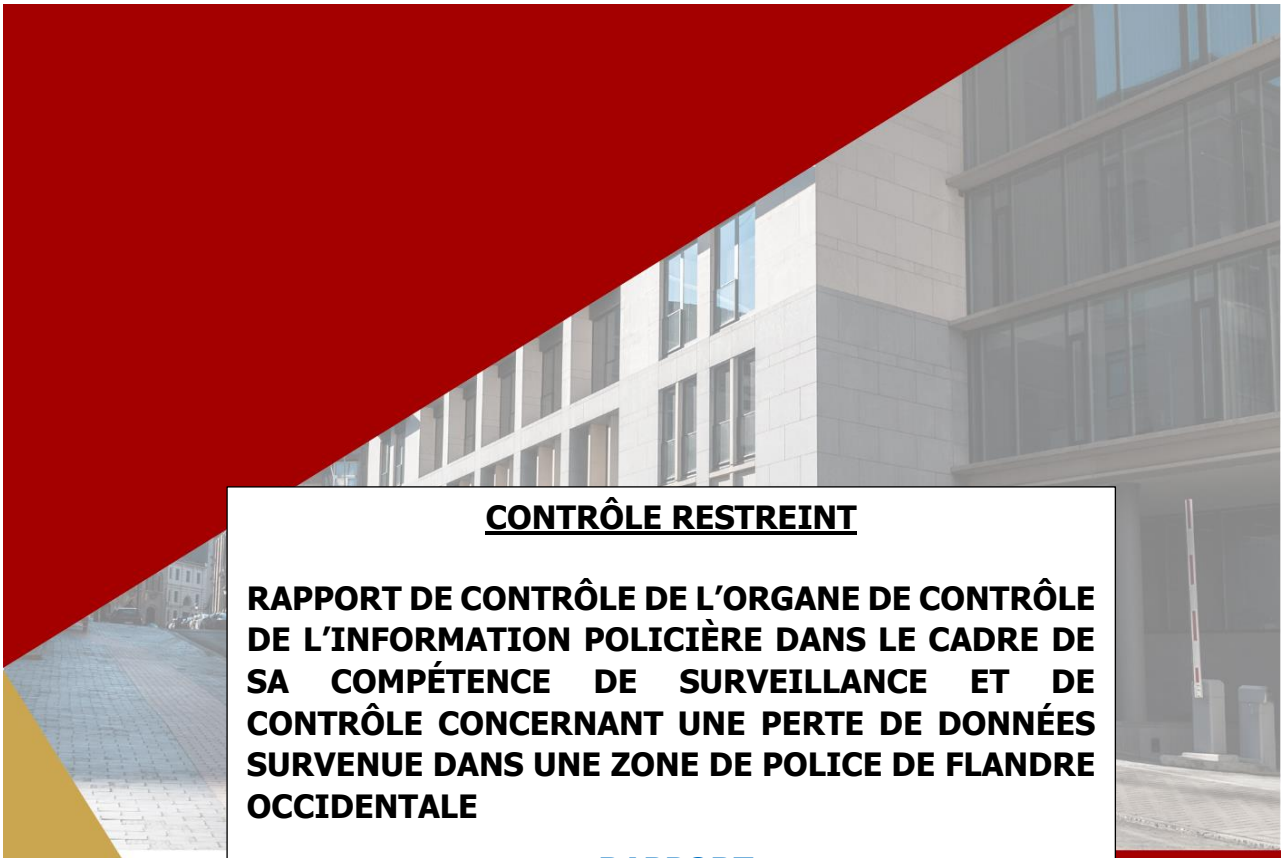


CONTRÔLE RESTREINT

RAPPORT DE CONTRÔLE DE L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LE CADRE DE SA COMPÉTENCE DE SURVEILLANCE ET DE CONTRÔLE CONCERNANT UNE PERTE DE DONNÉES SURVENUE DANS UNE ZONE DE POLICE DE FLANDRE OCCIDENTALE

RAPPORT

Référence : DIO24005

1. Table des matières

1. RAPPORT

Le présent rapport est la **version publique** du rapport de contrôle.

Cela signifie qu'il ne comporte pas ou pas nécessairement tous les éléments ou passages figurant dans le rapport de contrôle adressé aux destinataires. Certains éléments ou passages ont été omis ou anonymisés. Il peut y avoir diverses raisons à cela, qui peuvent être de nature légale ou être dictées par des motifs d'opportunité : la volonté de ne pas divulguer des techniques ou tactiques policières, le secret de l'enquête, le secret professionnel, le fait qu'un manquement a été résolu dans l'intervalle, etc.

2. INTRODUCTION

Résumé

Le 12 novembre 2023, le COC a été informé d'une perte de données survenue le 31 octobre 2023 auprès d'une zone de police de la province de Flandre occidentale (ci-après dénommée 'la ZP de la province de Flandre occidentale'). Il s'agissait d'une erreur humaine qui a engendré la perte de toutes les saisies numériques de 2022. Il s'est avéré que bien que diverses directives et recommandations l'exigent, il n'existait pas de copie de sauvegarde (back-up) de ces données. Le présent rapport se penche sur les obligations prévues par la législation, les directives et les recommandations en matière de back-up.

Il soulève également des questions quant aux délais de réponse pratiqués par la ZP de la province de Flandre occidentale et au fait que certains éléments des documents transmis au COC aient été supprimés ou rendus non reconnaissables. Le rapport s'achève sur quelques recommandations.

Mots-clés

Zone de police de Flandre occidentale, sécurité de l'information, back-up, copie de sauvegarde, saisie numérique, ISO 27k, high availability, haute disponibilité, redondance

3. LES COMPÉTENCES DE L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

1. La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (la 'LPD' ou 'loi sur la protection des données')[1] a réformé l'Organe de contrôle en notamment une autorité de surveillance à part entière en plus des compétences de contrôle en matière de gestion de l'information policière prévues par la loi du 5 août 1992 sur la fonction de police (LFP). L'article 71 §1er et les Titres 2 et 7 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 la gestion de l'information et de l'intervention policière. Sur la base de la réglementation susmentionnée, le COC dispose donc d'une compétence de surveillance générale à l'égard de tous les traitements opérationnels et non opérationnels de données (à caractère personnel) effectués par la GPI.

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.

[1] *M.B.* 5 septembre 2018. Elle contient également des dispositions d'application du Règlement (UE) n° 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 'le RGPD', et de 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 aux fins de l'exécution de sanctions pénales, et de libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après la 'directive Police-Justice' ou *LED* (***L**aw **E**nforcement **D**irective*)).

1. RAPPORT

À travers un contrôle 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 « MPA »[2]. 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[3]. Les membres et les membres du personnel de l'Organe de contrôle[4] disposent de compétences d'investigation et le comité de direction du COC peut, en marge des requêtes et recommandations, prendre également des mesures correctrices[5] comme «*ultimum remedium* » si le COC constate des infractions à la réglementation applicable.

Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG') visée dans 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 »* et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016 *« relative au traitement des données des passagers »*, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/14 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[6].

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

Enfin, l'Organe de contrôle est également chargé, dans le cadre de la législation sur la rétention des données et en vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE')[7], de la validation des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police, une matière dans le cadre de laquelle il exerce toutes les compétences qui lui ont été attribuées par le Titre 7 de la loi du 30 juillet 2018. Il est par ailleurs également chargé, en application de l'article 42 §3, 2e et 3e alinéas de la LFP, du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

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[8].

[2] **M**éthodes **P**articulières en police **A**dministrative.
[3] Article 240, 4° de la LPD.
[4] À savoir les membres du personnel du **D**ienst **O**nderzoeken / **S**ervice d'Enquête (DOSE) et du secrétariat, en l'occurrence des juristes et des experts en TIC.
[5] Articles 244 (compétences d'investigation des membres et des membres du personnel) et 247 (mesures correctrices à prendre par le comité de direction (DIRCOM) du COC) de la LPD.
[6] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.
[7] Telle que modifiée par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (*M.B.* du 8 août 2022).
[8] Article 248 de la LPD.

4. OBJECTIF DU CONTRÔLE ET MÉTHODOLOGIE

2. Le 12 novembre 2023, le COC a été informé par la zone de police de la province de Flandre occidentale[9] d'une brèche de sécurité[10] (notification d'une brèche de sécurité conformément aux modalités prévues à l'article 61 de la LPD). Sur la base des éléments de ce dossier, le COC a décidé d'initier un contrôle restreint dont les résultats sont consignés dans le présent rapport.

3. À la lecture de la réponse de la ZP de la province de Flandre occidentale selon laquelle il n'est pas procédé à un back-up des archives judiciaires numériques (saisies numériques), le COC a conclu à un problème dans la manière de travailler de la zone de police dès lors que celle-ci, de l'avis du COC, ne satisfait pas à la législation en vigueur, aux directives de la Direction de l'information policière et des moyens ICT (DRI) ni aux normes de sécurité applicables à l'échelle internationale pour la gestion des données.

Par ailleurs et à titre subsidiaire, le COC constate que les délais de réponse ont été dépassés et que la zone de police avait supprimé certaines données pertinentes dans les réponses transmises.

Pour cette raison, le COC a décidé de procéder à un contrôle restreint.

4. L'objectif du contrôle restreint était :

- de vérifier s'il a été satisfait aux dispositions légales du Titre 2 de la loi sur la protection des données du 30 juillet 2018 (LPD) et de la loi sur la fonction de police du 5 août 1992 (LFP) ainsi qu'aux règles régissant la sécurité de l'information, dont – notamment – la directive ministérielle contraignante du 13 juillet 2021[11], le courrier du 1er février 2023 du ministre de l'Intérieur concernant *« la sécurité de l'information, la sécurité des systèmes d'information et les modalités de traitement des informations policières »* et les directives pour la Police intégrée (GPI) telles qu'elles sont communiquées sur sa plateforme de communication (Sharepoint interne Bpol) ;
- d'évaluer la notification faite par la zone de police en fonction d'une part du délai légal prévu pour la notification de la brèche de sécurité et du temps écoulé, et d'autre part des documents transmis ;
- d'inventorier le cadre légal de la gestion et de la sécurisation des informations, en citant à la fois les directives et les sources de ces directives ;
- d'évaluer la chronologie de la notification de la brèche de sécurité ainsi que des questions et réponses pertinentes du dossier initial DB230034.

Le 5 avril 2024, le projet de rapport a été transmis en prélecture à la ZP de la province de Flandre occidentale afin que cette dernière fasse le cas échéant part de ses remarques dans le cadre du droit de réponse.

Par e-mail du 7 mai 2024 du chef de corps de la ZP de la province de Flandre occidentale, le COC a été informé des remarques et/ou des suggestions au sujet du projet de rapport et, dans la mesure où elles étaient pertinentes, en a tenu compte dans le présent rapport définitif.

5. CONCLUSIONS DE L'ENQUÊTE

5. Le 12 novembre 2023, la ZP de la province de Flandre occidentale a notifié au COC une brèche de sécurité qui impliquait la perte des données des saisies numériques de toute l'année 2022 à la suite d'une erreur humaine[12]. Voici les éléments pertinents qui pouvaient être distillés de cette notification (pièce 1) :

[9] Dossier DB230034 du COC.
[10] *« « brèche de sécurité » : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »* (art. 26, 11° de la LPD).
[11] Directive contraignante commune des Ministres de la Justice et de l'Intérieur relative aux mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2 de la Loi sur la Fonction de Police, *M.B.* 13 juillet 2021.
[12] Dossier DB230034 du COC.

1. RAPPORT

- Le 31 octobre 2023 vers 11:00 heures, un incident décrit comme suit s'est produit : *« Un collaborateur du carrefour d'information local, en voulant adapter un dossier, a supprimé[13] le répertoire « saisies numériques de 2022 ». »*
- Dans la rubrique *« Étapes suivantes »* du formulaire de notification, on peut lire : *« Le collaborateur a immédiatement avisé le service ICT et son chef de service, après quoi le service ICT a dans un premier temps essayé de récupérer les données. Les démarches suivantes ont été entreprises :*
    - *La corbeille locale a été contrôlée, mais sans résultat.*
    - *L'action « Ctrl-Z » a été effectuée, mais sans résultat.*
    - *Les lecteurs SMB-share et xxx-storage ne disposent pas d'une corbeille.*
    - *xxx, le fournisseur du système, a été contacté afin de vérifier comment les informations pouvaient être récupérées, mais il s'avère que ce n'est pas possible. »*
- Selon le formulaire de notification, cet incident a été détecté 10 jours plus tard, le 9 novembre 2023, lors de la concertation ICT bimensuelle, après quoi il a été notifié au COC.
- La ZP de la province de Flandre occidentale a décrit l'impact de l'incident en ces termes :
    - *« Le matériel numérique saisi pour servir de preuves dans un dossier pénal n'est plus disponible sur le serveur xxx pour les dossiers dont les tribunaux ont été saisis en 2022.*
    - *La saisie numérique consiste en des contenus de supports numériques, des enquêtes bancaires et du matériel visuel.*
    - *Au total, il s'agit de 502 procès-verbaux, parmi lesquels des procès-verbaux initiaux et des procès-verbaux subséquents. Le nombre de dossiers uniques n'a pas encore été établi. »*
- Cet impact doit être vu en combinaison avec le nombre de personnes concernées, à propos desquelles la ZP de la province de Flandre occidentale déclare qu'il s'agit de *« toute personne impliquée dans une enquête pénal dont le dossier a été déposé au greffe en 2022 et contient des pièces à conviction numériques »*. Cependant, les personnes concernées n'ont pas été informées au moment de la notification de la brèche de sécurité étant donné qu'elles n'étaient *« pas définies à ce moment »*.
- Cette notification avait été catégorisée par la ZP de la province de Flandre occidentale elle-même comme une *« Notification en plusieurs étapes – Première notification »*, de sorte que le COC est parti du principe que la ZP de la province de Flandre occidentale avait l'intention d'encore fournir elle-même des données complémentaires lorsqu'elle en aurait connaissance.

6. Le COC a ensuite posé des questions additionnelles. La correspondance échangée par e-mail le 30 janvier 2024 entre la ZP de la province de Flandre occidentale et le COC (pièce 4) démontre qu'il n'existe pas de back-up des informations perdues. Les remarques et constatations pertinentes suivantes peuvent être distillées de cet échange d'e-mails :

- Concernant la responsabilité de l'absence de back-up, la question posée par le COC était littéralement formulée en ces termes : *« Vous indiquez que le back-up n'avait pas été prévu en raison du coût de cette fonctionnalité. Pouvez-vous nous transmettre les documents étayant cette décision ? Qui a pris cette décision et qui en assume la responsabilité ? »*. La réponse de la ZP de la province de Flandre occidentale était littéralement formulée comme suit : *« Le chef de corps assume la responsabilité de cette décision. Cette décision n'a pas été documentée. Lors de la concertation hebdomadaire entre le service ICT et la Direction Gestion, les priorités sont abordées verbalement. En fonction des besoins des différents services en termes de moyens ICT et des budgets alloués à la zone de police, il est décidé des dépenses à soumettre au comité de direction. Par essence, un budget est prévu annuellement pour le renouvellement de l'infrastructure ICT, tant pour la connectivité que pour les serveurs, pour le renouvellement du matériel afin de permettre à nos collaborateurs de travailler de manière optimale (ordinateurs, écrans, …) et pour l'investissement dans des licences de logiciels permettant à nos collaborateurs de s'acquitter plus efficacement de leur tâche (par ex. les logiciels utilisés pour les enquêtes judiciaires LCCU) ; … »*.
- À la question du COC portant sur le back-up, qui était littéralement formulée comme suit dans l'e-mail susmentionné du 30 janvier 2024 : *« Il est question dans vos schémas d'un serveur de back-up xxx. Devons-nous en déduire que ce serveur n'a pas été acheté, ou est-il utilisé pour d'autres back-ups ? »*, la zone de police

[13] Soulignement du COC.

a répondu : *« Le serveur de back-up xxx a été acheté et est utilisé pour le back-up d'une part de l'architecture des serveurs numériques, et d'autre part des données du (des) serveur(s) de fichiers. Le lien OneDrive vous permettra d'accéder à un aperçu détaillé. Il n'est pas procédé à un back-up des données enregistrées sur le serveur qui contient les images des caméras ANPR, les images des bodycams et les archives judiciaires numériques. »*.

7. Le COC a également constaté que la communication avec la ZP de la province de Flandre occidentale laissait à désirer et a à cet égard épinglé les éléments suivants :

- il est apparu qu'il manquait dans les documents transmis certaines informations pertinentes dont le COC a besoin pour pouvoir dûment enquêter sur la brèche de sécurité ;
- le temps qui s'est écoulé entre le moment où la ZP de la province de Flandre occidentale a constaté la brèche de sécurité et le moment où elle l'a notifiée ;
- la question de savoir de quelles données il s'agit exactement – pas d'identification des personnes concernées ;
- les raisons et la motivation avancées pour justifier l'absence d'un système de back-up.

6. CADRE JURIDIQUE

6.1. Introduction

8. Il existe un cadre réglementaire pour la gestion et la sécurisation des informations. L'exposé qui suit présente de manière concise ce cadre réglementaire en mettant l'accent sur l'obligation de disposer de back-ups :

- la loi sur la protection des données du 30 juillet 2018, et en particulier les articles 50-51 et 60 (le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées) ;
- la *LED* 2016/680, et en particulier le considérant 53 ;
- la directive ministérielle contraignante[14] du 13 juillet 2021 ;
- cette directive ministérielle est basée sur le document *« Baseline Information Security Guidelines »* (*BSG*) du Centre pour la Cybersécurité Belgique (CCB), qui aborde également l'aspect du back-up ;
- le courrier du 1er février 2023 du ministre de l'Intérieur concernant *« la sécurité de l'information, la sécurité des systèmes d'information et les modalités de traitement des informations policières »*[15], adressé au commissaire général et à tous les chefs de corps de la police locale ;
- les directives concernant la gestion de l'information au sein de la GPI[16], qui accordent une attention spécifique à l'aspect du back-up ;
- les normes internationales utilisées dans les documents susmentionnés (ISO 27k).

6.2. Brèche de sécurité

9. L'article 26, 11° de la LPD définit une *« brèche de sécurité »* comme *« une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »*.

[14] Directive contraignante commune des Ministres de la Justice et de l'Intérieur relative aux mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2 de la Loi sur la Fonction de Police.
[15] À la page 4 de ce courrier, plus précisément sous le titre *« Cadre général »*, dans la 4e et dernière colonne sous l'intitulé *« Moyens technologiques »*, les *« back-ups »* sont explicitement mentionnés en tant que 7e des 9 moyens techniques énumérés.
[16] Voir notamment https://bpolb.sharepoint.com/sites/WiKiPolDataprotection-PSI_nl/SitePages/TECH_OPS_BACKUP.aspx.

10. La LPD s'étend dans les travaux parlementaires concernant les articles 60 à 62 sur la perte de données (brèche de sécurité) et dispose à ce sujet : *« Une brèche de sécurité risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social important. »*.

6.3. Mesures techniques et organisationnelles appropriées

11. En vertu de l'article 50 de la LPD, le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour contrer les risques qui menacent la protection des droits et libertés des personnes concernées. Bien qu'il soit dans ce contexte tenu compte de l'état des connaissances et des coûts de la mise en œuvre (travaux parlementaires, article 51 §1er de la LPD), *« la mise en œuvre de ces mesures ne peut pas dépendre uniquement de considérations économiques »*.

Par ailleurs, l'article 60 §2, 2° de la LPD dispose que le responsable du traitement met en œuvre les mesures nécessaires pour *« empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés[17] de façon non autorisée »*.

12. Il convient à cet égard d'attirer également l'attention sur l'article 60 §2, 9° de la LPD, qui impose au responsable du traitement l'obligation de *« garantir que les systèmes installés puissent être rétablis en cas d'interruption »*. Cette obligation implique notamment de prévoir un système de back-up afin que les données, en cas d'indisponibilité ou de perte des données sur le support de données, soient encore accessibles sur un autre support de données.

L'exposé des motifs concernant l'article 60 de la LPD (DOC 54/3126[18]) se penche à la page 105 sur cette obligation et fait référence à la norme ISO 27000, de sorte que ces normes doivent également s'appliquer.

6.4. Les normes ISO pertinentes

13. Les normes de base sur lesquelles se fonde la réglementation sont les normes ISO à partir de 27000. Il s'agit d'un ensemble de normes qui commencent toutes par le numéro 'ISO 27000' et qui sont pour cette raison désignées en tant que 'ISO 27k'. Les directives et recommandations (voir plus haut) font référence à ces normes. Cependant, le législateur n'attend pas de chaque professionnel qu'il analyse et applique lui-même ces normes, raison pour laquelle il les a transposées dans les directives susmentionnées. Mais ces normes n'en constituent pas moins une base et sont internationalement reconnues.

Bien qu'il s'agisse de normes industrielles, le législateur n'y fait pas moins explicitement référence, notamment dans l'exposé des motifs de la loi sur la protection des données (DOC 54/3126, page 105 concernant l'article 60 de la LPD).

La page WikiPol Dataprotection qui figure sur le site web interne de la police (Sharepoint GPI) fait également référence à ces normes.

6.5. La loi sur la fonction de police (LFP)

14. L'obligation relative à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel est également régie par l'article 44/4 §2 de la LFP, qui prévoit d'emblée d'en régler les modalités dans une directive ministérielle contraignante. La directive ministérielle contraignante en question est la directive contraignante susmentionnée du 13 juillet 2021.

[17] Soulignement du COC.

[18] www.lachambre.be, https://www.lachambre.be/FLWB/PDF/54/3126/54K3126001.pdf.

6.6. Directive ministérielle contraignante[19] du 13 juillet 2021

15. Cette directive ministérielle est contraignante, ce qui signifie qu'elle ne peut pas être considérée comme purement indicative, mais qu'elle impose une obligation juridique à ses destinataires. La directive s'adresse notamment aux chefs de corps : *« Les chefs de corps pour la police locale et le commissaire général, les directeurs généraux et les directeurs pour la police fédérale sont les garants de la bonne exécution de ces directives en ce qui concerne les banques de données visées à l'article 44/2, §§ 1er et 3 LFP. »*. En la matière, on peut donc considérer que le chef de corps assume la responsabilité (également juridique) de la mise en œuvre – ou du moins du contrôle de la mise en œuvre et de l'application – de cette directive. Le chef de corps endosse à cet égard la responsabilité finale.

16. Le champ d'application inclut également les banques de données policières dans lesquelles sont conservées les saisies numériques.

17. Cette directive dispose explicitement : *« Les services de police prévoient la protection nécessaire de l'information et des données qu'ils traitent contre la perte, la modification ou la destruction non autorisée, soit par accident soit par acte malveillant. »*.

18. Cette *« protection »* est également explicitée dans la directive au point *« 9) La sécurité liée aux opérations »* :
« Les mesures techniques minimales qui doivent être prévues pour les moyens ICT des services de police (6), sont :
…
- des procédures de back-up et de continuité des activités (sécurité opérationnelle). »

6.7. WikiPol Dataprotection

19. La DRI formule également quelques directives sur la manière dont la GPI doit gérer les données. Parmi les dispositions pertinentes pour le présent rapport, nous citerons la recommandation 'D.1.12 Back-up d'informations'[20]. Cette recommandation dispose *expressis verbis* : « *Parmi d'autres mesures, les sauvegardes sont exhaustives, les supports de sauvegarde sont adéquats et l'intégrité des sauvegardes est vérifiée à intervalles réguliers, afin de produire l'assurance que toutes les informations et tous les logiciels seront récupérables en cas d'incident, de défaillance ou de perte du support d'informations sauvegardées* ».

Cette recommandation de la page WikiPol Dataprotection s'inspire fortement des normes ISO 27k (voir plus haut).

6.8. Centre pour la Cybersécurité Belgique : « *Baseline Information Security Guidelines* » (*BSG*)

20. La directive ministérielle contraignante reconnaît explicitement s'être inspirée des *BSG*, de sorte qu'il est judicieux de revenir à la source et plus particulièrement d'examiner ce que les *BSG* stipulent au sujet de la gestion du back-up de données.

Ces dispositions figurent dans la directive sous les *« mesures techniques minimales qui sont prises pour l'architecture »*, où l'on peut lire : *« Disposer de procédures de back-up : réalisation, tests de restauration. »*.

Bien qu'il s'agisse de mesures absolument minimales, l'Organe de contrôle remarque qu'elles vont déjà beaucoup plus loin que le seul fait de 'posséder' un back-up puisqu'elles incluent également le fait de tester (régulièrement) la restauration.

---

[19] Directive contraignante commune des Ministres de la Justice et de l'Intérieur relative aux mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2 de la Loi sur la Fonction de Police.
[20] https://bpolb.sharepoint.com/sites/WiKiPolDataprotection-PSI_fr/SitePages/TECH_OPS_BACKUP.aspx

7. ÉVALUATION

7.1. Déroulement chronologique des faits pertinents après la notification de la brèche de sécurité portant la référence DB230034 du COC

21. Le COC a transmis un accusé de réception par e-mail du 13 novembre 2023 (pièce 2), dans lequel il posait également des questions additionnelles en accordant à la zone de police un délai de réponse jusqu'au 3 décembre 2023.
Le COC a ensuite demandé des précisions le 5 décembre 2023 (pièce 3). Ces précisions avaient principalement trait aux aspects suivants :

- le fait que certaines données de la documentation transmise avaient été 'masquées'[21] ;
- le fait que la zone de police indique qu'il n'est délibérément pas réalisé de back-up des archives numériques. Il s'agit en l'occurrence de « *contenus de supports numériques, d'enquêtes bancaires et de matériel visuel* »[22], rassemblés et conservés dans le cadre d'enquêtes pénales (pièce 1).

Vu la période de fin d'année, le délai de réponse avait été fixé à 5 semaines.

22. Le 10 janvier 2024, le COC a envoyé un e-mail de rappel accordant un nouveau délai jusqu'au 23 janvier 2024. Le 22 janvier 2023, le COC a été informé que le chef de corps n'avait pas encore été consulté. Finalement, les réponses aux questions du 5 décembre 2023 sont parvenues au COC le 30 janvier 2024 (pièce 4).

Dans l'exposé qui suit, nous confrontons les informations reçues de la ZP de la province de Flandre occidentale dans le cadre du dossier DB230034 à la réglementation et aux recommandations susmentionnées. Nous abordons ensuite la question des délais de réponse et de l'absence de certaines données pertinentes dont le COC a besoin pour pouvoir enquêter sur la brèche de sécurité.

23. Dans le cadre de l'enquête de contrôle, la ZP de la province de Flandre occidentale a objecté qu'un back-up des archives numériques et du matériel visuel impliquerait un coût additionnel de 180 KEUR (pièce 1, pièce 2, pièce 3) et/ou de 200 KEUR (pièce 5). Initialement, la ZP de la province de Flandre occidentale invoquait ce coût comme une raison de ne pas avoir prévu ni prévoir un back-up des archives numériques.

La ZP de la province de Flandre occidentale invoque dans ce contexte les éléments suivants (citation littérale, pièce 5) :

> *Il a été estimé que l'impact du risque de perte de données était minimal conformément à l'article 29 de la directive UE 2016/680 (degré de probabilité et de gravité des risques), tel que transposé à l'article 51 de la LPD, et ce en raison de l'accès restreint à ce serveur xxx et du nombre restreint de collaborateurs disposant de droits d'écriture sur ce serveur.*
>
> *La décision de ne pas disposer d'un back-up dans ce contexte spécifique reposait en partie sur des considérations économiques, mais se fondait tout autant sur le type de données qui sont conservées sur ce serveur.*
>
> *Il a été procédé à une évaluation du type de données nécessitant un back-up.*
>
> *Les données des archives numériques qui ont été perdues sont des pièces qui ont déjà été déposées au greffe. Il s'agit de captures d'écrans, de données retranscrites de la lecture de supports de données et de matériel photographique, autant de données qui ont été jointes aux procès-verbaux. Les procès-verbaux sont gérés et conservés dans le système de la police locale, qui en réalise également un back-up. Additionnellement, un exemplaire intégral est conservé dans une archive numérique xxx.*

Le COC ne peut pas adhérer à ce raisonnement, et ce en raison de divers éléments et arguments qui sont exposés dans le présent rapport, dont les suivants :

[21] Ces données sont des adresses IP internes et des noms de collaborateurs de projet externes figurant dans le document qui décrit l'architecture et le projet. Or, le COC a en vertu de ses compétences un accès illimité à **toutes** les données (article 244 §1er de la LPD).
[22] Selon la notification de la brèche de sécurité.

- en soi, l'aspect économique ne peut pas être invoqué comme une raison suffisante pour ne pas prévoir de back-up ;
- de l'avis du COC et pour les raisons évoquées dans le présent rapport, la perte de données a bel et bien un impact sérieux ;
- il n'existe aucune preuve que les archives numériques perdues se composent **exclusivement** de pièces et de procès-verbaux déjà déposés au greffe. Il semble d'ailleurs à cet égard y avoir une contradiction[23] dans la réplique du 6 mai 2024 de la ZP de la province de Flandre occidentale (pièce 5) ;
- l'enregistrement final des procès-verbaux, au bout d'un certain temps (le temps nécessaire pour établir et finaliser les procès-verbaux, les transmettre au parquet et enfin les archiver sur le serveur xxx), ne peut pas être considéré comme une alternative valable à un back-up direct des archives numériques ;
- la perte de données a ou peut avoir de toute manière un impact procédural ou pénal en ce sens qu'il n'est plus possible d'ordonner une enquête (complémentaire) en cas par exemple de contestations quant au contenu (correct) d'un procès-verbal (que ce soit durant l'enquête pénale ou lors de l'instruction à l'audience), puisque les données originales qui ont servi de source pour l'établissement des procès-verbaux ont été perdues[24]. Cet impact (négatif) peut être préjudiciable tant au ministère public qu'au(x) prévenu(s) ou à la (aux) partie(s) civile(s) ou victime(s) (voir aussi le point 34) ;
- la limitation des droits d'accès n'a d'utilité que si un principe du moindre privilège est implémenté. Selon le principe du moindre privilège, les rôles sont clairement définis au préalable et l'utilisateur (*user*) n'endosse parmi les rôles qui lui ont été attribués qu'un seul rôle s'assortissant uniquement des droits absolument nécessaires pour l'exécution des tâches qu'il doit réaliser à ce moment. Ce principe implique d'une part que ces rôles sont clairement définis et séparés, et d'autre part que les utilisateurs doivent temporairement changer de rôle pour les accès qui requièrent un niveau de priorité supérieur ou différent, comme la suppression (l'effacement) de données.

Bien que le COC comprenne que l'installation d'un système de back-up puisse représenter un coût (considérable), on ne peut passer outre à la responsabilité qui incombe au responsable du traitement – en l'occurrence la ZP de la province de Flandre occidentale – de prévoir un back-up comme le prescrit la réglementation.

Dans la phase finale du droit de réponse, la ZP de la province de Flandre occidentale a finalement déclaré (littéralement) : *« Nous avons déjà dû beaucoup rationaliser les dépenses ces dernières années, mais nous sommes certainement disposés à envisager (soulignement propre) à l'avenir l'achat du serveur de back-up additionnel (estimé à environ 200.000 €). Cette possibilité devra être évaluée en concertation avec l'autorité administrative. »* (pièce 5). On peut en déduire que la question n'a encore jamais été soumise à l'autorité administrative.

7.2. Délais de notification et de réponse

24. Selon la notification de la brèche de sécurité, l'incident s'est produit le 31 octobre 2023 vers 11:00 heures. Bien que la notification indique que cet incident a été notifié 'immédiatement' (pièce 1), il a fallu attendre le 9 novembre 2023 pour que cette brèche de sécurité soit abordée par la ZP de la province de Flandre occidentale lors de la *« concertation bimensuelle interne avec le service ICT concernant les affaires courantes ainsi que les incidents constatés et la manière d'y remédier »*, et ensuite le 12 novembre 2023 pour qu'elle soit notifiée au COC. Or, les brèches de sécurité doivent être notifiées dans les 72 heures de leur constatation[25]. **La ZP de la province de Flandre occidentale ne fournissait dans sa notification aucune explication au fait que cet incident n'ait été notifié qu'au bout de 2 (deux) semaines plutôt que dans les 72 heures**.

25. Le 5 décembre 2023, le COC a demandé des renseignements complémentaires. Le COC s'efforce toujours de prévoir dans ces cas-là un délai raisonnable et avait en l'occurrence fixé le délai de réponse à 5 (cinq) semaines pour tenir compte de la période de fin d'année. La réponse était donc attendue pour le 10 janvier 2024 au plus tard. Ne la recevant

[23] Il est en effet dit d'une part à la page 2 (avant-dernier §) : *« Les données des archives numériques qui ont été perdues sont des pièces qui ont déjà été déposées au greffe. »*, alors qu'on peut lire à la page 3 (3e §, 3e tiret) : *« Archives numériques : contiennent toutes les preuves qui ne peuvent **pas** être déposées au greffe et qui peuvent être invoquées à l'audience. »*.

[24] La ZP de la province de Flandre occidentale le confirme aussi implicitement dans sa réplique du 6 mai 2024 (pièce 5) en indiquant à la page 3 (3e §, 3e tiret) : *« Archives numériques : contiennent toutes les preuves qui ne peuvent pas être déposées au greffe **et qui peuvent être invoquées à l'audience**. »*. Cette possibilité peut se présenter non seulement « à l'audience », mais aussi pendant toute l'enquête pénales.

[25] Considérant 61 de la *LED* et article 30/1 transposé à l'article 61 §1er de la LPD.

pas, le COC a envoyé un e-mail de rappel dans lequel il accordait un délai de réponse supplémentaire de 2 (deux) semaines, fixant la date ultime de réponse au 23 janvier 2024. Le 22 janvier 2024, la ZP de la province de Flandre occidentale a répondu que ce délai ne pourrait pas être respecté. La réponse est finalement parvenue au COC le 30 janvier 2024.

Le COC constate que la ZP de la province de Flandre occidentale a mis près de 2 (deux) mois pour répondre à l'Organe de contrôle.

7.3. Données manquantes

26. Dans sa communication, la ZP de la province de Flandre occidentale a transmis au COC le document présentant l'architecture et le projet d'introduction de l'infrastructure xxx. En ouvrant le document, le COC a cependant remarqué que certaines données de ce document avaient été masquées sans même que la zone de police ne s'en justifie.

Concrètement, il s'agit d'adresses IP ainsi que des noms des collaborateurs de projet (externes) (et donc sous-traitants de la zone de police). Cependant, ces données peuvent par la suite revêtir de l'importance dans le cadre de vérifications ultérieures portant par exemple sur la protection et la ségrégation du réseau et les parties externes impliquées, ainsi que sur les conseils que ces dernières pourraient avoir fournis lors de l'installation de l'architecture et des appareils achetés.

27. Hormis les exceptions prévues à l'article 245 §2, 2e alinéa, dernière phrase de la LPD (les informations qui concernent une information ou une instruction judiciaire en cours ou qui doivent être tenues secrètes pour protéger l'intégrité physique des personnes), le COC a accès à **toutes les informations** qu'il demande en vertu de l'article 244 §1er de la LPD. Aucune de ces exceptions n'a toutefois été invoquée par la ZP de la province de Flandre occidentale, et il semble d'ailleurs qu'elle n'ait pas la possibilité de les invoquer.

28. À la demande explicite du COC, les documents contenant l'intégralité des données ont finalement été transmis.

Recommandation n° 1

Documenter et communiquer de manière transparente aux parties prenantes les décisions ayant un impact sur la protection des données en général et sur les procédures ICT en particulier.

Dans le cadre du droit de réponse, la ZP de la province de Flandre occidentale a indiqué ce qui suit (pièce 5, citation littérale) :

- *« Nous sommes d'accord que nous devons consentir en la matière des efforts additionnels pour parvenir à une approche reposant davantage sur une analyse des risques et déterminer les aspects que nous considérons ou non comme critiques. L'année dernière, il a été décidé de prévoir un budget pour la réalisation d'un audit et d'un test d'intrusion (« pentest ») afin d'inventorier les points faibles de nos systèmes ICT (cette décision a été prise bien avant l'incident, justement parce que nous souhaitons disposer d'une bonne vue d'ensemble des aspects critiques de notre gestion de l'information). »*
- *« Dans le sillage du résultat de cet audit, nous avons décidé d'élaborer un plan de sécurité et de réaliser les actions urgentes, compte tenu de la législation à laquelle vous faites référence dans ce rapport et en nous aidant des outils « cyfun » mis à disposition par le CCB. Nous bénéficions dans ce contexte du soutien d'un consultant externe. ».*

Le COC prend acte des mesures en cours et projetées dont la zone de police a fait état.

7.4. Définition du concept de « back-up »

29. Le concept de back-up est un concept technique qui consiste à conserver des données enregistrées – dans l'état dans lequel elles se trouvent à un moment donné – sur un autre support de données de manière à pouvoir en cas de calamité – perte, incident de sécurité (virus, indisponibilité à la suite d'une panne de matériel, rançongiciel, erreur humaine ayant engendré la modification ou la suppression des données, etc.) – 'récupérer' les données dans l'état dans lequel elles se trouvaient au moment du back-up. De plus, un back-up ne se limite pas à une seule version antérieure, mais remonte de plusieurs versions dans le temps.

30. Le concept de back-up ne peut pas être confondu avec ceux de haute disponibilité et de redondance, qui consistent à faire en sorte que les systèmes restent disponibles même si une partie du matériel tombe en panne. De fait, les données d'un système servant à garantir une haute disponibilité qui sont effacées ou modifiées disparaissent bel et bien du système et seul le back-up permet alors d'encore les restaurer.

31. En ce sens, le COC considère le '*serveur xxx*' de la ZP de la province de Flandre occidentale comme un système servant à garantir une haute disponibilité, mais ne prévoyant pas les mesures de back-up nécessaires pour les données des archives numériques et du matériel visuel dont il est question ici.

32. La législation et la réglementation applicables font référence dans ce contexte aux *« mesures techniques et organisationnelles »* visant à garantir la disponibilité et à empêcher la perte de données.

7.5. Back-up

33. Comme le prescrivent les sources juridiques (la directive ministérielle contraignante du 13 juillet 2021), les directives internes de la police (WikiPol), les recommandations des autorités (les *BSG* du Centre pour la Cybersécurité Belgique) et les normes internationales (ISO 27k), la réalisation d'un back-up n'est pas seulement une précaution d'usage dans le cadre de la gestion de l'information, mais tout bonnement une obligation légale. Dans ses réponses, la ZP de la province de Flandre occidentale indique explicitement choisir de ne **pas** se conformer à ces obligations en ce qui concerne *« les images des caméras ANPR, les images des bodycams et les archives judiciaires numériques »* (pièce 3).

34. Dans le cadre de l'information et des poursuites pénales, la perte de saisies numériques peut avoir des conséquences (graves) d'une part pour l'enquête pénale (information/instruction et le cas échéant l'instruction à l'audience), et d'autre part pour les droits de la défense étant donné que les faits ne peuvent plus être prouvés du fait de la perte des (potentielles) preuves et pièces à conviction. Les victimes éventuelles peuvent également potentiellement en subir les conséquences dans la mesure où la perte des données rend impossible, ou du moins complique fortement l'information et les poursuites pénales. Le COC ne peut qu'espérer que les conséquences pénales (et civiles) sont restées acceptables, mais n'est pas en mesure d'en juger concrètement.

Dans le cadre du droit de réponse, la ZP de la province de Flandre occidentale a souligné que des back-ups étaient en revanche réalisés pour d'autres systèmes. Bien que le COC prenne acte de cette remarque de la ZP de la province de Flandre occidentale, il convient de faire observer que l'enquête de contrôle porte uniquement sur la perte des données des archives judiciaires numériques, de sorte que les autres systèmes de traitement de la ZP de la province de Flandre occidentale ne sont pas pris en considération ici.

Recommandation n° 2

Prévoir des mesures pour garantir la sécurité de l'information et en l'occurrence pour empêcher la perte de données, notamment en réalisant des back-ups conformément à toutes les réglementations et normes industrielles en vigueur (susmentionnées).

Dans le cadre du droit de réponse, la ZP de la province de Flandre occidentale a déclaré (pièce 5, citation littérale) :

- *« Comme nous le disions dans la communication au sujet de la perte des données, aucun membre opérationnel ne dispose encore de droits d'écriture sur le serveur xxx. Les fichiers enregistrés dans les archives numériques sont placés par le carrefour d'information local dans un répertoire de leur NAS et enregistrés sur le serveur xxx par le biais d'un script. Au bout de 24 heures, ces fichiers peuvent encore uniquement être lus. »*
- *« … ».*

En formulant cette remarque, la ZP de la province de Flandre occidentale laisse entendre que les données perdues des saisies numériques ne seraient 'pas critiques'. En effet, si elles l'étaient, elles auraient été incluses dans le schéma de back-up. Le COC n'adhère pas au raisonnement de la ZP de la province de Flandre occidentale selon lequel ces données ne seraient 'pas critiques'. Lors d'une saisie numérique, diverses données sont rassemblées et sont ou non intégrées dans les dossiers judiciaires. Ce traitement implique (souvent uniquement) des sélections, ce qui implique que les données ne sont **pas toutes** transmises (ou ne sont que rarement toutes transmises) et qu'il est fréquent que des données soient « traitées » (résumées, réduites aux métadonnées, etc.). Or, comme nous le disions plus haut, il peut être nécessaire de revenir durant l'enquête pénale ou lors de l'instruction à l'audience (première instance, appel, renvoi

après cassation) aux données initiales pour en établir la force probante, en cas de contestations des preuves, pour des raisons de contextualisation, pour approfondir l'enquête, pour apporter des précisions, etc. Le COC maintient donc que ces données sont bel et bien des 'données critiques' et doivent par conséquent être incluses dans le back-up.

7.6. Délais de réponse

35. Après la notification de l'incident, le COC a constaté que la ZP de la province de Flandre occidentale a attendu très longtemps avant de répondre aux questions du COC. L'ampleur de l'incident, qui était en l'occurrence décrit dans la notification comme une potentielle perte de preuves, laissait cependant à penser que l'incident méritait de se voir accorder une priorité plus élevée.

Dans le cadre du droit de réponse, la ZP de la province de Flandre occidentale a déclaré à ce sujet (pièce 5, citation littérale) :

> *« Nous nous devons d'ajouter ici que la priorité lors de la première notification était de vous informer de la perte des données. La notification a été effectuée tardivement parce que nous étions initialement partis du principe que les données pourraient être intégralement récupérées. La perte des données était due à une erreur humaine sans aucune intention malveillante. Ce n'est qu'après concertation avec le sous-traitant et consultation du helpdesk xxx qu'il a été établi que ces données ne pourraient pas être récupérées.*
>
> *Le délai de réponse accordé pour les questions additionnelles a malheureusement coïncidé avec la période des fêtes de fin d'année, de sorte qu'il n'a effectivement pas été possible de réunir les différentes personnes concernées pour une concertation. La détermination du nombre exact de dossiers impactés a été tout un exercice. Aujourd'hui, nous avons décidé de cesser les recherches entreprises pour retrouver les preuves perdues, et de transmettre le nombre final au parquet. ».*

Le COC trouve important que les délais légaux imposés pour la notification (72 heures après l'incident) soient respectés, même si l'on parvient par la suite à « réparer » la perte de données. Le COC s'efforce aussi toujours d'être réaliste dans les délais de réponse retenus ; en l'occurrence, le COC avait par exemple déjà tenu compte de la période des fêtes de fin d'année, comme nous le disions aux points 21 et 25. Autrement dit, le COC tient à faire remarquer que pour la notification de la brèche de sécurité proprement dite, le fait que les données puissent ou non être récupérées n'est pas pertinent puisqu'il ne change rien à la perte de données.

Recommandation n° 3

Implémenter les processus permettant de notifier dans les délais impartis une brèche de sécurité portant atteinte à la protection des données, de manière à garantir en tout temps un traitement correct et ponctuel.

Dans le cadre du droit de réponse, la ZP de la province de Flandre occidentale a indiqué (pièce 5, citation littérale) :

- *« Il existe à ce jour une procédure de gestion des incidents, et la procédure consiste normalement à … »*
- *« La perte des données a en effet démontré que le processus n'était pas encore ancré dans les usages et que des efforts de sensibilisation additionnels sont nécessaires. »*
- *« Cet aspect est également repris dans le plan de sécurité, et il faudra du temps pour qu'il s'intègre à notre culture. »*.

Le COC prend acte des mesures en cours et projetées dont la zone de police a fait état.

7.7. La compétence de supprimer des données

36. Le 2e alinéa du point 11 fait référence à l'article 60 §2, 2° de la LPD, selon lequel la ZP de la province de Flandre occidentale doit prendre des mesures pour empêcher que des supports de données puissent, notamment, être supprimés de façon non autorisée. Cette obligation fait partie intégrante du devoir général de prendre des mesures techniques et organisationnelles appropriées pour notamment protéger l'intégrité et la disponibilité des données à caractère personnel. Ces deux garanties sont matérialisées dans la directive commune contraignante des Ministres de la Justice et de l'Intérieur *« relative aux règles d'accès des membres des services de police à la banque de données*

nationale générale, aux banques de données de base, particulières et techniques » du 10 juillet 2021[26] et élaborées plus en détail dans la fiche D41 non publiée de la directive MFO-3.

37. Il en découle qu'un membre de la GPI est uniquement légitimement compétent pour accéder aux informations et données à caractère personnel visées à l'article 44/1 §1er de la LFP lorsque cet accès est nécessaire et proportionnel en fonction du rôle qui lui a été attribué. Le rôle attribué a également un impact sur la portée et la délimitation de la compétence de traitement dont certains traitements font ou ne font pas partie. Il est évident que la possibilité de **supprimer** (ce qui, pour toute clarté, constitue un traitement) des informations et des données à caractère personnel de l'environnement policier ne peut pas être accordée à tous les membres de la GPI (ni en l'occurrence de la zone de police).

38. Un membre du personnel peut endosser à différents moments des rôles différents. Pour cette raison, il peut être nécessaire qu'un membre du personnel passe d'un rôle à l'autre. Un membre du personnel investi du rôle de 'collaborateur du carrefour d'information local' peut par exemple créer et consulter des données, mais pas en supprimer. Pour supprimer des données, il doit passer au rôle de 'gestionnaire/administrateur (système)', rôle qu'il n'endosse pas de manière permanente, mais qu'il utilise uniquement pour une finalité spécifique nécessitant ce rôle. La journalisation des traitements doit alors notamment prouver quel collaborateur (qui) a effectué quelle action (quoi) à quel moment et dans quel rôle.

39. L'avis d'initiative non publié DD210006 du 24 mars 2021 du COC (disponible sur le Sharepoint interne de la GPI) *« relatif au développement d'une politique de profil en général, à l'octroi du profil de recherche « exploitation avancée », en particulier aux membres de la police intégrée, et relatif à l'utilisation de l'application BNG contrôle par le collaborateur de l'accueil »* stipule à ce sujet :

*Il faut également rappeler que la MFO 3 – une directive **contraignante** pour **tous** les services de police au sens de l'art. 62, 6° de la Loi sur la Police Intégrée du 7 décembre 1998 – dispose dans sa fiche D41 entre autres :*

- *« Il sera tenu compte des besoins opérationnels et des tâches effectivement exercées par l'utilisateur dans l'attribution des accès aux applications ».*
- *« Le responsable tendra à procurer à chaque membre de son personnel un accès en BNG personnalisé, c'est-à-dire en concordance avec les tâches exercées par ce membre ».*

Il convient en la matière d'attribuer des accès aussi personnalisés que possible à la BNG en déterminant *mutatis mutandis* les rôles pour toutes les autres applications et banques de données policières.

Recommandation n° 4

Définir clairement l'accès aux systèmes dans des rôles, avec pour chaque rôle d'une part l'accès indispensable, mais d'autre part le moins possible d'accès (principe du moindre privilège). Cela implique que les personnes doivent temporairement changer de rôle pour les accès nécessitant un niveau de priorité supérieur, comme la suppression (l'effacement) de données. Les réglementations et normes industrielles en vigueur (susmentionnées) doivent pour ce faire être suivies.

Dans le cadre du droit de réponse, la ZP de la province de Flandre occidentale déclare (pièce 5, citation littérale) :

- *« Il existe une procédure d'onboarding et d'offboarding dans le cadre de laquelle les demandes d'accès aux applications sont passées en revue et évaluées lors de la concertation hebdomadaire avant d'accorder et/ou de modifier les accès. ».*
- *« Nous ajoutons les procédures dans le OneDrive partagé. »*.

Cette précision ne constitue cependant pas une réponse à la recommandation de travailler avec des rôles et d'implémenter le principe du moindre privilège.

[26] *M.B.* 13 juillet 2021.

8. CONCLUSION

39. La réglementation et les directives sont claires : chaque système informatique de la police doit être doté de mesures efficaces en matière de sécurité de l'information, dont un back-up. Le système de la ZP de la province de Flandre occidentale qui a été touché par la brèche de sécurité fait partie des systèmes informatiques de la police, de sorte qu'il aurait fallu prévoir un système de back-up efficace pour les archives judiciaires numériques.

40. La ZP de la province de Flandre occidentale indique que le chef de corps a choisi de ne pas installer de back-up pour les *bodycams*, les caméras ANPR et les archives judiciaires numériques, et qu'il en assume l'entière responsabilité. Quelle que soit la portée de ce sens des responsabilités, ce processus décisionnel n'a pas été documenté et ne peut manifestement pas être étayé. L'argument selon lequel ce n'est économiquement pas faisable, en plus de ne pas pouvoir être retenu sur la base de la législation et de la réglementation en vigueur, n'est, vu les conséquences potentiellement très graves, pas non plus défendable du point de vue de l'ancien 'bon père de famille' (que le Nouveau Code civil désigne à présent sous le terme de 'personne prudente et raisonnable').

41. La perte des données des archives judiciaires numériques, avec ses conséquences (potentiellement) graves pour le fonctionnement de la Justice ainsi que pour toutes les personnes concernées et parties prenantes, aurait pu être évitée si la zone de police avait consenti les efforts et entrepris les démarches nécessaires (également à l'égard de ses autorités de police) pour garantir un niveau de protection optimal en termes de sécurité de l'information des archives judiciaires numériques. Et prévoir un back-up des archives judiciaires numériques est dans ce contexte l'évidence même.

42. Le COC fait à cet égard remarquer que les délais légaux n'ont pas été respectés pour la notification de l'incident et qu'un temps inutilement long s'est ensuite écoulé avant qu'il ne soit répondu aux différentes demandes d'informations de l'autorité de contrôle.

43. De plus, le COC fait remarquer qu'il manquait des données dans la première communication, alors que le COC doit avoir un accès illimité à **toutes** les informations disponibles.

44. Enfin, des mécanismes doivent être mis en place pour qu'un membre de la zone de police de la province de Flandre occidentale ne puisse pas supprimer aussi aisément des informations et des données à caractère personnel d'une banque de données policière.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

adresse les recommandations suivantes à la zone de police de la province de Flandre occidentale :

Recommandation n° 1

Documenter et communiquer de manière transparente aux parties prenantes les décisions ayant un impact sur la protection des données en général et sur les procédures ICT en particulier.

Recommandation n° 2

Prévoir des mesures pour garantir la sécurité de l'information et en l'occurrence pour empêcher la perte de données, notamment en réalisant des back-ups conformément à toutes les réglementations et normes industrielles en vigueur (susmentionnées).

Recommandation n° 3

Implémenter les processus permettant de notifier dans les délais impartis une brèche de sécurité portant atteinte à la protection des données, de manière à garantir en tout temps un traitement correct et ponctuel.

Recommandation n° 4

1. RAPPORT

Définir clairement l'accès aux systèmes dans des rôles, avec pour chaque rôle d'une part l'accès indispensable, mais d'autre part le moins possible d'accès (principe du moindre privilège). Cela implique que les personnes doivent temporairement changer de rôle pour les accès nécessitant un niveau de priorité supérieur, comme la suppression (l'effacement) de données. Les réglementations et normes industrielles en vigueur (susmentionnées) doivent pour ce faire être suivies.

décide de **ne pas assurer de suivi actif** des recommandations susmentionnées adressées à la zone de police de la province de Flandre occidentale,

informe néanmoins la zone de police de la province de Flandre occidentale qu'elle doit en tout temps, en sa qualité de responsable du traitement (fonctionnel) et conformément aux principes et obligations du Titre 2 de la loi sur la protection des données, pouvoir prouver à l'Organe de contrôle qu'elle respecte les règles en matière de protection des données et de gestion de l'information policière, par exemple dans le cadre d'un éventuel autre contrôle ou dossier ou de contrôles par échantillonnage organisés par le COC.

Rapport approuvé le 11 juin 2024 par l'Organe de contrôle de l'information policière.

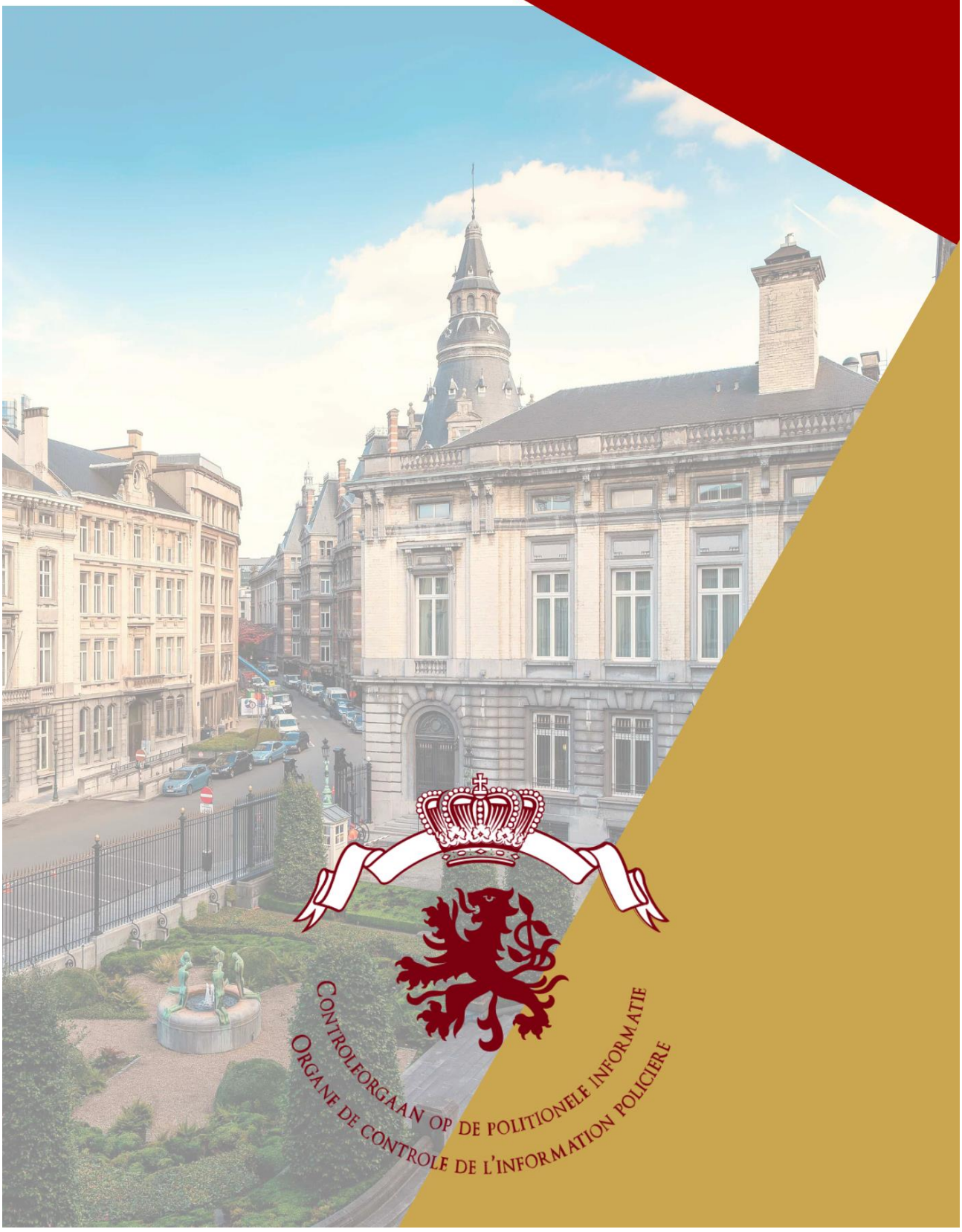
Copie :

- au bourgmestre de Flandre occidentale[27]
- au procureur du Roi de Flandre occidentale[28]

Pour l'Organe de contrôle,

Frank SCHUERMANS
Président *a.i.* (s)

[27] Cf. art. 237, 3e alinéa de la loi sur la protection des données.
[28] Cf. art. 237, 4e alinéa de la loi sur la protection des données.



Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière