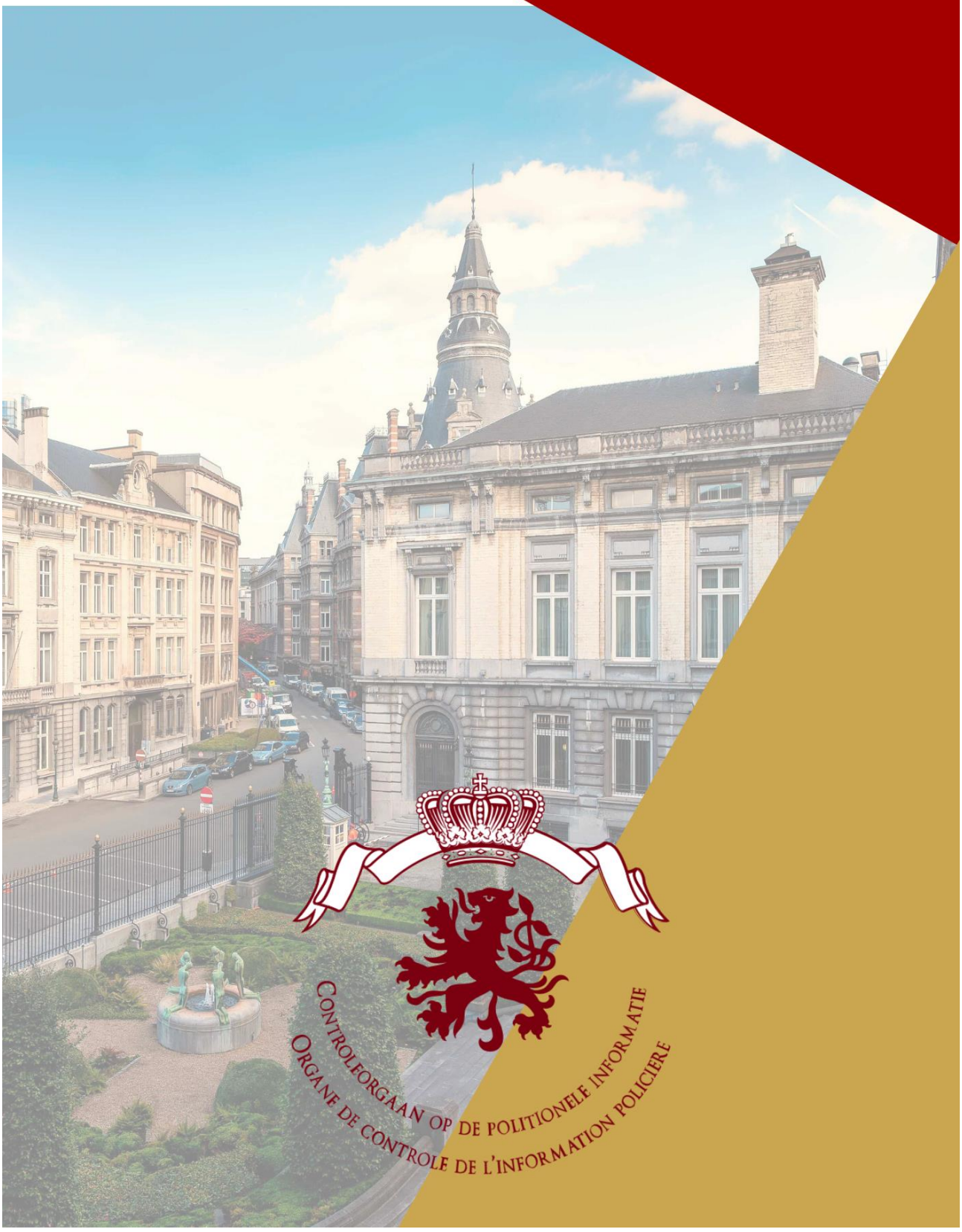
Dit pour droit que pour le calcul des délais imposés pour le respect des recommandations, requêtes et mesures correctrices 1 à 7 incluse, il y a lieu de prendre comme date de transmission du présent rapport définitif de l'Organe de contrôle la date de sa transmission plus deux jours ouvrables.

L'Organe de contrôle rappelle la possibilité, pour la zone de police, d'introduire un recours auprès de la Cour d'appel du ressort du domicile ou du siège du demandeur dans les 30 jours de la décision définitive de l'Organe de contrôle (article 248 §1er, premier alinéa, et §2 de la LPD).

Ainsi décidé par l'Organe de contrôle de l'information policière le 2 juin 2021.

Pour l'Organe de contrôle (SIGNÉ)

Koen Gorissen	Frank Schuermans	Philippe Arnould
Membre-conseiller	Membre-conseiller	Président



Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière