

CONTRÔLE TECHNIQUE

CONTRÔLE TECHNIQUE EFFECTUÉ PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE AUPRÈS DE LA DIRECTION DE L'INFORMATION POLICIÈRE ET DES MOYENS ICT DE LA POLICE FÉDÉRALE ET DE LA ZP ANTWERPEN (ANVERS) CONCERNANT FOCUS

RAPPORT

Référence : CON23005



TABLE DES MATIÈRES

1. INTRODUCTION 3
2. OBJECTIF DU CÔNTROLE ET DE LA VISITE ET MÉTHODOLOGIE 3
3. LE CADRE JURIDIQUE PERTINENT 4
3.1. Les principes de base des traitements de données effectués par la police 4
3.2. Les banques de données de base 4
3.3. Les banques de données particulières (GBO) 4
3.4. Les banques de données techniques 5
3.5. L'interconnexion des banques de données 5
3.6. Les délais de conservation dans les banques de données de base et les banques de données particulières 6
4. CONCLUSIONS DE L'ENQUÊTE 6
4.1. Qu'est-ce que FOCUS? 6
4.2. La création de FOCUS@GPI et FOCUS Interzonal 6
4.3. Modules FOCUS@GPI et FOCUS Interzonal 7
4.3.1. Aperçu des modules FOCUS@GPI et FOCUS Interzonal 7
4.4. Imprécisions restantes et préoccupations du COC 8
4.4.1. Banque de données de base ou particulière ? 9
4.4.5. Gestion des accès 11
4.4.6. Journalisation 13
4.4.7. AIPD 14
4.4.8. Risque de et par (des) doubles traitements 14
4.4.9. Délais de conservation et exactitude des données à caractère personnel 14
4.4.10. Archivage 15
4.4.11. Sécurité de l'information 15
5. CONCLUSION 16

1. INTRODUCTION

1. Dans le cadre de ses compétences en tant qu'autorité de contrôle des traitements de données de la police intégrée organisée à deux niveaux (GPI), l'Organe de contrôle de l'information policière (ci-après 'l'Organe de contrôle' ou 'le COC') a décidé d'effectuer auprès de la Direction de l'information policière et des moyens ICT (DRI) et de la zone de police Antwerpen (Anvers, ZPA) un contrôle technique concernant les applications 'FOCUS@GPI' et 'FOCUS Interzonal'. Le présent rapport présente les constatations de l'enquête menée dans le cadre de ce contrôle technique. Les conclusions et les recommandations qui y sont formulées découlent de ces constatations et s'adressent donc aux responsables fonctionnels de la police au niveau politique et au niveau opérationnel.

2. OBJECTIF DU CONTRÔLE ET DE LA VISITE ET MÉTHODOLOGIE

2. Le 09.02.2024, le COC a effectué de sa propre initiative un 'contrôle technique'[1] auprès de la Direction de l'information policière et des moyens ICT (DRI) et de la zone de police d'Anvers (ZPA). Ce contrôle ne faisait donc pas suite à une plainte (individuelle) ni ne découlait de l'existence d'indications (concrètes) d'un non-respect, par la DRI et/ou par la ZPA, de la législation et de la réglementation.

3. À travers ce contrôle technique, le COC souhaite se faire une idée des processus de travail de la DRI et de la ZPA dans le cadre de la gestion de l'information policière, et plus spécifiquement dans les applications/banques de données 'FOCUS@GPI' et 'FOCUS Interzonal' et toutes les fonctionnalités qui y sont proposées.

4. Le contrôle s'est déroulé en quatre phases.

Durant la première phase, le COC a, dans son courrier du 09.02.2024 annonçant le contrôle, prié la DRI et la ZPA de transmettre les informations et documents requis repris ci-après :

- si un audit a été réalisé (en l'occurrence pour examiner la nécessité opérationnelle, la faisabilité juridique et technique et les vulnérabilités techniques préalablement à l'établissement d'une AIPD[2]) au sujet de FOCUS (voir le chapitre 4.4.4) ;
- les documents stratégiques internes concernant la création et l'utilisation de FOCUS@GPI et FOCUS Interzonal ;
- les notes permanentes/directives internes concernant FOCUS@GPI et FOCUS Interzonal.

La deuxième phase consistait en l'analyse des informations et documents reçus le 18.04.2024.

Durant la troisième phase, le COC a transmis le 25.07.2024 un questionnaire établi sur la base de l'analyse des documents transmis au cours de la deuxième phase par la DRI et la ZPA afin d'obtenir des précisions concernant les informations et les documents transmis.

En réponse à ces questions additionnelles, le COC a reçu de la DRI et de la ZPA une invitation en vue d'un entretien préparatoire. Cette réunion a eu lieu le 26.09.2024 au commissariat principal de la ZPA en présence des collaborateurs de la ZPA et de la DRI qui sont impliqués dans l'utilisation de FOCUS.

Dans une quatrième phase, le COC a reçu le 04.10.2024 un courrier accompagné d'un grand nombre de documents en réponse aux questions posées et aux documents demandés par écrit par le COC, ainsi que des réponses aux questions posées pendant la réunion.

Dans une cinquième phase, le projet de rapport a été transmis le 16.03.2026 pour prélecture avec droit de réponse au chef de corps de la ZP d'Anvers et au directeur du DTO de la DRI. Le COC a reçu les explications additionnelles le 17.04.2026. Dans la mesure de leur pertinence, ces explications ont été intégrées dans le texte avec les réponses qu'elles requéraient.

5. Au total, 142 documents ont été transmis au COC dans le cadre de ce contrôle. Dans l'intérêt de la clarté et de la lisibilité du présent rapport, nous faisons référence lorsque c'est pertinent à la date (de réception) du document dont il est question.

[1] Pour les différents types de contrôles et la signification et la teneur d'un contrôle technique, voir le Rapport d'activité 2024 de l'Organe de contrôle de l'information policière (p. 50, point 55), https://www.organedecontrole.be/publications/rapports-annuels.

[2] Analyse d'impact relative à la protection des données, en anglais *DPIA* pour *Data Protection Impact Assessment*.

3. LE CADRE JURIDIQUE PERTINENT

3.1. Les principes de base des traitements de données effectués par la police

6. Les principes de base de la gestion de l'information policière découlent d'une lecture conjointe des dispositions de l'article 44/1 §1er de la LFP et de l'article 28 de la LPD[3]. Les données à caractère personnel :

a) sont traitées de manière licite et loyale ;

b) sont collectées pour des finalités déterminées, explicites et légitimes[4] et ne sont pas traitées d'une manière incompatible avec ces finalités ; sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ;

c) sont exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables sont prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;

d) sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;

e) sont traitées de façon à garantir la sécurité des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

3.2. Les banques de données de base

7. L'article 44/11/2 §1er de la LFP dispose que les banques de données de base sont les banques de données policières créées au profit de l'ensemble de la police intégrée et qui ont pour finalité d'exécuter les missions de police administrative et de police judiciaire en exploitant les données à caractère personnel et informations qui y sont incluses et en informant les autorités compétentes de l'exercice de ces missions.

3.3. Les banques de données particulières (GBO[5])

8. L'article 44/11/3 §1er de la LFP stipule que la création d'une GBO n'est possible que si elle est nécessaire et proportionnelle. La création d'une GBO est donc soumise aux conditions cumulatives suivantes :
- pour des besoins particuliers ;
- pour l'exercice de missions de police administrative ou judiciaire.

9. L'article 44/11/3 §2 de la LFP dispose en outre que la création d'une GBO doit (additionnellement) être motivée par au moins un des besoins particuliers suivants (finalités) :

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[6] ;

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.

10. Les conditions à remplir pour la création d'une GBO sont donc clairement définies par la loi.

Ces dispositions légales forment dès lors le cadre de référence sur lequel le COC se base pour considérer une banque de données comme une GBO. Avant d'inclure cette banque de données dans REGPOL (le registre unique des traitements

[3] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
[4] Il s'agit en l'occurrence des finalités de police administrative et judiciaire qui, en fonction des circonstances, sont encore délimitées avec davantage de précision dans la LFP, comme nous le montrerons dans le présent avis.
[5] L'acronyme GBO utilisé pour désigner les banques de données particulières vient du néerlandais '**G**egevensbank **B**ijzondere **O**mstandigheden'.
[6] Le titre de cette loi a entretemps été modifié en : *« Loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé »*.

visé à l'article 145 de la LPI[7]) ou dans un registre local, le responsable du traitement doit examiner si la création d'une GBO est nécessaire et si l'enregistrement de données projeté répond aux conditions légales pour que la banque de données en question puisse être considérée comme une GBO. La finalité spécifique en vue de laquelle la GBO est créée doit cadrer dans une mission de police administrative et judiciaire.

11. Le responsable du traitement (l'entité de police) doit examiner si l'établissement d'une analyse d'impact relative à la protection des données (AIPD ou *DPIA* en anglais) est obligatoire ou indiqué (article 58 de la LPD). Dans certaines circonstances, le responsable du traitement devra consulter le COC préalablement au traitement (c'est-à-dire préalablement à l'enregistrement de données dans une GBO). C'est le cas :

- 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 de la LPD) ;
- lorsque l'AIPD indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ; ou si le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente un risque élevé pour les libertés et les droits des personnes concernées (art. 59 §1er, 1° et 2° de la LPD).

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

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

3.4. Les banques de données techniques

13. Il est important dans ce contexte de préciser qu'un régime spécifique s'applique à l'utilisation des caméras *ANPR*. Il s'agit de *« caméras intelligentes »*, à savoir des *« caméras qui comprennent également des logiciels qui, couplés ou non à des registres ou à des fichiers, peuvent traiter de manière autonome ou non les images recueillies »*[8]. Lorsque la surveillance par caméras *ANPR* est appliquée, les images sont enregistrées dans une *« banque de données technique »*[9], étant entendu que les données à caractère personnel et les informations sont alors également transmises à la banque de données technique nationale[10]. Les images peuvent être conservées pour une durée de maximum 12 mois (365 jours selon la modification légale) et il n'y a pas de délai de conservation minimum[11].

La banque de données technique contient, si elles apparaissent sur les images des caméras, les données suivantes[12] :
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[13], à l'arrière ;
4) une photo du véhicule ;
5) le cas échéant[14], 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 les images de la caméra *ANPR* incluent ces données.

3.5. L'interconnexion des banques de données

14. Comme prévu à l'article 44/4 §4 de la LFP, les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante[15] publiée au Moniteur belge, les modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique.

---

[7] Loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux.
[8] Art. 25/2 §1er, 3° *juncto* 44/2 §3, 3e alinéa de la LFP.
[9] Art. 44/2 §3, 1er alinéa de la LFP.
[10] Art. 44/11/3*sexies* de la LFP.
[11] Art. 44/11/3*decies* §2, 1er alinéa de la LFP.
[12] Art. 44/11/3*decies* §1er de la LFP.
[13] L'expression *« le cas échéant »* fait référence à la possibilité technique de la caméra de fournir ou non ces données.
[14] *Ibid*.
[15] Directive contraignante commune des ministres de la Justice et de l'Intérieur relative aux modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique.

Ces directives déterminent au moins, sur la base du caractère pertinent, adéquat et non excessif, les catégories de banques de données qui peuvent être connectées entre elles, les modalités relatives à l'interconnexion et les règles d'accès des membres des services de police relatives à l'existence d'une information pertinente au sein de ces banques de données interconnectées ou, le cas échéant, aux données elles-mêmes ainsi qu'aux traitements qui en résultent.

3.6. Les délais de conservation dans les banques de données de base et les banques de données particulières

15. Les délais de conservation qui s'appliquent aux enregistrements dans les banques de données de base sont mentionnés à l'article 44/11/2 §§ 2-6 de la LFP :

- 5 ans pour les données relatives aux missions de police administrative ;

- 15 ans pour les données relatives aux missions de police judiciaire, après quoi ces données sont consultables pendant un nouveau délai de :
  - 15 ans, et ce uniquement sur la base du numéro de notice du procès-verbal, du numéro de rapport d'information ou du numéro de dossier ;
  - 30 ans, et ce uniquement dans le cadre d'une enquête relative à des crimes ;

- 5 ans pour les données et informations relatives aux missions de police judiciaire relatives à des faits non concrets ;

- 5 ans pour les données et informations relatives aux infractions visées à l'arrêté royal du 1er décembre 1975 ;

- 30 ans pour les données et informations relatives à la gestion des enquêtes menées dans le cadre d'une information au sens de l'article 28*bis* du Code d'instruction criminelle ou d'une instruction judiciaire au sens de l'article 56 du Code d'instruction criminelle pour laquelle des devoirs d'enquête ont été prescrits à la police, et ce, à partir du moment où la fin de l'enquête a été communiquée par le magistrat compétent à la police.

16. Pour les banques de données particulières, la loi ne fixe pas de délais de conservation minimums ou maximums. Dans ces banques de données, les informations et données à caractère personnel peuvent exclusivement être traitées aussi longtemps qu'elles sont adéquates, pertinentes et non excessives. Dès que ces conditions ne sont plus remplies ou que le besoin particulier (la finalité) n'existe plus, ces données doivent être effacées, de même que la banque de données particulière elle-même.

4. RÉSULTATS DE L'ENQUÊTE

4.1. Qu'est-ce que FOCUS?

17. En soi, FOCUS semble pouvoir être décrite comme une 'plateforme' (ou des 'plateformes') facilitant une intégration et un support des applications existantes et des nouvelles applications à développer sur la base d'une structure intégrée, tant pour la police fédérale que pour la police locale. Les fonctionnalités de 'FOCUS@GPI' et 'FOCUS Interzonal' sont fournies par le biais d'une architecture applicative composée de différents modules. Les modules sont soit mis à la disposition de l'ensemble de la police intégrée dans le cadre de FOCUS@GPI, soit proposés moyennant une rétribution aux services de police et directions fédérales intéressés, qui s'y abonnent dans le cadre de FOCUS Interzonal. La ZPA dispose en outre d'une application 'FOCUS@ZPA' qui est exclusivement utilisée par cette zone de police, mais celle-ci n'est pas abordée dans le présent rapport de contrôle.

18. Selon les informations transmises au COC, les applications FOCUS@GPI et FOCUS Interzonal sont hébergées auprès de la DRI.

FOCUS@GPI et FOCUS Interzonal semblent par essence se composer de modules dans lesquels sont traitées des informations et des données à caractère personnel. En dernière analyse, il s'agit d'une part de modules identiques et d'autre part de modules qui sont créés par la ZPA à la demande et à l'intention d'une zone de police.

4.2. La création de FOCUS@GPI et FOCUS Interzonal

19. Le courrier du 17.04.2024 de la DRI et de la ZPA, qui a été joint aux réponses aux questions initiales posées par le COC, revient pour commencer sur la création des applications que sont actuellement FOCUS@GPI et FOCUS Interzonal. Il s'agit d'une solution qui a été mise en place à partir de FOCUS@ZPA pour répondre au besoin d'élargissement d'échelle.

En 2015, la ZPA a de sa propre initiative lancé FOCUS (devenue plus tard FOCUS@ZPA) en tant qu'outil permettant de mieux soutenir les équipes sur le terrain au sein de la zone de police.
En 2016, la plateforme a été élargie sur décision du ministre de l'Intérieur et déployée pour différentes zones de police et entités de la police fédérale, devenant ainsi l'application dite 'FOCUS@GPI' pour laquelle des conventions reprenant les différentes responsabilités ont été établies et signées en 2017 et 2022.

Selon les réponses fournies par écrit le 04.08.2024, FOCUS@GPI était cependant à ses débuts – en 2018 – une copie de la plateforme FOCUS@ZPA et se limitait à 10 modules.

Pour le déploiement de nouveaux modules dans FOCUS@GPI, il est toujours procédé à une évaluation budgétaire et à une recherche du plus grand dénominateur commun pour les modules qui sont ou seront proposés.

20. Selon ses explications, la ZPA attend pour faire passer FOCUS@ZPA à FOCUS@GPI que la DRI atteigne le niveau de gestion et de disponibilité correspondant à la continuité opérationnelle souhaitée par la ZPA. Pour l'instant, 2 plateformes coexistent donc, à savoir FOCUS@ZPA d'une part et FOCUS@GPI et FOCUS Interzonal d'autre part. Dans un courrier du 17.04.2025, la ZPA indique qu'une 'fusion' de ces deux plateformes n'est pas (encore) prévue. Pour autant que le COC ait compris correctement les explications fournies, il n'y aurait pas d'échange de données policières entre les deux 'plateformes' (abstraction faite des 'modules').

21. Dans le concept de FOCUS Interzonal, les zones de police peuvent, moyennant une rétribution, utiliser des modules additionnels et au besoin (faire) développer de nouveaux modules en collaboration avec la ZPA. En ce qui concerne FOCUS Interzonal, la ZPA a établi en juin 2020 un modèle de convention de collaboration interzonale qui a été revu en 2024. Cette convention doit être signée par toutes les zones de police participantes.

4.3. Modules FOCUS@GPI et FOCUS Interzonal

22. Dans son courrier susmentionné annonçant le contrôle, le COC souhaitait obtenir une réponse aux questions suivantes :

1) un aperçu de la structure de gestion de FOCUS et FOCUS Interzonal ;
2) les modalités de la gestion des accès, d'une manière générale ou par fonctionnalité ;
3) les modalités de la journalisation, d'une manière générale ou par fonctionnalité, et ce qu'il en est de l'interconnexion avec les banques de données de base existantes comme la BNG[16], ISLP[17], etc. ;
4) la manière dont les données sont actualisées en FOCUS et FOCUS Interzonal ;
5) les conditions à remplir pour un archivage (les mesures qui sont prises au niveau de la synchronisation avec les banques de données existantes pour s'assurer que les données soient supprimées à cet endroit également) et la durée de conservation des archives ;
6) les mesures qui sont prises pour garantir que les données restent dans l'environnement policier (autrement dit, ces applications peuvent-elles être utilisées sur des appareils personnels, au risque que des données fuitent vers des tiers ?).

4.3.1. Aperçu des modules FOCUS@GPI et FOCUS Interzonal

23. Le 18.04.2024, le COC a reçu de la DRI et de la ZPA un courrier contenant une réponse conjointe aux questions posées.

[16] 'BNG' est l'acronyme désignant la Banque de données nationale générale.
[17] ISLP signifie *Integrated System for Local Police.*

En ce qui concerne les modules, il ressort de ces réponses qu'il existe en FOCUS@GPI et FOCUS Interzonal des modules qui sont soit utilisés par l'ensemble de la GPI, soit achetés et utilisés par un certain nombre de zones de police et/ou de directions de la police fédérale. Il est également fait référence à un certain nombre de sites Sharepoint :

pour FOCUS@GPI : https://bpolb.sharepoint.com/sites/iNetwork-Focus ;

pour FOCUS Interzonal : https://bpolb.sharepoint.com/sites, actuellement https://bpolb.sharepoint.com/sites/CIS ;

FOCUSInterzonaalGrp/SitePages/fr/Home.aspx-Functioneledocumentatie: https://focus.pol.be/webhelp/Focus.

24. Voici une énumération des modules qui étaient cités dans la réponse de la DRI et de la ZPA ainsi que des modules trouvés sur les sites SharePoint renseignés par la DRI et la ZPA.

FOCUS@GPI

- Briefing.
- Ordre public – gestion des événements.
- Incidents et équipes.
- Aperçu des personnes sous conditions ('POV').
- Images et preuves.
- Messages.
- Contacts.
- Incidents.
- Notes.
- Recherche dans les sources externes, les banques de données de base et les banques de données FOCUS.
- ISLP.
- Rapport d'activités.
- Inbox et Delver.
- Mobilisation.
- Police maps.

FOCUS Interzonal

- Contrôle de domicile – WOCODO.
- Instruction judiciaire.
- Nuisances et surveillance.
- ANPR.
- Localisations de patrouilles – PATLOC.
- Cartes de données 5G.
- CERVUS.
- Cyber Sandbox Environment.
- Dossiers de délivrance FOCUS.
- Dossiers FOCUS (pas encore en usage).
- Mobile Office.
- Smartphones et abonnements.
- Track and Trace.
- UFED Unity Project.

4.4. Imprécisions restantes et préoccupations du COC

25. Après une analyse *prima facie* des documents et réponses reçus le 18.04.2024 concernant les modules FOCUS, il est cependant apparu que ces réponses contenaient des imprécisions et/ou se contredisaient sur certains points. Ce constat a soulevé pour le COC un certain nombre de questions additionnelles, de sorte que la DRI et la ZPA ont été priées le 25.07.2024 de transmettre un certain nombre de schémas permettant d'établir :

- quels sont les flux de données entre les composants/modules ;
- quelle est l'origine des données ;
- où ces données sont enregistrées, ne serait-ce que temporairement ;
- où elles finissent par se retrouver ;

- qui a accès aux données ;
- quand les données sont supprimées du système (archivées, ventilées, …).

Le COC a également demandé un *Entity Relationship Diagram* (*ERD*) afin de vérifier comment les données sont mises en relation les unes avec les autres et comment elles peuvent être rendues disponibles pour différents groupes cibles ou être cloisonnées.

Plusieurs autres questions ont encore été posées à titre subsidiaire au sujet d'un audit de FOCUS (voir le point 4), des profils de fonctions et de leur gestion, des fichiers de journalisation, de l'AIPD et de modules spécifiques.

26. Le 21.08.2024, le COC a reçu en réponse à ses questions additionnelles du 25.07.2024, un courrier de la DRI et de la ZPA invitant le COC à un entretien préparatoire. Cette réunion a eu lieu le 26.09.2024 dans les locaux de la ZPA. L'objectif de la DRI et de la ZPA était d'expliquer et d'affiner leurs ébauches de réponses, d'approfondir leur contexte et leur portée et de fournir éventuellement au COC des informations complémentaires, comme le choix de considérer des modules de FOCUS soit comme une banque de données de base, soit comme une banque de données particulière, le choix de délais de conservation différents en fonction des modules, etc. …

27. Pendant la réunion, il a également été question des aspects essentiels du concept 'FOCUS', de la journalisation, de la gestion des accès, du cloisonnement des données, de l'archivage et de la suppression. Ci-après, nous passons en revue les réponses verbales et écrites apportées par la DRI et la ZPA aux questions additionnelles.

28. Dans le sillage du courrier du 04.10.2024 de la DRI et de la ZPA, le COC a également reçu le 04.10.2024 un support contenant les réponses ainsi que les documents/données demandé(e)s. Le COC a ainsi reçu 35 fiches AIPD (fichier Excel) pour des modules de FOCUS@GPI, FOCUS Interzonal et FOCUS@ZPA, des ERD (fichier PNG), des fichiers de journalisation FOCUS (33 PDF), une matrice des droits FOCUS V4 (fichier Excel) et un fichier TXT 'Relations'.

En dépit de la quantité de réponses et d'informations, le COC n'est toujours pas en mesure d'établir avec certitude si des données (policières) sont enregistrées sur la *plateforme* FOCUS elle-même, ne serait-ce que temporairement, ni, dans l'affirmative, qui peut consulter ces données, les adapter, etc. …

4.4.1. Banque de données de base ou particulière ?

29. La DRI et la ZPA considèrent FOCUS@GPI comme une banque de données de base parce qu'elle a été créée sous la responsabilité des ministres compétents pour la police (comme prévu à l'article 44/4 §1er, 1er et 2e alinéas *juncto* l'article 44/11/2 de la LFP). FOCUS Interzonal est par contre considérée comme une banque de données particulière parce qu'elle est axée sur les besoins locaux et qu'elle n'a pas été créée sous la responsabilité du ministre (article 44/4 §1er, 3e alinéa de la LFP).

30. La qualification de banque de données de base ou banque de données particulière ne peut toutefois pas reposer uniquement sur la question de savoir qui a ou non 'créé' la banque de données, mais doit également ressortir des éléments concrets du traitement de données. À cet égard, le COC décèle deux anomalies dans le raisonnement de la DRI et de la ZPA.

31. Premièrement, les données policières (c'est-à-dire les informations et données à caractère personnel visées à l'article 44/1 §1er de la LFP) sont dans l'état actuel de la loi traitées dans une banque de données policière opérationnelle créée par la loi (article 44/2 de la LFP). **Or, comme nous le verrons plus loin, cet aspect n'est pas clair en ce qui concerne la plateforme FOCUS**. En revanche, il est clair que des traitements de données sont effectués dans les modules de FOCUS. **Un des modules énumérés au point 4.3.1 pour FOCUS Interzonal ('Instruction judiciaire') est par exemple un traitement qui, en vertu de la LFP, est effectué dans une banque de données de base et qui ne peut donc pas, légalement, être une banque de données particulière ou en faire partie.**

32. Deuxièmement, la DRI est chargée du développement et de la gestion (de la BNG et) des **banques de données de base** (art. 44/11 §1er et 44/11/2 §1er, 2e alinéa de la LFP). Techniquement, la DRI et la ZPA ont accès aux données techniques, et le cas échéant à des données policières, dans le *back-end* de FOCUS hébergé au centre de données de la DRI. Bien que la DRI semble techniquement avoir accès à FOCUS@GPI et FOCUS Interzonal, rien ne permet de déterminer si la DRI, contrairement à 'l'organisation de création' ('maakorganisatie', pour reprendre la formulation originale utilisée dans les conventions), en l'occurrence la ZPA, a techniquement connaissance aussi de la logique et de la structure des données techniques. Il ressort pourtant de l'article 44/11/2 §1er, 2e alinéa de la LFP que la DRI a évidemment (elle aussi) pleinement connaissance – ou devrait avoir connaissance – du système de traitement, en l'occurrence FOCUS, mais les conclusions de l'enquête ne permettent pas d'établir sans équivoque que c'est bien le cas.

33. Dans les circonstances données, la constatation qui précède semble impliquer que la DRI est par essence exclusivement chargée de la collecte (technique) des données, sans toutefois avoir techniquement une connaissance de contenu de ce système, de sorte que l'on peut se demander si la DRI est *de facto et de jure* en mesure de s'acquitter de ses obligations découlant de sa qualité de 'gestionnaire' de cette banque de données de base tel que visé à l'article 44/11/2 §1er, 2e alinéa de la LFP, et donc les respecte ou est en mesure de les respecter légalement. Cependant, la responsabilité en la matière incombe aux ministres de l'Intérieur et de la Justice (art. 44/4 §1er, 1er et 2e alinéas de la LFP).

La distinction entre une banque de données de base et une banque de données particulière ne peut pas être établie clairement à tous les égards. Néanmoins, le COC est d'avis qu'en cas de doute, il convient de préférer une qualification en tant que banque de données de base, et ce pour les raisons que nous exposons ci-après.

Le COC part dans ce contexte du principe du fonctionnement intégré de la police, dans le cadre duquel l'échange (l'exploitation) des informations et données à caractère personnel policières (données policières) est la norme. C'est là une caractéristique d'un service de police géré intelligemment, s'agissant également d'un concept de base propagé par la sphère politique et par la GPI pour la police belge. Cela signifie que les données policières sont disponibles (exploitables) lorsque c'est nécessaire et proportionnel pour l'exercice de missions de police administrative et judiciaire. La BNG et les banques de données de base forment dans ce contexte le système de base (étant entendu qu'un traitement de données policières dans une banque de données de base n'est pas nécessairement et/ou ne doit pas nécessairement être enregistré dans la BNG pour que les informations revêtent un intérêt opérationnel).

L'**obligation** opérationnelle d'exploiter les données policières (les transmettre, les échanger, les enrichir et en faire un usage ultérieur) n'est a priori pas évaluée en fonction de l'entité de police qui traite (initialement) les données policières (dans un module dit 'local'), et encore moins sur la base du nom qui est donné à un 'module', mais bien sur la base de la finalité policière opérationnelle qui est poursuivie (l'intérêt), d'une part, et du rôle et du profil de l'utilisateur (le destinataire) des données policières, d'autre part. Cette vision exprime l'intention qui était celle du législateur en 2014 et 2019. Telle était d'ailleurs (et, selon ce que le COC a pu comprendre, telle est toujours) la philosophie de base du projet *i-Police* – dont le contrat a entretemps été officiellement résilié –, qui ne permettait même plus la subdivision des banques de données en différents conteneurs.

Voilà pourquoi la LFP prévoit que la BNG et les banques de données de base soient développées et gérées par la DRI, de manière à mettre en place un support technique et une exploitation opérationnelle intégrés. L'exploitation de données policières passe par un support intégré grâce auquel les données policières indispensables sont disponibles dans ces banques de données, sans que l'existence de banques de données particulières ne soit requise. Le fait qu'il soit dans ce contexte question ou non d'un 'besoin local' n'est en principe pas pertinent.

Pour cette raison, une banque de données particulière ne peut être créée que 'dans des circonstances spécifiques'. Il s'agit de circonstances spécifiques en ce sens que le fait de ne pas exploiter les données policières de manière intégrée n'entrave pas l'exercice d'une mission opérationnelle[18].

La 'circonstance spécifique' ne saurait donc être basée (exclusivement) sur des motifs techniques, ni a fortiori sur des motifs organisationnels et/ou artificiels. Le fait que la BNG serait inadéquate ou ne répondrait pas suffisamment, d'un point de vue technique et pratique, aux besoins d'une police moderne, ne correspond pas non plus à la définition d'une 'circonstance spécifique' (il ne s'agit donc pas ici de l'impossibilité technique ou fonctionnelle d'alimenter la BNG telle que visée à l'article 44/11/3 §2, b) de la LFP). Par conséquent, le fait qu'un chef de corps ou un directeur de la police fédérale puisse lui-même 'demander' un module ou s'y 'abonner' ne saurait conduire à la conclusion que ces 'modules' doivent ou peuvent légalement être considérés comme une banque de données particulière. De même, un traitement répondant à un 'besoin local' ne satisfait pas automatiquement à la condition de la 'circonstance spécifique'. Un traitement local peut en effet bel et bien revêtir une importance (également) pour une autre entité de police. Cet élément ne suffit donc pas à considérer FOCUS Interzonal comme une banque de données particulière en raison de sa finalité technique et en partie liée à l'offre et à la demande[19].

[18] L'objectif poursuivi par la directive contraignante commune des ministres de la Justice et de l'Intérieur relative aux modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique, parue au Moniteur belge le 4 août 2021, n'y change rien.

[19] On peut donc se demander qui, en l'occurrence, détermine la finalité et les moyens, alors que selon l'article 26, 8° de la LPD et la jurisprudence de la Cour de Justice de l'Union européenne, la finalité et les moyens ne doivent pas nécessairement être déterminés par la même personne, et que le 'responsable du traitement' ne doit pas non plus déterminer lui-même la finalité et les moyens pour pouvoir être considéré comme responsable du traitement (voir par exemple CJUE 27 février 2025, C-638/23, avec renvois).

Par conséquent, la ZPA et la DRI doivent (pouvoir) justifier sur la base d'éléments juridiques spécifiques et objectifs que FOCUS Interzonal ne doive pas être considérée comme une banque de données de base. Dans l'état actuel des choses, le COC n'en est en tout cas nullement convaincu. Il revient à la ZPA et à la DRI de faire la clarté sur ce point et de présenter une argumentation autrement convaincante.

Le COC constate que la ZPA et la DRI n'ont pas soulevé dans le cadre de la phase du droit de réponse d'éléments démontrant que FOCUS Interzonal doive indiscutablement être considérée comme une banque de données particulière.

4.4.2. Responsable du traitement et sous-traitant

34. À la lumière de ces éléments, mais sous réserve des remarques formulées au point 33, nous ajoutons par souci d'exhaustivité que, dans la mesure où la DRI est chargée conformément à la LFP de la gestion de FOCUS@GPI, la DRI n'est pas considérée comme un *« sous-traitant »*[20] des données policières traitées dans cette banque de données de base. En revanche, la DRI doit être considérée comme un *« sous-traitant »* pour l'application FOCUS Interzonal dans la mesure où cette dernière est considérée comme une banque de données particulière[21].

4.4.3. Utilisation des applications existantes de la GPI

35. Le COC se demande pourquoi certains modules, par exemple le module 'Instruction judiciaire', sont développés au lieu d'utiliser les applications qui existent déjà au sein de l'environnement policier, comme GES pour les enquêtes pénales et BePad pour le module 'Nuisances et surveillance'. La DRI et la ZPA invoquent comme motif que les applications/banques de données susmentionnées ne répondent pas aux besoins de certaines zones de police, notamment celles de plus petite taille. Dans FOCUS@GPI et/ou FOCUS Interzonal, des modules sont développés pour surmonter cet obstacle. Pour d'autres applications, comme PACOS, la DRI et la ZPA font savoir qu'une interconnexion avec FOCUS est en cours d'établissement.

Bien que le COC ne doute pas des bonnes intentions de la DRI et de la ZPA, les traitements relatifs aux 'enquêtes' (pénales) n'en demeurent pas moins conformément à la LFP une composante d'une banque de données de base et non d'une banque de données particulière. Le fait que ces modules aient pour but de répondre à certains 'besoins', si légitimes soient-ils, n'y change donc rien (du point de vue légal).

4.4.4. Audit FOCUS

36. Bien que la loi ne l'exige pas, un audit est considéré vu la complexité technique de FOCUS comme une bonne pratique, notamment pour améliorer l'efficacité et mieux évaluer la gestion des risques. À la lumière de cette réflexion, le COC a posé dans son courrier introductif du 9 février 2024 la question suivante : *« Également dans le cadre de ce contrôle technique, le COC vous prie enfin de transmettre les documents suivants : a) l'**audit** le plus récent concernant FOCUS ; … »* (voir aussi le point 4). La DRI et la ZPA ont cependant répondu de manière évasive aux questions du COC portant sur le timing d'un audit de FOCUS, sur son caractère interne ou externe, sur sa portée et sur les parties impliquées. **Le COC déduit de cette réponse que FOCUS@GPI n'a pas encore fait l'objet d'un audit (technique) portant sur l'ensemble de la plateforme FOCUS**. Le COC recommande à la ZPA d'y procéder étant donné qu'il s'agit d'une application faisant l'objet d'un développement permanent.

Selon la ZPA, des tests de pénétration auraient en revanche été réalisés en 2018 dans le cadre de la mise en production de FOCUS au sein de la GPI. Un *Advanced Web Application Firewall* serait implémenté en 2025 pour FOCUS@GPI, après quoi des tests de pénétration seraient à nouveau réalisés.

4.4.5. Gestion des accès

37. À la question de savoir de quelle manière il est procédé au contrôle de l'exactitude des droits octroyés en FOCUS aux différents collaborateurs, la DRI et la ZPA ont répondu qu'en ce qui concerne FOCUS@GPI, ce sont les chefs de corps ou les directeurs de la police fédérale qui déterminent eux-mêmes une politique d'accès. D'une manière générale, il n'existe pas d'aperçu centralisé des procédures d'accès spécifiques appliquées au sein des entités de police. Les gestionnaires de FOCUS@GPI et de FOCUS Interzonal mettent en revanche à disposition des outils univoques et

[20] Selon l'article 26, 9° de la LPD, un *« sous-traitant »* est *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ou d'un autre sous-traitant »*. Attendu que la police fédérale se trouve sous l'autorité des ministres de la Justice et de l'Intérieur, chacun dans le cadre de leurs compétences, la DRI ne peut en l'occurrence pas être considérée comme une entité *externe* de la police fédérale qui traite les données à caractère personnel au nom des ministres susmentionnés.
[21] De l'avis du COC, la DRI ne peut pas être considérée comme un service *externe* à l'égard de la police fédérale, de sorte qu'elle ne peut pas être un sous-traitant de la police fédérale (pour laquelle les ministres compétents pour la police sont les responsables du traitement en ce qui concerne les banques de données de base).

maniables pour la gestion des accès afin de garantir le caractère contrôlable et la transparence (à noter que ces outils n'ont pas été examinés concrètement par le COC).

Pour la cartographie des droits au niveau des groupes d'utilisateurs, on utilise des 'règles de gestion' parce que c'est plus clair pour les gestionnaires. La modification des règles de gestion est journalisée dans un tableau d'historique du module 'Profils' de FOCUS.

Les systèmes suivants sont utilisés pour les accès :

- POLBACC[22] est utilisé pour l'accès de base à FOCUS@GPI ainsi que dans FOCUS Interzonal, de même que pour les accès détaillés aux différents modules de l'application FOCUS elle-même ;
- ISLP est utilisé pour la gestion des accès pour les recherches dans *Police-Search* et pour le module ISLP ;
- ACC[23] est utilisé pour la gestion de l'accès aux données authentiques comme le Registre national, la DIV[24], etc.

38. Dans un message diffusé au sein de la GPI à propos du déploiement de la version 3 de l'application mobile Focus, le COC constate qu'il est possible de s'identifier en utilisant des empreintes digitales, c'est-à-dire des données biométriques.

Dans la mesure où il serait accédé à l'application FOCUS sur un appareil (mobile) en utilisant les empreintes digitales, le COC attire l'attention sur ses avis antérieurs consacrés à l'utilisation de telles données biométriques, dont le traitement est très problématique dans l'état actuel de la loi[25].

Le consentement n'est en effet pas acceptable en tant que fondement juridique (art. 9.2 a) du RGPD) du fait du lien de subordination et de la relation d'autorité qui existent entre, en l'occurrence, les membres du service de police et la direction du service de police (considérants 42 et 43 du RGPD). Dans ce contexte, le consentement d'un membre du personnel de la police intégrée n'est, du point de vue juridique, pas 'libre' au sens du droit de la protection des données. Il en demeure ainsi même si une alternative est offerte en marge de l'utilisation des empreintes digitales, à moins que le législateur ne réglemente ce consentement et l'assortisse de garanties appropriées, ce qui n'est pas (encore) le cas.

Dans le cadre de la prélecture et du droit de réponse organisé, la ZPA et la DRI formulent la remarque suivante : '*Il n'est pas possible de s'identifier en utilisant une empreinte digitale. Les empreintes digitales ne peuvent être utilisées que pour enregistrer les informations d'identification sur l'appareil, les récupérer et les soumettre (souvent sous une forme non visuelle). L'identification sur les serveurs de FOCUS ne se fait donc pas au moyen d'empreintes digitales, mais bien au moyen d'informations d'identification complètes. Si l'utilisateur choisit d'utiliser une empreinte digitale sur son appareil, il s'agit de son propre choix.*'.

Le COC prend acte de cette réplique. Sans avoir effectué de vérifications additionnelles à ce sujet, il convient en tout état de cause de souligner que celui qui détermine la finalité et les moyens est et reste responsable des traitements.

39. Il ressort en outre de l'enquête menée dans le cadre du contrôle que le module 'Inbox-Delver' fonctionne avec un 'numéro 32'[26], ou que la police insiste pour que ce système soit utilisé, de sorte que les consultations ne peuvent plus être reliées à un utilisateur individuel. Comme nous le verrons ci-après, cette méthode a également des implications pour la journalisation de ces traitements.

À cet égard, la ZPA et la DRI déclarent ce qui suit en réponse au projet de rapport : '*FOCUS Inbox recourt à un utilisateur système pour récupérer les métadonnées des données ISLP et les préparer dans l'Inbox selon des critères déterminés par le gestionnaire fonctionnel. Quand un utilisateur va voir dans son Inbox ce qui a été préparé, il peut consulter le détail d'un élément ISLP. Cette deuxième étape du détail ISLP est effectuée à partir de son compte personnel, pour lequel tout est parfaitement journalisé.*'.

Le COC fait remarquer qu'il ne semble pourtant pas y avoir de journalisation des traitements (établissement de la requête) qui sont effectués par le membre compétent du service de police.

[22] PolBACC signifie *Police Based Access* et est une application web qui permet de gérer les droits d'un certain nombre d'applications de la police.
[23] ACC est un système qui permet de donner accès à des applications.
[24] DIV est l'acronyme désignant la Direction pour l'immatriculation des véhicules.
[25] Le COC a émis en la matière plusieurs avis, dont un seul a été rendu public, à savoir l'avis d'initiative du 13.02.2024 *« concernant le traitement de données à caractère personnel de membres du personnel d'une entité de police aux fins de gestion des accès à l'armement – Traitement d'empreintes digitales de membres du personnel pour la même finalité »* (DD220019).
[26] En marge des numéros (de matricule) 44 et 60, les numéros 32 sont les numéros de matricule qui sont utilisés pour l'accès par les processus système. En l'occurrence, ce numéro 32 procède à un *« bulk download »*.

4.4.6. Journalisation

40. Selon l'article 44/4 §2 de la LFP, les traitements opérationnels doivent être journalisés. D'une manière générale et sans vouloir être exhaustifs au sujet des journalisations, un certain nombre de questions demeurent sans réponse quant à cet aspect.

41. Pour commencer, selon les informations reçues de la DRI et de la ZPA, la journalisation se passe de la même manière pour FOCUS@GPI et pour FOCUS Interzonal. **Les modules sont journalisés dans des fichiers et des systèmes de journalisation différents**, à savoir soit au niveau interne de FOCUS, soit au moyen de fichiers de journalisation des sources de recherche fédérales (par ex. le Registre national). Des fichiers de journalisation sont ainsi conservés au niveau du Central Log, dans la 'ZPA Logdatabank', dans le tableau ZPA *Events*, *Central Mainframe*, Profile *history*, et dans une banque de données FOCUS dans laquelle seul l'historique des connexions et déconnexions est conservé.

42. Il ressort cependant de la réponse de la DRI et de la ZPA que **toutes les opérations ne sont pas journalisées** en FOCUS parce que cela engendre ou engendrerait une *surcharge* de données. **Le COC n'ayant pas obtenu de réponse affirmative univoque à la question de savoir si tout est journalisé conformément à l'article 44/4 §2 de la LFP, la question de savoir quelles opérations sont journalisées ou non, et si le choix qui est opéré à ce niveau est conforme au cadre légal, reste donc ouverte.**

Il ressort en outre d'une analyse plus approfondie que lorsque des informations sont transférées par exemple de la BNG au module Briefing, ce traitement n'est **pas** journalisé au niveau du destinataire. **Une diffusion ultérieure de ces données vers les autres modules comme 'Notes', 'Messages', etc. n'est pas journalisée non plus.**

Après prélecture, la ZPA et la DRI apportent à ce sujet la précision suivante : *« Rien de ce qui provient de la BNG n'est repris automatiquement dans le module 'Briefing'. C'est au rédacteur d'un briefing de décider s'il retranscrit dans un élément de briefing des informations provenant de la BNG. C'est pourquoi il n'existe pas de trace numérique de l'apparition de données de la BNG dans des éléments de briefing, de sorte que ce transfert ne peut pas non plus être journalisé en tant que tel. »*.

Il convient ici de faire remarquer que le COC ne prétend pas que des données soient reprises '*automatiquement*' de la BNG dans le module Briefing. Le COC fait seulement remarquer que lorsque des données sont diffusées et/ou reprises dans d'autres modules comme 'Notes', ces traitements ultérieurs ne sont pas journalisés.

Il apparaît notamment que, comme nous le disions plus haut, dès lors que le module 'Inbox-Delver' fonctionne uniquement avec un numéro 32 et ne peut donc plus être relié à un utilisateur individuel, **aucune journalisation** n'est prévue, **ce qui n'est pas conforme** à l'article 56 de la LPD lu conjointement avec l'article 44/4 §2 de la LFP.

Le COC a en outre reçu le 04.10.2024 de la ZPA 33 'fiches Centrallog' pour différents modules contenant des **données policières**, dont il ressort ce qui suit :

- Fiche 'Attribution tâche' – **Aucune journalisation prévue**, avec comme motif : *« Journalisation inutile étant donné l'absence de données policières sensibles. ».*
- Fiche 'AVR'[27] – Les actions 'Ajouter note', 'Modifier note' et 'Supprimer note' ne sont **pas journalisées**, avec comme motif : *« Pas de journalisation car il s'agit de données personnelles. ».*
- Fiche 'PROA'[28] – Les actions 'Updates', 'Export PDF', '*Posts* en vérification' et '*Posts* en examen' ne sont **pas journalisées**, avec comme motif : *« L'application est en mode de maintenance, le motif initial n'est pas connu. »*.
- Fiche 'Messaging' – **Aucune journalisation**, avec comme motif : *« Nous choisissons provisoirement de ne pas prévoir de journalisation parce que les conversations (entre deux parties ou en groupe) sont privées et que seuls les invités peuvent en prendre connaissance. »*.
- Fiche 'Notes' – **Aucune action n'est journalisée**, avec comme motif : *« Données propres. »*.
- Fiche 'PATLOC'[29] – Les domaines de gestion à l'exception du domaine de gestion/PATLOC ne sont **pas journalisés**, avec comme motif : *« Sujet abordé avec (…) et décision de ne pas journaliser parce que ce module ne contient pas de données opérationnelles. »*.
- Fiche 'Équipes' – **Aucun** des domaines de gestion n'est **journalisé**, avec comme motif : *« Sujet abordé avec (…) et conclu que la journalisation n'est pas utile. »*.

[27] AVR signifiant « rapport d'activités ».
[28] Cet acronyme n'a pas été explicité par la PZA.
[29] PATLOC est l'acronyme désignant la localisation des patrouilles.

- Fiche '*Policemaps'* – Nombre d'actions ne sont **pas journalisées**, avec comme motif : *« Sujet abordé avec (…) et conclu que la journalisation n'est pas utile. »*.

Il n'y a par ailleurs pas de fichiers de journalisation pour les contacts étant donné que ceux-ci sont accessibles à tous en FOCUS. **La gestion du dispatching des groupes lors d'incidents n'est pas journalisée parce que ce ne serait pas utile** (?).

Selon une enquête plus approfondie, les fichiers de journalisation pour le module 'POV' (Personnes sous conditions) fournissent uniquement une clé sans nom, prénom ni autres informations identifiables, de sorte que cette journalisation ne peut pas être suivie de bout en bout et n'est donc pas exploitable pour un audit.

4.4.7. AIPD

43. Les AIPD globales pour FOCUS@ZPA et FOCUS@GPI sont selon la DRI et la ZPA en cours d'établissement et/ou de révision, leur finalisation étant prévue pour début 2025 pour FOCUS@ZPA et mi-2025 pour FOCUS@GPI. La DRI et la ZPA sont priées de transmettre au COC l'AIPD de FOCUS@GPI et FOCUS Interzonal.

44. Pour ce qui est des différents modules de FOCUS, 35 AIPD ont été transmises, pour lesquelles le COC constate à l'issue d'une analyse *prima facie* que les mêmes remarques/questions peuvent être formulées pour quasiment toutes les AIPD, questions qui confirment d'ailleurs les préoccupations du COC, à savoir :

- le COC constate que dans 17 des 35 AIPD transmises, la rubrique *« Fondement juridique »* porte la mention « à compléter par le *DPO* » ;
- pour la rubrique *« Le traitement de données engendre un enregistrement persistant de données à caractère personnel dans une banque de données FOCUS afin qu'elles soient retrouvées directement (art. 44/1 de la LFP) »*, le COC constate que la réponse est « oui » dans 31 des 35 AIPD, **alors qu'il est affirmé partout ailleurs qu'il n'est procédé à aucun enregistrement de données** ;
- pour les rubriques *« Supports d'informations entrants/sortants dans la mesure où il s'agit de données à caractère personnel »* et *« Transmission de données à des parties externes »*, le COC constate qu'il est régulièrement fait mention de la création et de la transmission d'un rapport/d'une impression de fichiers PDF et que ces documents peuvent également être communiqués à des parties externes, **alors qu'il est affirmé partout ailleurs qu'il n'est procédé à aucun enregistrement de données**.

Le COC prend acte de la précision apportée par la ZPA et la DRI dans le cadre de la procédure de prélecture, à savoir que *« les 35 fiches transmises par la ZPA n'étaient en soi pas des AIPD. Ces fiches sont des documents que le service TIC de la ZPA a transmis à la DRI en vue de l'établissement de l'AIPD (les volets spécifiques par module) ».*

4.4.8. Risque de doubles traitements

45. Le COC constate qu'il existe de nombreuses possibilités qu'il soit procédé à des saisies redondantes des mêmes informations et données à caractère personnel (en double, voire en davantage d'exemplaires) dans des modules différents et auprès de différentes zones de police, comme les mêmes informations et données à caractère personnel qui sont saisies à la fois dans le module 'Briefing', dans le module 'Instruction judiciaire' et en GES. Ces doublons empêchent une gestion correcte de l'information. De plus, les AIPD transmises ne permettent pas d'exclure l'enregistrement dans certains modules de données à caractère personnel qui, lorsqu'elles ne sont pas actualisées, peuvent potentiellement faire l'objet d'un usage impropre.

Inutile de dire que c'est précisément l'actualisation des informations et données à caractère personnel policières qui constitue un énorme défi et qui préoccupe – ou devrait préoccuper – la GPI depuis des années. Rien qu'au niveau des traitements dans la BNG, le COC en fait l'expérience chaque jour.

4.4.9. Délais de conservation et exactitude des données à caractère personnel

46. Les délais de conservation divergent fortement d'un module à l'autre, ce qui n'est évidemment pas exclu par la loi étant donné les différentes finalités et les différents types de données policières qui sont collectées. **Toutefois, le COC constate ici aussi que pour certains modules, il n'est pas mentionné de délais de conservation et/ou les données peuvent être conservées pour une durée illimitée**, par exemple dans les modules 'Notes' et 'Messages'. De même, la possibilité de copier ces éléments à plusieurs reprises induit un risque que le délai de conservation soit « réinitialisé », de sorte qu'il peut arriver que les délais de conservation soient prolongés abusivement, parfois même involontairement.
C'est notamment le cas pour l'application 'Rapport d'activités', pour laquelle il n'a pas encore été fixé de délai de conservation, et pour les modules 'Messages' et 'Briefing', dans lesquels les données sont conservées pour une durée illimitée.

Ce constat est non seulement contraire aux dispositions légales applicables relatives aux délais de conservation maximums, mais il enfreint également les principes (légaux, eux aussi) du caractère pertinent, adéquat et non excessif des données.

47. Pour le module 'Messages', il n'existe aucune garantie que les données soient actuelles, exactes et complètes.

Selon la DRI et la ZPA, il s'agit par définition d'un instantané. Les données ne sont pas contrôlées ni validées. Le module 'Messages' n'a pas été conçu comme une banque de données au sens de la LFP, mais il n'est pas exclu pour autant que des messages contenant des données policières opérationnelles puissent être partagés avec plusieurs collaborateurs de police et qu'il soit bel et bien question de traitements de données opérationnels, et donc policiers. **Les modules de FOCUS font en effet partie de l'environnement policier opérationnel.**

4.4.10. Archivage

48. En ce qui concerne l'archivage, le COC constate que plusieurs délais sont utilisés, ce qui n'est encore une fois pas exclu par la loi. Toutefois, comme nous le verrons ci-après, **il existe aussi des modules qui ne prévoient pas l'archivage des données**.

49. Bien que la DRI et la ZPA indiquent qu'il n'est pas procédé à l'enregistrement de données sur la plateforme FOCUS en dehors des traitements effectués dans les modules – du moins selon ce que le COC a pu comprendre –, le COC constate le contraire dans les AIPD des modules. On peut par exemple y lire que l'application 'Images' met de l'espace de stockage à la disposition des autres applications de FOCUS pour l'enregistrement et la consultation de fichiers médias. Ces images peuvent être transférées vers notamment l'application 'Messages', pour laquelle aucun archivage n'est prévu, ou être compilées dans un fichier PDF. **Lors de la réunion, la DRI et la ZPA ont déclaré utiliser parfois le terme 'archivage' pour désigner le 'cloisonnement', ajoutant dans la foulée qu'il n'est pas prévu d'archivage proprement dit.**

50. Lorsque des traitements de données opérationnels sont effectués sur une plateforme ou dans des modules et, *in fine*, dans une banque de données, des dispositions légales s'appliquent selon la nature de la banque de données pour les délais de conservation maximums et/ou l'archivage, exception faite des banques de données particulières. Lors de la réunion du 26.09.2024, la DRI et la ZPA ont fait savoir qu'il n'avait encore été procédé à aucune suppression de données étant donné que celles-ci seraient encore pertinentes. En matière de pertinence, une simple 'supposition' comme celle-là ne suffit cependant pas. **Il convient de procéder pour toutes ces données à une évaluation de leur caractère pertinent, adéquat et non excessif.**

4.4.11. Sécurité de l'information

51. Pour ce qui est de la sécurité de l'information, le COC constate qu'il existe plusieurs possibilités de permettre l'accès aux données des modules de FOCUS. Concrètement, il s'agit ici de modules dans lesquels des données peuvent être enregistrées pour et par l'utilisateur (par exemple le module 'Notes') ou de possibilités d'envoyer des données par e-mail à des tiers, par exemple au parquet.

52. Il est possible de créer en FOCUS un nombre illimité de modules en fonction des besoins des utilisateurs. Comme FOCUS peut dès lors consolider une grande quantité de données dans des modules, cela engendre de nombreux effets indésirables du point de vue de la sécurité de l'information :

- la divulgation (indésirable) de données. Il n'est pas impensable que des données qui peuvent être envoyées par e-mail à des destinataires légitimes puissent être également – intentionnellement ou non – envoyées à d'autres utilisateurs. Il existe donc un risque élevé d'atteinte à la protection des données. **Or, le COC n'a pas relevé de mesures appropriées pour atténuer ou éliminer ce risque** ;
- tout comme dans les autres applications policières, les données qui quittent FOCUS ne sont plus contrôlables à l'égard des délais de conservation fixés par la loi ;
- les données qui quittent FOCUS ne sont plus actualisées lorsque c'est nécessaire.

Vu l'obligation de prendre les mesures techniques et/ou organisationnelles appropriées pour protéger les données contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, le COC entrevoit ici un problème à l'égard de la sécurité de l'information.

53. Le COC apprend qu'un délai d'inactivité de pas moins de 14 heures a été demandé/imposé dans l'intérêt de la convivialité de FOCUS@GPI et FOCUS Interzonal. Ce choix implique un risque énorme d'usage impropre (en cas de perte d'un appareil, de collègues qui abusent d'une session ouverte par un autre collègue pour effectuer des recherches illicites, etc. …).

54. De même, la problématique évoquée au point 35 – à savoir le fait que de nouvelles applications sont développées pour des aspects pour lesquels il existe déjà des applications (par ex. la banque de données GES pour les enquêtes pénales) – implique du point de vue de la sécurité de l'information le risque que s'il n'est pas possible de garantir que l'architecture renvoie toujours aux données initiales, des données non cohérentes ou non actuelles puissent être enregistrées et utilisées de manière éparse. Une adaptation de l'architecture s'assortissant de règles d'utilisation claires et un *life cycle management*[30] univoque indiquant quelles applications sont en cours de développement et lesquelles sont en cours d'extinction pourraient à cet égard apporter des solutions.

5. CONCLUSION

55. Le COC comprend parfaitement l'intérêt opérationnel de l'application FOCUS et la plus-value qu'elle représente pour l'efficacité de la gestion de l'information et du fonctionnement opérationnel de la police intégrée.

56. Le concept de FOCUS cadre dans les objectifs de la directive contraignante commune des ministres de la Justice et de l'Intérieur relative à l'interconnexion des banques de données (*M.B.* 04.08.2021). Il convient néanmoins de respecter les exigences de sécurité requises pour que les données soient traitées correctement et pour faire en sorte que les données rendues disponibles au sein de la GPI soient bien les données correctes et actualisées[31].

57. Dès l'annonce du contrôle technique, la DRI et la ZPA se sont mises à transmettre une importante quantité de documents et de réponses. Le COC conclut toutefois de l'évaluation de ces documents et réponses que la structure et la conception des plateformes et des modules ainsi que la scission qui est faite entre la plateforme et les modules sont à ce point complexes que même l'organisation de création (la ZPA) et a fortiori l'organisation de gestion (la DRI) ne semblent pas en avoir une vue d'ensemble tout à fait claire.

58. Le COC déduit des éléments de ce contrôle technique restreint que vu le rôle de la ZPA au sein du paysage actuel de la police en tant qu'organisation de création des modules de FOCUS@GPI et FOCUS Interzonal, il semble y avoir eu un glissement du niveau fédéral vers le niveau local et un abandon au moins partiel du modèle créé par la LPI de 1998, dans le cadre duquel la police fédérale est chargée de missions d'appui (gratuites) au profit de la police locale et des autorités (cf. notamment l'article 3, 3e alinéa *juncto* les articles 100*bis* – 115 et suivants de la LPI et l'A.R. du 14.11.2006). Le COC constate que cette transition qui s'opère depuis plusieurs années acquerra une base légale plus claire grâce au projet de loi qui a été adopté au sujet des zones de police bruxelloises[32], qui prévoit un régime légal pour les projets dits de cocréation entre la police locale et la police fédérale (nouveau projet d'article 115*bis*/1 de la LPI).

Il semble que FOCUS Interzonal soit devenu un modèle dans lequel la police fédérale se voit attribuer en sa qualité d'organisation de gestion un rôle passif, dès lors que les données ne semblent être pour elle qu'un ensemble de données sans structure.

Dans le cadre du futur article 115*bis*/1 de la LPI, il semble indiqué de procéder à cet égard à un recalibrage.

59. Le COC déduit de la réponse conjointe du 18.04.2025 de la ZPA et de la DRI qu'une migration complète de FOCUS@ZPA vers l'infrastructure de la DRI n'aura lieu que *« lorsque le niveau de gestion et de disponibilité correspondra à la continuité opérationnelle souhaitée par la ZP Antwerpen »*, ce qui suggère à tout le moins un manque ou une perte de confiance à l'égard des systèmes et de la capacité de la DRI.

60. Tout comme pour d'autres applications policières, le COC relève au niveau du concept de FOCUS, dans la manière dont les accès sont octroyés – à savoir par le biais de plusieurs systèmes et avec une interprétation large des responsables du traitement –, un problème qui nuit à la gestion de l'information policière et à la transparence. Le fait que le choix s'est porté sur l'utilisation de profils génériques soutient cette hypothèse.

---

[30] Le *life cycle management* est le processus informatique qui gère l'ensemble du cycle de vie des systèmes informatiques (matériel et logiciels), depuis leur planification, achat/développement/déploiement jusqu'à leur mise hors service en passant par la maintenance et l'optimalisation. Par extension, on prendra également dans le sillage des actions relevant de ce processus des décisions visant à intégrer les nouveaux systèmes dans l'architecture et à éviter les doubles fonctions.

[31] Directive commune des Ministres de la Justice et de l'Intérieur relative aux mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2 de la loi sur la fonction de police.

[32] Projet de loi modifiant la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux et diverses autres dispositions relatives aux services de police, DOC 56 1342/11 du 8 mai 2026, www.lachambre.be.
Voir aussi l'avis DA250008 du 28.08.2025 de l'Organe de contrôle relatif au projet de loi modifiant la loi du 7 décembre 1998 organisant un service de police intégré structuré à deux niveaux et la loi du 26 avril 2002 relative aux éléments essentiels du statut des membres du personnel des services de police et portant diverses autres dispositions relatives aux services de police, www.organedecontrole.be/publications/avis-r%C3%A9glementation.

61. Pour ce qui est des journalisations, l'enquête menée dans le cadre du contrôle a révélé que les traitements ne sont pas tous journalisés alors que toutes les informations et données à caractère personnel enregistrées en FOCUS doivent être considérées comme des données policières. Par ailleurs, les données de journalisation ne sont pas toutes structurées de manière à satisfaire aux dispositions de l'article 44/4 §2, 2e et 3e alinéas de la LFP.

62. Le COC constate également que la terminologie utilisée dans l'explication au sujet de l'archivage et du cloisonnement n'est pas correcte, ce qui prête à confusion pour l'évaluation des garanties légales prévues au Titre 2 de la LPD et dans la LFP. En tout état de cause, le terme 'archivage' tel que visé dans la LFP et le terme 'cloisonnement' ne sont pas interchangeables d'un point de vue juridique. L'archivage est en effet réglementé explicitement et en vue de finalités particulières.

63. Le COC constate que la DRI et la ZPA ont choisi de catégoriser les plateformes respectivement en tant que banques de données de base et en tant que banque de données particulière. En dépit de cette subdivision, le COC ne peut que constater que la plupart des traitements ont leur place dans une banque de données de base. Dès lors que la DRI et la ZPA choisissent de catégoriser Focus Interzonal en tant que banque de données particulière, il est à l'évidence dérogé également aux délais légaux de conservation, d'archivage et d'effacement tels qu'ils sont fixés dans la LFP pour les banques de données de base. Cette manière de procéder soulève des questions quant à la conformité à la loi de ces traitements.

64. Il est néanmoins apparu dans le cadre de ce contrôle technique que la DRI et la ZPA sont absolument de bonne foi et sont déterminées à organiser tous les traitements en FOCUS conformément à la législation en vigueur. Cependant, il est clair qu'il reste du travail à accomplir. L'utilisation des différents modules de FOCUS doit être (plus) clairement décrite et les collaborateurs doivent être sensibilisés au cadre juridique des recherches, du motif de consultation, etc. … Une gestion adéquate, par le truchement du *DPO*, de la poursuite de l'implémentation de la sécurisation des informations en général au sein de toutes les entités de police est à cet égard primordiale.

65. L'Organe de contrôle est donc d'avis que, comme en attestent les constatations établies dans le rapport de contrôle, il y a encore matière à amélioration dans plusieurs domaines, dont certains relèvent du périmètre du présent contrôle.

66. L'accord de coalition fédérale projette d'élaborer une 'loi sur les données policières' pour remplacer l'article 44 de la LFP. Là encore, il apparaît que la classification artificielle en plusieurs types de banques de données ayant des responsables du traitement différents, désignés formellement d'un point de vue juridique, n'est plus judicieuse dès lors qu'elle engendre d'interminables discussions et des problèmes d'interprétation qui ne contribuent en aucune manière à la réalisation de l'objectif principal du droit de la protection des données, à savoir la garantie d'un niveau élevé de protection des droits et libertés fondamentaux, et en particulier de la vie privée, à travers le traitement des données à caractère personnel. Néanmoins, la loi est aujourd'hui ce qu'elle est (*dura lex sed lex*), et elle doit être respectée.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

prie le ministre de la Sécurité et de l'Intérieur, le ministre de la Justice, le commissaire général de la police fédérale, le chef de corps de la zone de police Antwerpen et le président de la Commission Permanente de la Police Locale de prendre connaissance du présent rapport, d'en tirer les conclusions qui s'imposent et de prendre les initiatives adéquates.

Ainsi décidé par l'Organe de contrôle de l'information policière le 16 juin 2026.

Pour l'Organe de contrôle de l'information policière,

Frank SCHUERMANS
Président a.i. (Sé)



Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière