SERVICE PUBLIC FEDERAL JUSTICE

[C − 2023/48297]

23 NOVEMBRE 2023. — Arrêté royal relatif à l'accès direct des services de renseignement et de sécurité aux données à caractère personnel et informations de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police

RAPPORT AU ROI

Sire,

Introduction

Le présent projet d'arrêté concerne les conditions afférentes à l'accès direct des services de renseignement et de sécurité à la Banque de données Nationale Générale (B.N.G.) visée à l'article 44/7 de la loi sur la fonction de police.

Les dispositions légales qui permettent l'accès direct des services de renseignement et de sécurité à la B.N.G. sont les articles 14 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, 44/11/8*bis* et 44/11/12 de la loi du 5 août 1992 sur la fonction de police.

Cet accès direct n'empêche en rien les services de renseignement et de sécurité de s'adresser aux services de police afin d'étayer les données qui sont disponibles dans la B.N.G.

Le présent projet d'arrêté est commun aux deux services de renseignement et de sécurité. Dans la foulée, un protocole spécifique sera conclu entre chaque service de renseignement et de sécurité et la Direction de l'information policière et des moyens ICT de la police fédérale pour déterminer, dans le détail, les modalités d'accès de chaque service.

Par ailleurs, l'article 44/11/8*bis* de la loi sur la fonction de police prévoit également le principe de réciprocité, c'est-à-dire la communication des données et informations gérées par les services de renseignement et de sécurité aux services de police.

Etant donné le degré de protection de certaines données et informations gérées par les services de renseignement et de sécurité et le fait que tous les membres de la police ne sont pas habilités à traiter des données et informations classifiées, un accès direct similaire de la police vers les services de renseignement et de sécurité est difficilement envisageable actuellement.

Cela n'empêche bien entendu pas que, les services de renseignement et de sécurité s'inscrivent totalement dans une logique d'échange le plus efficace possible avec la Police, dans le respect des contraintes mutuelles et des principes de bonne coopération tels qu'inscrits déjà dans les articles 19 et 20 de la Loi organique des services de renseignement et de sécurité (30/06/1998).

Ceci concerne en premier lieu les échanges de fond où une des finalités des services de renseignement et de sécurité doit être de valoriser, exploiter et enrichir les données policières en vue de réaliser sa mission de détection et de réduction des menaces. En mettant en perspective les données policières à l'aide des données classifiées issues de la collecte nationale ou internationale du renseignement, les services de renseignement et de sécurité seront en mesure de retourner vers les services de Police avec des hypothèses solides qui peuvent être des leviers à des actions de police administrative et judiciaire.

Cela signifie à la fois que des données sont communiquées d'initiative par les services de renseignement et de sécurité à la Police et qu'ils répondent aux demandes d'informations formulées par la Police

Le contenu que doit avoir le projet d'arrêté est par ailleurs précisé au paragraphe 2 de l'article 44/11/12 de la loi sur la fonction de police, à savoir :

a) le besoin d'en connaître (voir article 2) ;

b) les catégories de membres du personnel qui, sur la base de l'exécution de leurs missions, disposent d'un accès direct à la B.N.G. (voir article 2) ;

c) les traitements automatisés qui sont effectués sur la base des données et informations de la B.N.G. (voir article 7) ;

d) l'obligation du respect du secret professionnel par toutes les personnes qui prennent directement ou indirectement connaissance des données et informations de la B.N.G. (voir article 3) ;

e) les mesures de sécurité dont notamment :

1° la sécurité des infrastructures et des réseaux (voir article 4) ;

2° l'obligation d'effectuer une journalisation de toutes les transactions et de conserver ces données de journalisation pendant minimum dix ans (voir article 6) ;

f) l'obligation de suivre une formation préalablement à l'obtention de l'accès direct (voir article 2) ;

g) l'évaluation de la fiabilité, du milieu et des antécédents des membres du personnel visés au point *b)* (voir article 2).

FEDERALE OVERHEIDSDIENST JUSTITIE

[C − 2023/48297]

23 NOVEMBER 2023. — Koninklijk besluit betreffende de rechtstreekse toegang van de inlichtingen- en veiligheidsdiensten tot de persoonsgegevens en de informatie van de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt

VERSLAG AAN DE KONING

Sire,

Inleiding

Dit ontwerp van besluit betreft de voorwaarden omtrent de rechtstreekse toegang van de inlichtingen- en veiligheidsdiensten tot de Algemene Nationale Gegevensbank (A.N.G.) bedoeld in artikel 44/7 van de wet op het politieambt.

De wetsbepalingen die de rechtstreekse toegang van de inlichtingen- en veiligheidsdiensten tot de A.N.G. toelaten, zijn de artikelen 14 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, 44/11/8*bis* en 44/11/12 van de wet van 5 augustus 1992 op het politieambt.

Deze rechtstreekse toegang belet niet dat de inlichtingen- en veiligheidsdiensten zich tot de politiediensten kunnen wenden om de in A.N.G. beschikbare gegevens te staven.

Dit ontwerp van besluit geldt voor beide inlichtingen- en veiligheidsdiensten. Aansluitend zal een specifiek protocol gesloten worden tussen elke inlichtingen- en veiligheidsdienst en de Directie van de politionele informatie en de ICT-middelen van de federale politie om de toegangsmodaliteiten van elke dienst in detail vast te leggen.

Bovendien voorziet artikel 44/11/8*bis* van de wet op het politieambt ook in het wederkerigheidsbeginsel, d.w.z. de mededeling van door de inlichtingen- en veiligheidsdiensten beheerde gegevens en informatie aan de politiediensten.

Gelet op de graad van bescherming van bepaalde gegevens en informatie die door de inlichtingen- en veiligheidsdiensten worden beheerd en het feit dat niet alle leden van de politie gemachtigd zijn om met geclassificeerde gegevens en informatie om te gaan, is een gelijkaardige rechtstreekse toegang van de politie tot de inlichtingen- en veiligheidsdiensten momenteel moeilijk haalbaar.

Dit neemt niet weg dat de inlichtingen- en veiligheidsdiensten volledig de lijn van de meest efficiënt mogelijke gegevensuitwisseling met de Politie volgen, met naleving van de wederzijdse verplichtingen en de principes van goede samenwerking zoals deze al zijn opgenomen in de artikelen 19 en 20 van de organieke wet van de inlichtingen- en veiligheidsdiensten (30/06/1998).

Dit betreft in de eerste plaats grondige uitwisselingen waarbij het één van de finaliteiten van de inlichtingen- en veiligheidsdiensten moet zijn om de politiegegevens te valoriseren, benutten en verrijken met het oog op het opsporen en verminderen van de dreigingen. Door de politiegegevens in perspectief te plaatsen met behulp van de geclassificeerde gegevens afkomstig van de nationale of internationale inlichtingenvergaring, zullen de inlichtingen- en veiligheidsdiensten in staat zijn om terug te keren naar de Politiediensten met solide hypothesen die hefbomen kunnen zijn voor bestuurlijke en gerechtelijke handelingen.

Dit betekent dat de inlichtingen- en veiligheidsdiensten op eigen initiatief gegevens meedelen aan de Politie en dat ze tegelijkertijd een antwoord geven op de vragen om informatie van de Politie op de meest gepaste manier

De inhoud die het ontwerp van besluit moet bevatten, wordt trouwens nader bepaald in paragraaf 2 van artikel 44/11/12 van de wet op het politieambt, met name:

a) de behoefte tot kennisname (zie artikel 2);

b) de categorieën van personeelsleden die op basis van de uitoefening van hun opdrachten over een rechtstreekse toegang tot de A.N.G. beschikken (zie artikel 2);

c) de geautomatiseerde verwerkingen die uitgevoerd worden op basis van de gegevens en informatie van de A.N.G. (zie artikel 7);

d) de verplichting tot naleving van het beroepsgeheim door alle personen die rechtstreeks of onrechtstreeks kennisnemen van de gegevens en informatie van de A.N.G. (zie artikel 3);

e) de veiligheidsmaatregelen, waaronder:

1° de beveiliging van de gebouwen en netwerken (zie artikel 4);

2° de verplichting om alle transacties op te lijsten en deze logbestanden gedurende minimaal tien jaar te bewaren (zie artikel 6);

f) de verplichting om voorafgaand aan het verkrijgen van de rechtstreekse toegang een opleiding te volgen (zie artikel 2);

g) de evaluatie van de betrouwbaarheid, de omgeving en de antecedenten van de personeelsleden bedoeld in punt b) (zie artikel 2).

Force est de constater que les droits en matière de traitements à effectuer dans la B.N.G. conférés aux agents des services de renseignement et de sécurité, qui ont le besoin d'en connaître, sont d'emblée limités dans la loi (articles 44/11/8*bis* et 44/11/12), puisqu'il s'agit uniquement de leur conférer un droit d'accès direct à la B.N.G. Il ne saurait être question dans le présent projet de leur attribuer des droits directs de modification, de création ou d'effacement des données de la B.N.G..

Dans le même ordre d'idée, comme le rappelle l'Organe de contrôle dans son avis sur le projet de cet arrêté (avis DA230004 du 25.04.2023) les outils d'exploitation doivent se limiter à pouvoir consulter les données de la B.N.G.

L'Organe de contrôle se demande cependant quels outils d'exploitation peuvent être utilisés ou pas pour consulter la B.N.G. (point 16 de son avis).

Dans les points 5 et 6 de son avis 2/CPR/2023 du 8 juin 2023, le Comité permanent R se pose des questions similaires : « *Peut-on uniquement chercher des noms individuels ?*(1) *Des listes de noms peuvent-elles être corrélées (ponctuellement/sur une période déterminée/ permanente) ?*(2) *Des recherches peuvent-elles être effectuées à partir de critères d'évaluation prédéterminés et quels peuvent être ces critères ?*(3) ».

Il n'est bien entendu pas dans l'optique du gouvernement de reprendre le mode d'emploi d'une banque de données et de déterminer dans le corps d'un arrêté royal délibéré en Conseil des Ministres les types de possibilités pour consulter une banque de données.

De manière classique, cette consultation peut se dérouler

- en introduisant une à une des données comme par exemple un nom, prénom, et date de naissance, un numéro RRN, numéro de compte (...)

ou- à l'aide de liste de noms/prénom, numéros de compte, ... pour gagner du temps et éviter les erreurs manuelles,

- ou encore à l'aide de l'option fuzzy search.

Cependant, dès lors qu'il s'agit de consulter la B.N.G. avec des critères préétablis, le gouvernement estime que des règles de précaution supplémentaires s'appliquent pour entourer ces accès et éviter tout arbitraire.

Ces règles, précisées à l'article 2 de l'arrêté royal sont les suivantes :

1) l'accès à la B.N.G. sur la base de critères préétablis fait l'objet d'une décision écrite motivée du dirigeant du service de renseignement et de sécurité concerné ou de son délégué.

2) en cas d'urgence, le dirigeant du service ou son délégué peut décider verbalement de procéder à l'accès sur la base de critères préétablis. Cette décision verbale est confirmée par une décision écrite, le premier jour ouvrable qui suit la date de la décision verbale.

3) la décision du dirigeant du service ou de son délégué et sa motivation sont transmises au Comité permanent R dans les meilleurs délais.

4) la décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, une liste des accès ponctuels est communiquée une fois par mois au Comité permanent R.

5) le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans des conditions qui ne respectent pas les dispositions légales.

Ces critères préétablis permettent d'effectuer des recherches sur une période de temps et/ou dans des lieux (enregistrés en B.N.G.) alors que l'identité des personnes ou l'identification des données à caractère personnel recherchées (véhicule par exemple) ne sont pas stipulées de manière précise dans la recherche (la question).

Ces recherches à l'aide de critères préétablis doivent par exemple permettre de fournir toutes les personnes enregistrées pour des faits de terrorisme en B.N.G. du 1/1/ 2020 au 1/1/2023 sur l'arrondissement judiciaire d'Anvers ou encore de donner la liste de tous les véhicules enregistrés en BNG qui sont liés à des faits de terrorisme du 1/1/2020 au 1/1/2023.

Par ailleurs, le gouvernement précise, si c'était encore nécessaire, que l'accès direct n'a pas pour objectif ou comme corollaire de permettre aux services de renseignement et de sécurité de créer de nouvelles informations dans la B.N.G.

Dans le cadre des échanges réciproques, les éventuels enrichissements d'une donnée issue de la B.N.G. par le traitement ultérieur des services de renseignement et de sécurité seront le cas échéant apportés dans la B.N.G. par les services de police eux-mêmes.

Enfin, l'objet de ce projet d'arrêté royal est de fournir un cadre général sur l'accès direct des services de renseignement et de sécurité et non d'en préciser les procédures fonctionnelles et techniques qui seront, elles, détaillées dans des protocoles fonctionnels et techniques.

Er dient te worden vastgesteld dat de rechten aangaande de in de A.N.G. uit te voeren verwerkingen die toevertrouwd zijn aan de agenten van de inlichtingen- en veiligheidsdiensten die de behoefte tot kennisname hebben, in de wet onmiddellijk beperkt worden (artikelen 44/11/8*bis* en 44/11/12) aangezien hen enkel een recht op rechtstreekse toegang tot de A.N.G. toegekend wordt. Er is in dit ontwerp geen sprake van om hen rechtstreekse rechten toe te kennen inzake wijziging, creatie of uitwissing van gegevens van de A.N.G.

In dezelfde geest, zoals het Controleorgaan aangeeft in zijn advies over het ontwerp van dit koninklijk besluit (advies DA23004 van 25.04.2023) moeten de exploitatiemiddelen beperkt blijven tot het kunnen raadplegen van gegevens van de A.N.G.

Het Controleorgaan vraagt zich echter af welke exploitatietools kunnen worden gebruikt of niet om de A.N.G. te raadplegen (punt 16 van zijn advies).

In punten 5 en 6 van zijn advies 2/VCI/2023 van 8 juni 2023 stelt het Vast Comité I gelijkaardige vragen: "*Mag slechts gezocht worden op individuele namen? (1) Mogen er (eenmalig/ gedurende een bepaalde tijd/ permanent) lijsten met namen gecorreleerd worden? (2) Mogen er zoekingen gebeuren op basis van vooropgestelde evaluatiecriteria en welke criteria kunnen dit zijn? Mogen er gegevens overgenomen worden(3) ».*

Het is natuurlijk niet de bedoeling van de regering om aan micromanagement te doen en in een koninklijk besluit dat in de ministerraad wordt besproken, te bepalen welke mogelijkheden er zijn om gegevensbanken te raadplegen.

Deze raadpleging kan één voor één gebeuren, bijvoorbeeld door

- een naam, voornaam, geboortedatum, een RRN nummer, een rekeningnummer(..) in te voeren,

- of door een lijst van namen/voornamen, rekeningnummers te gebruiken om tijd te besparen en handmatige fouten te vermijden,

- of door de optie fuzzy search te gebruiken.

Zodra de A.N.G. echter moet worden geraadpleegd volgens vooraf vastgestelde criteria, gelden aanvullende voorzorgsregels om deze toegang te omkaderen en willekeur te voorkomen.

Deze regels, uiteengezet in artikel 2 van het Koninklijk Besluit, zijn als volgt:

1) de toegang tot de A.N.G. op basis van vooraf vastgestelde criteria maakt het voorwerp uit van een schriftelijke en met redenen omklede beslissing van het diensthoofd van de inlichtingen- en veiligheidsdienst of zijn afgevaardigde.

2) in geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde mondeling beslissen om over te gaan tot de toegang op basis van vooraf vastgestelde criteria. Deze mondelinge beslissing wordt op de eerste werkdag die volgt op de datum van de mondelinge beslissing bevestigd door een schriftelijke beslissing.

3) de beslissing van het diensthoofd of zijn afgevaardigde wordt met de motivering van deze beslissing zo spoedig mogelijk aan het Vast Comité I betekend.

4) De beslissing kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek inlichtingenonderzoek. In dit geval wordt een lijst van de gerichte toegangen een maal per maand aan het Vast Comité I doorgegeven.

5) Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden waarin de wettelijke bepalingen niet nageleefd werden.

Deze vooraf opgestelde criteria maken het mogelijk om bevragingen uit te voeren over een bepaalde periode en/of op plaatsen (geregistreerd in het A.N.G.) waar de identiteit van de persoon of de gezochte persoonsgegevens (voertuig bijvoorbeeld) niet in de opzoeking worden vermeld (de vraag).

Deze opzoekingen aan de hand van vooraf vastgelegde criteria moeten het bijvoorbeeld mogelijk maken om alle personen die van 1/1/2020 tot 1/1/2023 in het gerechtelijk arrondissement Antwerpen in de A.N.G. geregistreerd staan voor terroristische feiten, of ook een lijst van alle voertuigen die van 1/1/2020 tot 1/1/2023 in de A.N.G. geregistreerd staan en in verband gebracht worden met terroristische feiten, te verstrekken.

Bovendien heeft de regering duidelijk gemaakt dat, als het nog nodig zou zijn, rechtstreekse toegang niet bedoeld is om de inlichtingen- en veiligheidsdiensten in staat te stellen nieuwe informatie in de A.N.G. te creëren.

In het kader van de wederzijdse uitwisseling zal elke verrijking van gegevens uit de A.N.G. door verdere verwerking door de inlichtingen- en veiligheidsdiensten in voorkomend geval door de politiediensten zelf in de A.N.G. worden aangebracht.

Tot slot is het doel van dit ontwerp van Koninklijk Besluit om een algemeen kader te bieden voor de rechtstreekse toegang door de inlichtingen- en veiligheidsdiensten en niet om de functionele en technische procedures te specificeren, die zullen worden gedetailleerd in functionele en technische protocollen.

Article 1er. L'article 1er reprend les définitions qui sont pertinentes dans le présent projet d'arrêté.

Art. 2. L'article 2 détermine, conformément à l'article 83, 2° de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à l'article 44/11/12, § 2 de la loi sur la fonction de police, les agents des services de renseignement et de sécurité qui jouissent d'un accès direct à la B.N.G.

Afin d'assurer une bonne gestion des accès, les agents des services de renseignement et de sécurité habilités à consulter directement la B.N.G. seront mentionnés sur une liste gérée par le service de renseignement et de sécurité concerné et mise à la disposition du Comité permanent R.

Pour répondre à la recommandation du Comité permanent R dans les points 8 et 9 de son avis, il est bien entendu que l'accès du Comité permanent R à l'historique des listes nominatives et aux versions antérieures de ces listes est garanti, puisque le Comité permanent R a accès aux archives des services de renseignement et de sécurité et que ceux-ci sont en outre tenus par une obligation de conserver la journalisation des traitements dans la B.N.G. pendant 30 ans.

Vu que cette liste constitue 'une photo' des accès accordés par chaque service de renseignement et de sécurité, elle devra être actualisée en permanence. Cela sera par exemple nécessaire lorsqu'un agent part à la pension ou change d'activité.

Cette liste permettra d'effectuer un contrôle a priori du besoin d'en connaître, vu qu'elle mentionnera les tâches spécifiques dévolues à chaque agent disposant d'un accès et justifiant son accès.

Compte tenu de la protection due à l'identité des agents des services de renseignement et à leurs enquêtes, en vertu de l'article 47 de la loi précitée du 30 juillet 2018, la liste ne sera pas transmise à la direction qui gère les accès à la B.N.G. Elle sera conservée au sein du service de renseignement et de sécurité concerné. Cela ne signifie pas pour autant que les consultations des services de renseignement et de sécurité ne seront soumises à aucun contrôle. L'article 6 du présent projet d'arrêté prévoit en effet un mécanisme de contrôle adapté aux spécificités des services de renseignement et de sécurité.

En ce qui concerne le contrôle en matière de protection des données à l'égard des traitements des services de renseignement et de sécurité, il n'y a pas lieu de prévoir une transmission de la liste susvisée vers l'Autorité de protection des données, à l'instar de ce qui est prévu dans les arrêtés royaux du 30 octobre 2015 relatifs à l'accès direct à la B.N.G. de l'Organe de contrôle, du Comité permanent P et du Comité permanent R, puisque c'est le Comité permanent R qui exerce ledit contrôle depuis l'entrée en vigueur de la loi précitée du 30 juillet 2018, en lieu et place de l'ancienne Commission de la protection de la vie privée. Les modalités d'accès, la liste des agents habilités à consulter la B.N.G.et les modalités de contrôle exercé en application de l'article 47 susvisé sont mises à la disposition du Comité permanent R, qui pourra effectuer les recommandations ou les contrôles qu'il estime nécessaires.

Cela étant, la direction qui gère la B.N.G sera immédiatement informée par le service de renseignement et de sécurité concerné, dans l'hypothèse où l'une de leurs consultations provoque un incident sur le plan de l'intégrité, de la fiabilité ou de la disponibilité de la B.N.G., afin de prendre les mesures appropriées pour rétablir l'intégrité, la fiabilité et la disponibilité de la B.N.G. dans les plus brefs délais (article 8).

L'article 2 précise aussi le besoin d'en connaître des agents des services de renseignement et de sécurité. Celui-ci découle logiquement de l'exécution de leurs missions légales définies dans les articles 7 et 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Précisons d'emblée que la consultation effectuée directement par les services de renseignement dans la B.N.G. permet de cibler les données qui sont pertinentes pour le travail de renseignement et d'écarter toutes celles qui ne le sont pas dans le cadre des recherches en cours.

Le besoin d'en connaître des services de renseignement et de sécurité par rapport aux données de la B.N.G. se justifie donc certainement par le fait qu'ils soient les seuls aptes à pouvoir déterminer ce qui leur est utile au sens de l'article 74, 3° de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. C'est un exercice qui s'effectue in concreto dans chaque dossier et pas de manière théorique.

Artikel 1. Artikel 1 herneemt de in het kader van dit ontwerp van besluit relevante definities.

Art. 2. Overeenkomstig artikel 83, 2° van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en artikel 44/11/12, §2 van de wet op het politieambt, bepaalt **artikel 2** de agenten van de inlichtingen- en veiligheidsdiensten die een rechtstreekse toegang tot de A.N.G. genieten

Om een goed beheer van de toegangen te verzekeren, zullen de agenten van de inlichtingen- en veiligheidsdiensten die gemachtigd zijn om de A.N.G. rechtstreeks te raadplegen, vermeld worden op een onder het gezag van de betrokken inlichtingen- en veiligheidsdienst beheerde lijst die ter beschikking gesteld wordt van het Vast Comité I.

In antwoord op de aanbeveling van het Vast Comité I in de punten 8 en 9, wordt ervan uitgegaan dat de toegang van het Vast Comité I tot de historiek van de lijsten en tot de vorige versies van de nominatieve lijsten gewaarborgd is, aangezien het Vast Comité I toegang heeft tot de archieven van de inlichtingen- en veiligheidsdiensten, die ook gebonden zijn door een verplichting om de logbestanden van de verwerkingen in de A.N.G. gedurende 30 jaar te bewaren.

Aangezien deze lijst een 'foto' vormt van de door elke inlichtingen- en veiligheidsdienst verleende toegangen, zal zij bijgevolg permanent dienen bijgewerkt te worden. Dit zal bijvoorbeeld noodzakelijk zijn wanneer een agent op pensioen gaat of van betrekking verandert.

Deze lijst maakt het mogelijk om de behoefte tot kennisname a priori te controleren aangezien zij de specifieke taken zal vermelden die aan elke agent, die over een toegang beschikt, zijn toevertrouwd en die zijn toegang rechtvaardigen

Gelet op de bescherming van de identiteit van de agenten van de inlichtingendiensten en van hun onderzoeken, zal de lijst krachtens artikel 47 van de voornoemde wet van 30 juli 2018 niet worden bezorgd aan de directie die de toegangen tot de A.N.G. beheert. De lijst zal bewaard worden in de betrokken inlichtingen- en veiligheidsdienst. Dit betekent echter niet dat de raadplegingen van de inlichtingen- en veiligheidsdiensten niet aan controle zullen worden onderworpen. Artikel 6 van dit ontwerp van besluit voorziet in een aan de specifieke kenmerken van de inlichtingen- en veiligheidsdiensten aangepast controlemechanisme .

Wat betreft de controle op de gegevensbescherming met betrekking tot de verwerkingen van de inlichtingen- en veiligheidsdiensten, is het niet nodig dat de voornoemde lijst bezorgd wordt aan de Gegevensbeschermingsautoriteit, naar het voorbeeld van wat voorzien is in de koninklijke besluiten van 30 oktober 2015 met betrekking tot de rechtstreekse toegang tot de A.N.G. van het Controleorgaan, het Vast Comité P en het Vast Comité I, aangezien het Vast Comité I deze controle uitoefent sinds de inwerkingtreding van de voornoemde wet van 30 juli 2018, ter vervanging van de toenmalige Commissie voor de bescherming van de persoonlijke levenssfeer. De toegangsmodaliteiten, de lijst van agenten die gemachtigd zijn om de A.N.G. te raadplegen en de controlemodaliteiten uitgevoerd in toepassing van voormeld artikel 47 worden ter beschikking gesteld van het Vast Comité I, dat de aanbevelingen zal kunnen doen of de controles zal kunnen uitvoeren die het nodig acht.

De directie die de A.N.G. beheert, wordt echter onverwijld geïnformeerd door de betrokken inlichtingen- en veiligheidsdienst, indien een van hun raadplegingen aanleiding geeft tot een incident op het gebied van integriteit, betrouwbaarheid of beschikbaarheid van de A.N.G., teneinde de gepaste maatregelen te nemen om de integriteit, betrouwbaarheid en beschikbaarheid van de A.N.G. zo spoedig mogelijk te herstellen (artikel 8).

Artikel 2 wijst ook op de behoefte tot kennisname van de agenten van de inlichtingen- en veiligheidsdiensten. Die behoefte is het logische gevolg van de uitvoering van hun wettelijke opdrachten bepaald in de artikelen 7 en 11 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Vooreerst moet worden opgemerkt dat rechtstreekse raadpleging door de inlichtingendiensten in de A.N.G. het mogelijk maakt om enkel de gegevens die relevant zijn voor het inlichtingenwerk te weerhouden en alle gegevens die dat niet zijn voor het lopende onderzoek, terzijde te leggen.

De kennisbehoefte van de inlichtingen- en veiligheidsdiensten met betrekking tot de gegevens in de A.N.G. is dus zeker gerechtvaardigd omdat alleen zij kunnen bepalen wat voor hen nuttig is in de zin van artikel 74, 3° van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Dit moet in de praktijk uitgevoerd worden, en zal dus in concrete gevallen van elkaar verschillen. Dit kan niet in een theoretisch kader gevat worden.

En d'autres termes, il s'agit d'un travail humain qui peut être guidé par des directives internes mais qui n'est pas automatisable.

Le besoin d'en connaître des agents des services de renseignement et de sécurité a déjà été illustré dans l'exposé des motifs de la loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière. (doc 54 3697/001) :

La question de l'étendue du besoin d'en connaître pour les services de renseignement y avait été explicitée.

Que la B.N.G. soit dans les fait composées de plusieurs containers techniques (la B.N.G. judiciaire, la B.N.G. de police administrative et la B.N.G. roulage,...) n'est in casu pas pertinent (voir point 16 de l'avis de l'organe de contrôle).

L'intention du législateur en 2019 est claire : l'ensemble des données et information contenues dans la B.N.G. doit pouvoir être accessible aux services de renseignement. C'est bien dans cette optique que la loi sur la fonction de police avait été modifiée.

Pour répondre à la demande de l'Organe de contrôle qui demande des précisions quant à l'étendue de l'accès, nous reprenons ce qui est mentionné dans l'exposé des motifs de la loi du 22 mai 2019.

Les passages les plus éclairants sont reproduits ici.

« De manière générale, pour pouvoir réaliser leurs missions, les services de renseignement et de sécurité doivent pouvoir mettre en œuvre leur loi organique, et en particulier son article 14*, de la manière la plus efficace possible.*

A cet égard, les données et informations policières contenues dans la B.N.G. sont essentielles aux services de renseignement et de sécurité pour réaliser leurs missions de protection, de détection, de prévention et d'entrave des menaces à la "sécurité nationale" ou à l'État, qu'il s'agisse de terrorisme ou d'espionnage et d'ingérence.

En effet, les menaces sur lesquelles travaille les services de renseignement et de sécurité trouvent souvent leurs prémisses dans des faits infractionnels ou de menaces à l'ordre public, référencés par la Police dans la B.N.G. et d'autre part, ces menaces peuvent avoir un impact potentiel sur la sécurité/l'ordre public

L'information policière peut donc pour les services de renseignement et de sécurité, signifier le point de départ d'une enquête de renseignement dans des domaines où il y a notamment une responsabilité partagée (ex. terrorisme ou extrémisme).

Par ailleurs, l'information policière constitue pour les enquêtes de renseignement une information contextuelle historique indispensable des antécédents judiciaires et administratifs concernant des individus ou des données à caractère personnel permettant d'enrichir les informations du renseignement et de répondre aux questions investigatives visant à identifier des personnes, à les localiser (par exemple, tel individu a été verbalisé à tel endroit pour un excès de vitesse permet de le localiser à un moment précis), d'établir des liens entre elles et de définir leurs activités en vue d'évaluer si elles représentent une menace au sens de l'article 8 *et de l'art.* 11 *de la Loi organique des services de renseignement et de sécurité du* 30 *novembre* 1998 *(LRS) et d'aider à la prise de décisions politiques, administratives et judiciaires.*

D'un point de vue méthodologique, les finalités des services de renseignement et de sécurité impliquent que la formulation d'hypothèses de recherche est au départ très large et se restreint progressivement au travers de la sélection de données à chaque étape du questionnement investigatif pour détecter des targets et des menaces potentielles.

Pour les services de renseignement et de sécurité, c'est sur l'utilisation des données, leur sélection, au fil des étapes de la recherche qu'est évaluée la proportionnalité. C'est cette sélection de données pertinentes, dans le contexte de la recherche, qui doit être traitée par les services de renseignements et de sécurité avec la plus grande discrétion.

Nous pouvons en outre ajouter que des faits infractionnels sont très souvent commis en marge des menaces sur lesquelles travaillent les services de renseignement et de sécurité. La constatation de ces faits par des agents assermentés qui en dressent des rapports officiels et leur enregistrement dans la B.N.G. font de la B.N.G. une source très utile, dans la mesure où il s'agit d'une base de données de référence pour les missions de police. La consultation de la B.N.G. permet aux services de renseignement et de sécurité de recouper les informations qui sont en leur possession, et éventuellement les compléter, les corriger ou leur apporter un éclairage différent.

Met andere woorden, het is een menselijke taak die kan worden geleid door interne richtlijnen, maar die niet kan worden geautomatiseerd.

De behoefte tot kennisname van de agenten van de inlichtingen- en veiligheidsdiensten is reeds geïllustreerd in de memorie van toelichting bij de wet van 22 mei 2019 tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft(doc 54 3697/001) :

De vraag naar de omvang van de behoefte tot kennisname van de inlichtingendiensten werd toegelicht.

Dat de A.N.G. feitelijk bestaat uit meerdere technische containers (de gerechtelijke A.N.G., de bestuurlijke A.N.G. en de verkeer A.N.G.,...) is in ieder geval hier niet relevant (zie punt 16 van het advies van het Controleorgaan) .

De bedoeling van de wetgever in 2019 is duidelijk: alle gegevens en informatie in het A.N.G. moeten toegankelijk zijn voor de inlichtingendiensten. Met dit in gedachten werd de Politiewet gewijzigd.

In reactie op het verzoek van het Controleorgaan om de reikwijdte van de toegang te verduidelijken, herhalen wij hetgeen is vermeld in de memorie van toelichting bij de wet van 22 mei 2019.

De meest verhelderende passages zijn hier weergegeven.

"In het algemeen moeten de inlichtingen en veiligheidsdiensten, om hun opdrachten te kunnen uitvoeren, haar organieke wet, en in het bijzonder het artikel 14, zo efficiënt mogelijk kunnen aanwenden.

In dit opzicht zijn de politiegegevens en -informatie die vervat zijn in de A.N.G. zijn van essentieel belang voor de inlichtingen en veiligheidsdiensten voor de uitvoering van hun opdrachten op het gebied van bescherming, detectie, preventie en de belemmering van dreigingen voor de "nationale veiligheid" of voor de Staat, of het nu gaat om terrorisme of spionage en inmenging.

De dreigingen die de inlichtingen en veiligheidsdiensten opvolgen, vinden immers vaak hun oorsprong in strafbare feiten of bedreigingen voor de openbare orde, waar de Politie verwijzing van maakt in de A.N.G. en anderzijds kunnen die bedreigingen een impact hebben op de veiligheid/de openbare orde.

De politie-informatie kan voor de inlichtingen en veiligheidsdiensten dus het vertrekpunt zijn van een inlichtingenonderzoek binnen domeinen waar er een gedeelde verantwoordelijkheid is (bv. terrorisme of extremisme).

Voor wat betreft de inlichtingenonderzoeken, vormt de politie-informatie overigens ook een onontbeerlijke bron van historische contextuele informatie, in de vorm van gerechtelijke en administratieve antecedenten van individuen of persoonsgegevens, aan de hand waarvan men de informatie uit het inlichtingenwerk kan aanvullen, een antwoord kan bieden op de onderzoeksvragen voor de identificatie en lokalisatie van personen (bijvoorbeeld wanneer persoon x op plaats x werd bekeurd voor overdreven snelheid kan men deze op een precies tijdstip lokaliseren), verbanden kan leggen tussen deze personen en hun activiteiten kan vaststellen, om zo te beoordelen of deze een bedreiging vormen in de zin van artikel 8 en van 11 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (WIV) en om de politieke, administratieve en gerechtelijke besluitvorming te ondersteunen.

Vanuit methodologisch oogpunt bepalen de finaliteiten van de inlichtingen en veiligheidsdiensten dat de formulering van onderzoekshypotheses in het begin zeer breed is en dan steeds beperkter wordt doorheen de selectie van gegevens bij elke fase van de onderzoeksvraagstelling om potentiële targets en dreigingen te detecteren.

Voor de inlichtingen en veiligheidsdiensten wordt de proportionaliteit beoordeeld aan de hand van het gebruik van de gegevens en de selectie ervan doorheen de verschillende fases van het onderzoek. Het is deze selectie van relevante gegevens, binnen de context van het onderzoek, die door de inlichtingen en veiligheidsdiensten met de grootst mogelijke discretie moet worden behandeld.

We kunnen ook aanhalen dat strafbare feiten heel vaak worden gepleegd binnen het kader van de bedreigingen waar de inlichtingen- en veiligheidsdiensten zich op toeleggen. De vaststelling van deze feiten door beëdigde agenten die hierover officiële verslagen opmaken en hun registratie in de A.N.G., maken van de A.N.G. een zeer nuttige bron aangezien het een referentiedatabank is voor politieopdrachten. Het raadplegen van de A.N.G. stelt de inlichtingen- en veiligheidsdiensten in staat de informatie waarover zij beschikken te vergelijken en eventueel aan te vullen, te corrigeren of er een ander licht op te werpen.

A côté des besoins opérationnels évidents décrits plus haut, ajoutons qu'un accès direct à la B.N.G. permet aussi d'éviter des lenteurs et des lourdeurs administratives. En effet,

- dans le cadre des enquêtes de sécurité, la consultation des données policières par les services d'enquêtes des services de renseignement et de sécurité est déjà prévue par la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Sur demande des services de renseignement et de sécurité, les services de police fournissent les éléments qu'ils estiment pertinents. Un accès direct à la B.N.G supprimerait la lourdeur administrative et les charges de travail respectives ;

- dans le cadre des vérifications de sécurité que les services de renseignement et de sécurité effectuent en tant qu'autorités de sécurité déléguées, l'accès aux données policières est également déjà prévu, mais jusqu'à présent cela s'effectue sur demande des services de renseignement et de sécurité. La consultation directe de la B.N.G facilitera le traitement des dossiers de part et d'autre : les services de police se voient allégés d'une charge de travail et les services de renseignement ne sont plus tributaires du délai de réponse ni de son contenu. Ils ont une vue d'ensemble sur tous les éléments leur permettant de vérifier si la personne concernée n'a pas adopté un comportement problématique au regard du niveau de sécurité recherché.

Comme la plupart des agents des services de renseignement et de sécurité ne sont pas issus à l'origine des services de police, le § 4 de cet article 2 du projet d'AR prévoit une formation préalable à l'accès direct à la B.N.G. pour les agents habilités.

Le protocole d'accord entre chaque service de renseignement et de sécurité et la Direction de l'information policière et des moyens ICT de la police fédérale précisera le contenu et les modalités pratiques de cette formation (qui sera chargé du cours, qui évaluera le suivi de la formation,...)..

Enfin, en exécution de l'article 44/11/12, § 2, *g)* de la loi sur la fonction de police, l'article 2, § 5 du projet d'arrêté entérine le fait que la possession d'une habilitation de sécurité de niveau TRES SECRET, dans le chef des agents des services de renseignement et de sécurité, répond aux exigences de fiabilité, du milieu et des antécédents des agents des services de renseignement et de sécurité ayant un accès direct aux données et informations de la B.N.G.

Art. 3. Le projet d'arrêté veut aussi mettre l'accent sur la responsabilité individuelle des agents des services de renseignement et de sécurité qui jouissent d'un accès direct à la B.N.G.

Ainsi, afin de sensibiliser le personnel sur la responsabilité individuelle en matière de sécurité et de protection des données et de la vie privée afférente à l'accès direct à la B.N.G., chaque agent accédant à la B.N.G. prendra un engagement par écrit (article 3).

Cette responsabilité individuelle s'inscrit bien entendu dans un processus plus large, au niveau de l'institution, relatif à la gestion de la sécurité et de la protection des données. Ce processus global sera d'ailleurs détaillé dans la politique de sécurité de chaque service de renseignement et de sécurité, laquelle sera communiquée aux agents des services de renseignement et de sécurité et sera révisée régulièrement.

Le respect du secret professionnel visé à l'article 36 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité est en outre d'application aux agents des services de renseignement et de sécurité qui accèdent à la B.N.G. La violation de l'article 36 est sanctionnée par les peines énoncées à l'article 43 de la même loi.

Le secret professionnel prescrit par l'article 36 susvisé a un champ d'application plus large que le secret professionnel visé à l'article 458 du Code pénal. Il couvre à la fois les secrets confiés par des particuliers aux agents des services de renseignement, mais aussi l'identité des personnes qui prêtent leur collaboration à l'exécution de la loi et tous les secrets dont les agents ont connaissance dans le cadre de leurs missions.

Art. 4. Le conseiller en sécurité de l'information et le délégué à la protection des données désignés par chaque service de renseignement et de sécurité joueront aussi un rôle important tant préventif que curatif en matière de sécurité des accès à la B.N.G. octroyés aux agents des services de renseignement et de sécurité.

Naast de hierboven beschreven voor de hand liggende operationele behoeften, voorkomt rechtstreekse toegang tot de A.N.G. ook administratieve vertragingen en bureaucratie. Immers,

- in het kader van de veiligheidsonderzoeken werd reeds voorzien in de raadpleging van politionele gegevens door de diensten enquêtes van de inlichtingen- en veiligheidsdiensten door de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Op verzoek van de inlichtingen- en veiligheidsdiensten verstrekken de politiediensten de elementen die zij relevant achten. Een rechtstreekse toegang tot de A.N.G. zou de administratieve rompslomp en respectieve werklast wegnemen;

- in het kader van de veiligheidscontroles die de inlichtingen- en veiligheidsdiensten als gedelegeerde veiligheidsautoriteiten uitvoeren, is ook al voorzien in toegang tot politionele gegevens, maar tot nu toe gebeurt dit op verzoek van de inlichtingen- en veiligheidsdiensten. Rechtstreekse raadpleging van de A.N.G zal de verwerking van dossiers voor beide partijen vergemakkelijken: de politiediensten worden ontlast en de inlichtingendiensten zijn niet langer afhankelijk van responstijd of inhoud. Ze hebben een overzicht van alle elementen waarmee ze kunnen nagaan of de betrokkene geen probleemgedrag heeft vertoond met betrekking tot het nagestreefde veiligheidsniveau.

Aangezien de meeste agenten van de inlichtingen- en veiligheidsdiensten oorspronkelijk niet afkomstig zijn van de politiediensten, voorziet § 4 van dit artikel 2 van het ontwerp van KB in een opleiding voorafgaand aan de rechtstreekse toegang tot de A.N.G. voor gemachtigde agenten.

Het protocolakkoord tussen elke inlichtingen- en veiligheidsdienst en de Directie van de politionele informatie en de ICT-middelen van de federale politie zal de inhoud en de praktische nadere regels van deze opleiding (wie zal de lesgever zijn, wie zal de opvolging van de opleiding beoordelen,...) vastleggen.

In uitvoering van artikel 44/11/12, §2, g) van de wet op het politieambt, bevestigt artikel 2, § 5 van het ontwerp van besluit ten slotte het feit dat het bezitten van een veiligheidsmachtiging van het niveau ZEER GEHEIM, in hoofde van de agenten van de inlichtingen- en veiligheidsdiensten, beantwoordt aan de vereisten van betrouwbaarheid, omgeving en antecedenten van de agenten van de inlichtingen- en veiligheidsdiensten met rechtstreekse toegang tot de gegevens en informatie van de A.N.G.

Art. 3. Het ontwerp van besluit wil ook de klemtoon leggen op de individuele verantwoordelijkheid van de agenten van de inlichtingen- en veiligheidsdiensten die een rechtstreekse toegang tot de A.N.G. genieten.

Om het personeel te sensibiliseren wat betreft de individuele verantwoordelijkheid aangaande de veiligheid en de bescherming van de gegevens en de persoonlijke levenssfeer met betrekking tot de rechtstreekse toegang tot de A.N.G., zal elke agent die toegang tot de A.N.G. heeft, zich op dit vlak schriftelijk engageren (artikel 3).

Deze individuele verantwoordelijkheid maakt vanzelfsprekend deel uit van een breder proces betreffende het beheer van de veiligheid en de gegevensbescherming op het niveau van de instelling. Dit globale proces zal overigens uitvoerig beschreven worden in het veiligheidsbeleid van elke inlichtingen- en veiligheidsdienst, dat aan de agenten van de inlichtingen- en veiligheidsdiensten meegedeeld zal worden en dat regelmatig herzien zal worden.

De naleving van het beroepsgeheim bedoeld in artikel 36 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten is bovendien van toepassing op de agenten van de inlichtingen- en veiligheidsdiensten die toegang hebben tot de A.N.G. Een inbreuk van artikel 36 wordt bestraft met de in artikel 43 van dezelfde wet vermelde straffen.

De reikwijdte van het in artikel 36 voorgeschreven beroepsgeheim is ruimer dan het in artikel 458 van het strafwetboek bedoelde beroepsgeheim. Het betreft niet alleen geheimen die door particulieren aan agenten van de inlichtingendiensten zijn toevertrouwd, maar ook de identiteit van personen die hun medewerking verlenen aan de uitvoering van de wet en alle geheimen waarvan de agenten in de uitoefening van hun functie kennis krijgen.

Art. 4. De informatieveiligheidsconsulent en de functionaris voor gegevensbescherming aangewezen door elke inlichtingen- en veiligheidsdienst zullen ook een belangrijke (zowel preventieve als 'helende') rol spelen in het kader van de veiligheid van de toegangen tot de A.N.G. die verleend worden aan de agenten van de inlichtingen- en veiligheidsdiensten.

En amont, ils devront insérer dans la politique de sécurité, un volet préventif dédié aux règles de sécurité à appliquer lors de l'accès à la B.N.G. Ces règles de sécurité ne seront pas obligatoirement spécifiques à la B.N.G. Elles pourront être globales et valables pour tous les accès à des banques de données externes, pour autant qu'elles soient pertinentes au regard du degré de sensibilité des données et informations enregistrées dans la B.N.G. Ces règles de sécurité répondront en tout état de cause au niveau de garanties fixé par le gestionnaire de la B.N.G. (article 4, §1er, 1°).

Des modalités pratiques relatives à la communication des données de la B.N.G. vers ses partenaires telles que prévue à l'article 5 du projet d'AR devront également être décrites dans cette politique de sécurité.

Enfin, la politique de sécurité du service de renseignement et de sécurité devra inclure des règles internes visant à détecter et mettre fin à un incident de sécurité ou une violation de données.

Ces mesures viendront ainsi compléter les modalités relatives à la communication des incidents de sécurité et de violation de données visée à l'article 8 du projet d'AR.

Un autre point important de ce projet d'arrêté concerne la sécurité des accès à la B.N.G.

Le paragraphe 2 de l'article 4 est relatif à l'obligation de sécurisation du réseau permettant aux agents des services de renseignement et de sécurité d'accéder directement à la B.N.G.

Les modalités concrètes de cette sécurisation n'y sont pas spécifiées, vu qu'elles sont susceptibles d'évoluer, notamment sur la base de l'état d'évolution de la technique et des moyens financiers disponibles.

Ces modalités fonctionnelles et techniques, bien qu'évolutives, sont cependant décrites dans le protocole d'accord entre le service de renseignement et de sécurité concerné et la direction de l'information policière et des moyens ICT de la police fédérale.

Elles sont accessibles au Comité permanent R qui pourra effectuer les recommandations ou les contrôles qu'il estime nécessaires.

Enfin, **le paragraphe 3 de l'article 4** impose aux services de renseignement et de sécurité de prendre les mesures adéquates afin d'assurer la sécurité physique des lieux où des stations de travail des agents des services de renseignement et de sécurité peuvent accéder à la B.N.G.

Les services de renseignement et de sécurité devront aussi s'engager à prendre les mesures de sécurité adéquates pour assurer la protection physique des stations de travail accédant à la B.N.G. Pour cette matière, intrinsèquement liée à l'état de l'évolution de la technique, il s'agit d'inscrire dans le projet d'arrêté une obligation générale de protection, mais pas d'en décrire les modalités concrètes, car celles-ci sont par essence évolutives. L'on peut en effet facilement imaginer que l'accès à la B.N.G., en fonction de l'évolution technique, ne se fasse pas exclusivement au sein des bâtiments des services de renseignement et de sécurité, mais puisse se dérouler dans d'autres lieux.

Vu que les règles relatives aux mesures de sécurité des stations de travail des agents des services de renseignement et de sécurité qui permettent l'accès à la B.N.G. sont liées à l'évolution technique de la B.N.G., il est important qu'avant d'adopter des mesures concrètes, les services de renseignement et de sécurité consultent le délégué à la protection des données désigné pour la B.N.G. et les conseillers en sécurité de l'information des services de renseignement et de sécurité. Ces derniers leur fourniront un avis, notamment sur la faisabilité technique de ces mesures et, s'il échet, leur coût éventuel.

Ces mesures sont transcrites dans le protocole d'accord entre chaque service de renseignement et de sécurité et la direction de l'information policière et des moyens ICT de la police fédérale et sont également mises à la disposition du Comité permanent R.

Ensuite, chaque consultation de la B.N.G. doit faire l'objet d'une motivation par les agents des services de renseignement et de sécurité, de sorte que lorsque son service demande une justification, l'agent qui a consulté la B.N.G. puisse retracer la raison pour laquelle il a effectué la consultation de la B.N.G.

L'agent qui veut consulter la B.N.G. doit, préalablement à chaque consultation, enregistrer cette motivation. De manière concrète, l'enregistrement de la motivation sera sauvegardé par une journalisation, conformément à l'article 3 de l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 et sera accessible selon les règles décrites à l'article 6 du projet d'AR.

Allereerst zal hun veiligheidsbeleid een preventief luik moeten omvatten dat gewijd is aan de veiligheidsregels die moeten worden toegepast bij toegang tot de A.N.G. Die veiligheidsregels zijn niet noodzakelijk specifiek voor de A.N.G. Het kan gaan om globale regels die gelden voor alle toegangen tot externe gegevensbanken, voor zover ze relevant zijn wat betreft de graad van gevoeligheid van de gegevens en informatie geregistreerd in de A.N.G. De veiligheidsregels moeten in ieder geval beantwoorden aan het garantieniveau bepaald door de beheerder van de A.N.G. (artikel 4, §1, 1°).

Praktische regelingen betreffende de mededeling van de gegevens van de A.N.G. aan partners zoals bepaald in artikel 5 van het ontwerp van KB moeten ook beschreven worden in dit veiligheidsbeleid.

Ten slotte moet het veiligheidsbeleid van de inlichtingen- en veiligheidsdienst interne regels bevatten bedoeld om een veiligheidsincident of een inbreuk in verband met gegevens op te sporen en er een einde aan te maken.

Die maatregelen zijn een aanvulling op de modaliteiten betreffende de mededeling van veiligheidsincidenten en inbreuken in verband met gegevens bedoeld in artikel 8 van het ontwerp van KB.

Een ander belangrijk punt van dit ontwerp van besluit heeft betrekking op de beveiliging van de toegangen tot de A.N.G.

Paragraaf 2 van artikel 4 betreft de verplichting tot beveiliging van het netwerk dat de agenten van de inlichtingen- en veiligheidsdiensten toelaat om zich een rechtstreekse toegang tot de A.N.G. te verschaffen.

De concrete nadere regels van deze beveiliging werden hierin niet specifiek opgenomen aangezien deze waarschijnlijk zullen evolueren, onder meer in functie van de stand der techniek en de beschikbare financiële middelen.

Alhoewel ze evolutief zijn, worden deze functionele en technische nadere regels beschreven in het protocolakkoord tussen de betrokken inlichtingen- en veiligheidsdienst en de directie van de politionele informatie en de ICT-middelen van de federale politie.

Zij zijn toegankelijk voor het Vast Comité I dat de aanbevelingen zal kunnen doen of de controles zal kunnen uitvoeren die het nodig acht.

Ten slotte verplicht **paragraaf 3 van artikel 4** de inlichtingen- en veiligheidsdiensten om de gepaste maatregelen te treffen teneinde de fysieke beveiliging te verzekeren van de plaatsen waar werkstations van de agenten van de inlichtingen- en veiligheidsdiensten toegang tot de A.N.G. kunnen hebben.

De inlichtingen- en veiligheidsdiensten zullen zich er ook moeten toe verbinden om de gepaste veiligheidsmaatregelen te treffen teneinde de fysieke beveiliging van de werkstations die een toegang tot de A.N.G. verschaffen, te verzekeren. Voor deze materie, die intrinsiek verbonden is aan de stand der techniek, gaat het erom in het ontwerp van besluit een algemene verplichting tot bescherming in te schrijven, maar niet de concrete nadere regels ervan te beschrijven aangezien deze in essentie evolutief zijn. Men kan zich inderdaad gemakkelijk inbeelden dat de toegang tot de A.N.G., in functie van de technische evolutie, niet uitsluitend in de gebouwen van de inlichtingen- en veiligheidsdiensten zal plaatsvinden, maar dat deze ook op andere plaatsen zal kunnen gebeuren.

Aangezien de regels met betrekking tot de veiligheidsmaatregelen van de werkstations van de agenten van de inlichtingen- en veiligheidsdiensten die zich een toegang verschaffen tot de A.N.G. gebonden zijn aan de technische evolutie van de A.N.G., is het, alvorens concrete maatregelen te treffen, belangrijk dat de inlichtingen- en veiligheidsdiensten de functionaris voor gegevensbescherming aangewezen voor de A.N.G. en de informatieveiligheidsconsulenten van de inlichtingen- en veiligheidsdiensten, raadplegen. Deze laatsten zullen hen een advies verstrekken, onder meer over de technische haalbaarheid van deze maatregelen en, in voorkomend geval, hun eventuele kost.

Deze maatregelen worden beschreven in het protocolakkoord tussen elke inlichtingen- en veiligheidsdienst en de directie van de politionele informatie en de ICT-middelen van de federale politie, en worden ook ter beschikking gesteld van het Vast Comité I.

Elke raadpleging van de A.N.G. moet vervolgens het voorwerp uitmaken van een motivering door de agenten van de inlichtingen- en veiligheidsdiensten zodat, wanneer de dienst van de agent die de A.N.G. heeft geraadpleegd een rechtvaardiging vraagt, de agent de reden kan achterhalen waarom hij de A.N.G. heeft geraadpleegd.

De agent die de A.N.G. wil raadplegen, moet voorafgaand aan elke raadpleging deze motivering registreren. Concreet moet de registratie van de motivering worden opgeslagen door middel van de logbestanden, overeenkomstig artikel 3 van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998, en moet ze toegankelijk zijn volgens de regels beschreven in artikel 6 van het ontwerp van KB.

Les modalités de cet enregistrement sont décrites dans le protocole d'accord entre chaque service de renseignement et de sécurité et la direction de l'information policière et des moyens ICT de la police fédérale.

Des contrôles quant à la légitimité de cet accès devront être effectués régulièrement. Comme recommandé par le Comité permanent R dans son avis (point 11), le présent projet d'arrêté prévoit que ces contrôles réguliers feront l'objet d'un rapport, dont une copie sera adressée au Comité permanent R.

Les données permettant le traçage des traitements effectués constituant elles-mêmes des données sensibles, elles ne pourront, conformément à l'article 6, être utilisées en dehors d'une finalité de contrôle que par le service de renseignement et de sécurité concerné.

Art. 5. Vu les missions dévolues aux services de renseignement et de sécurité, il se peut, comme indiqué à l'article 5, qu'ils soient en outre amenés à communiquer, essentiellement à travers leurs analyses, des données de la B.N.G. à une autorité publique, tant au niveau national qu'au niveau international. Cela sera notamment le cas, lors d'une communication vers les autorités judiciaires belges, dans le cadre d'enquêtes judiciaires, lorsque des données de la B.N.G. sont recoupées par des informations recueillies avec des méthodes de collecte différentes des services de renseignement et de sécurité.

Ce sera aussi le cas lors des échanges avec des correspondants étrangers, dans le cadre d'une enquête de renseignement ayant des ramifications sur le plan international, comme c'est souvent le cas, par exemple, dans le cadre de la prévention du terrorisme. Les données de la B.N.G. intégrées dans les notes d'analyse des services de renseignement seront transmises à des fins de « renseignement » et ne pourront pas être utilisées dans des procédures judiciaires sans autorisation préalable de l'autorité judiciaire. Elles seront revêtues d'un niveau de classification adapté, afin de protéger la confidentialité de ces données sensibles.

Les données de la B.N.G ne seront pas communiquées isolément, telles qu'elles sont enregistrées dans la B.N.G., mais seront intégrées dans l'analyse que les services de renseignement et de sécurité ont réalisée.

Le service de renseignement et de sécurité veillera donc à traiter/enrichir la donnée ou information issue de la B.N.G. avant de la communiquer. Cela signifie que le service de renseignement et de sécurité établit le lien entre la donnée émanant de la B.N.G. et une menace qu'il est lui-même chargé de surveiller dans le cadre de ses missions légales. En effet, la transmission d'une donnée brute risque, par une interprétation erronée, d'influencer la perception du destinataire et l'amener à prendre des décisions inadéquates.

En outre, il ne faudrait pas non plus que la donnée brute soit mise à la disposition des tiers, par l'intermédiaire du destinataire, alors qu'elle devrait bénéficier d'un accès limité au sein des services de police.

Cette communication est, au minimum, soumise aux mêmes conditions de sécurité que les autres données et informations contextualisées par les services de renseignement, est limitée au cadre strict des missions légales des services de renseignement et tient compte de la nature parfois très sensible de certaines données et informations enregistrées dans la B.N.G. (par exemple en matière de terrorisme).

Art. 6. Comme indiqué ci-avant, à propos de l'explication relative à la tenue d'une liste des agents qui ont accès à la B.N.G., les consultations effectuées par chaque service de renseignement et de sécurité feront l'objet de contrôles.

L'article 6 du projet d'arrêté est relatif à un mécanisme clef du contrôle « a posteriori » des accès, à savoir l'imputabilité des traitements effectués aux agents des services de renseignement et de sécurité habilités à consulter directement la B.N.G. C'est pour assurer cette imputabilité qu'un système de journalisation des accès est prévu pendant 30 ans à partir du traitement effectué. Ce système de journalisation doit permettre d'établir de manière irrévocable quel agent des services de renseignement et de sécurité a réalisé quel traitement, à quel moment et pour quelle raison.

Ces données de journalisation faisant le lien entre la consultation effectuée et l'agent du service de renseignement et de sécurité qui l'a réalisée étant par essence sensibles, elles ne seront accessibles qu'au service de renseignement et de sécurité concerné. En revanche, les données de journalisation faisant le lien entre la consultation et le service de renseignement et de sécurité concerné sont accessibles, de manière limitée, dans les conditions fixées à l'article 47 de la loi du 30 juillet 2018.

De modaliteiten van deze registratie worden beschreven in het protocolakkoord tussen elke inlichtingen- en veiligheidsdienst en de directie van de politionele informatie en de ICT-middelen van de federale politie.

Controles aangaande de wettelijkheid van deze toegang zullen op regelmatige wijze moeten uitgevoerd worden. Zoals aanbevolen door het Vast Comité I in haar advies (punt 11), voorziet dit ontwerpbesluit in een verslag over deze regelmatige controles, waarvan een exemplaar zal worden toegezonden aan het Vast Comité I.

De gegevens die de traceerbaarheid van de uitgevoerde verwerkingen mogelijk maken, zijn zelf gevoelige gegevens, en kunnen daarom in overeenstemming met artikel 6, buiten controledoeleinden, slechts door de betrokken inlichtingen- en veiligheidsdienst gebruikt worden.

Art. 5. Gelet op de aan de inlichtingen- en veiligheidsdiensten toevertrouwde opdrachten en zoals aangegeven in artikel 5, kan het voorkomen dat deze diensten er bovendien toe gehouden zullen zijn om, hoofdzakelijk via hun analyses, gegevens van de A.N.G. mee te delen aan een publieke overheid, zowel op nationaal als op internationaal niveau. Dat zal in het bijzonder het geval zijn bij een mededeling aan de Belgische gerechtelijke overheden, in het kader van gerechtelijke onderzoeken, wanneer gegevens van de A.N.G. worden getoetst aan informatie vergaard via verschillende verzamelmethoden van de inlichtingen- en veiligheidsdiensten.

Dat zal ook het geval zijn bij uitwisselingen met buitenlandse correspondenten, in het kader van een inlichtingenonderzoek met vertakkingen op internationaal vlak, zoals vaak het geval is, bijvoorbeeld in het kader van de preventie van terrorisme. De in de analysenota's van de inlichtingendiensten geïntegreerde gegevens van de A.N.G. zullen worden verzonden voor "inlichtingendoeleinden" en zullen niet kunnen worden gebruikt in gerechtelijke procedures zonder voorafgaande goedkeuring van de gerechtelijke overheid. Ze zullen een aangepast classificatieniveau krijgen om de vertrouwelijkheid van deze gevoelige gegevens te beschermen.

De gegevens van de A.N.G. zullen niet afzonderlijk worden meegedeeld, zoals ze geregistreerd zijn in de A.N.G., maar zullen worden geïntegreerd in de analyse uitgevoerd door de inlichtingen- en veiligheidsdiensten.

De inlichtingen- en veiligheidsdienst waakt er dus over de gegevens of informatie uit de A.N.G. te verwerken/verrijken alvorens deze mee te delen. Dit betekent dat de inlichtingen- en veiligheidsdienst het verband legt tussen de gegevens die afkomstig zijn van de A.N.G. en een dreiging die het zelf in het oog moet houden in het kader van zijn wettelijke taken. De verzending van ruwe gegevens zou immers door een foute interpretatie de perceptie van de ontvanger kunnen beïnvloeden en hem ertoe leiden ongepaste beslissingen te nemen.

Bovendien zou het niet kunnen dat de ruwe gegevens via de ontvanger aan derden ter beschikking worden gesteld, terwijl ze binnen de politiediensten beperkt toegankelijk moeten zijn.

Deze mededeling is minstens onderworpen aan dezelfde veiligheidsvoorwaarden als de andere gegevens en informatie verwerkt door de inlichtingendiensten, is beperkt tot het strikte kader van de wettelijke opdrachten van de inlichtingendiensten en houdt rekening met de soms zeer gevoelige aard van bepaalde gegevens en informatie geregistreerd in de A.N.G. (bijvoorbeeld wat terrorisme betreft).

Art. 6. Zoals hoger aangegeven in de uitleg over het bijhouden van een lijst van de agenten die toegang hebben tot de A.N.G., zullen de raadplegingen uitgevoerd door elke inlichtingen- en veiligheidsdienst het voorwerp uitmaken van controles.

Artikel 6 van het ontwerp van besluit heeft betrekking op een sleutelmechanisme om de toegangen "a posteriori" te controleren, met name de toerekenbaarheid voor de uitgevoerde verwerkingen aan de agenten van de inlichtingen- en veiligheidsdiensten die gemachtigd zijn om rechtstreeks de A.N.G. te raadplegen. Om deze verantwoordelijkheid te verzekeren wordt er voorzien in een systeem van logbestanden van de toegangen gedurende 30 jaar vanaf de uitgevoerde verwerking. Dit loggingsysteem moet het mogelijk maken om definitief vast te stellen welke agent van de inlichtingen- en veiligheidsdiensten welke verwerking uitgevoerd heeft, op welk ogenblik en om welke reden dat gebeurde.

Omdat deze logbestanden die de uitgevoerde raadpleging koppelen aan de agent van de inlichtingen- en veiligheidsdienst die deze heeft uitgevoerd in wezen gevoelig zijn, zullen ze alleen toegankelijk zijn voor de betrokken inlichtingen- en veiligheidsdienst. Anderzijds zijn de logbestanden die de link leggen tussen de raadpleging en de betrokken inlichtingen- en veiligheidsdienst beperkt toegankelijk onder de voorwaarden bepaald in artikel 47 van de wet van 30 juli 2018.

En d'autres termes, du côté de la police, chaque transaction sera loggée de sorte que les personnes autorisées puissent voir que la VSSE ou le SGRS a accédé à telle ou telle donnée sans toutefois identifier un agent de cette institution. Et du côté de la VSSE et du SGRS, l'identité de l'agent qui a effectué le traitement sera jointe aux données de journalisation. Il ne s'agit pas d'un double système de journalisation, mais d'un continuum de journalisation avec des accès différenciés aux données des logs (avec ou sans identification des agents).

En outre, ce système permet également le contrôle complet de tous les traitements effectués dans le cadre de cet accès. Une collaboration entre le Comité permanent R et l'Organe de contrôle de l'information policière permettra à ces instances d'optimiser les contrôles qu'ils seront amenés à effectuer dans le cadre de leurs compétences, à l'instar de ce qui est actuellement pratiqué pour la banque de données commune Terrorist Fighters.

Cette collaboration s'inscrit pleinement dans le protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données.

L'article 47 susvisé organise le contrôle qui peut être exercé à l'égard des traitements de données à caractère personnel que les services de renseignement et de sécurité effectuent dans des banques de données externes, comme ce sera le cas en l'occurrence pour la B.N.G. La journalisation de ces traitements des services de renseignement et de sécurité, prévue à l'article 6 du présent projet, est accessible à la personne désignée par le(s) responsable(s) du traitement pour la B.N.G. et au DPO désigné pour la B.N.G., d'une part, et, d'autre part, au service de renseignement et de sécurité concerné, bien entendu. L'accès à la journalisation des traitements et à son contenu n'est autorisé que pour une finalité de contrôle. Un accès pour une autre finalité n'est pas exclu dans la loi du 30 juillet 2018. Cette finalité, autre que le contrôle, doit alors être précisée dans un protocole d'accord.

Si pour une raison ou une autre, une consultation effectuée par les services de renseignement et de sécurité paraît problématique, un contrôle sera alors exercé en application de l'article 47 de la loi du 30 juillet 2018 et la personne déléguée par le(s) responsable(s) du traitement pour la B.N.G. et/ou le délégué à la protection des données pour la B.N.G. se concertent dans les meilleurs délais avec le dirigeant du service de renseignement concerné et/ou avec le délégué à la protection des données dudit service, pour prendre les mesures appropriées. Les modalités du contrôle exercé sur la base des données de la journalisation sont décrites dans le protocole d'accord mentionné plus haut.

A côté des contrôles effectués en application de l'article 47 susvisé, le Comité permanent R peut, à tout moment et en tous lieux, d'initiative ou à la suite d'une plainte ou d'une requête déposée par un particulier, effectuer des contrôles dans le cadre de ses compétences, d'une part, d'organe de contrôle général du fonctionnement des services de renseignement et de sécurité (loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace) et, d'autre part, d'autorité de contrôle en matière de protection des données contextualisées par les services de renseignement et de sécurité.

Art. 7. L'article 7 est relatif aux traitements automatisés qui peuvent être effectués sur la base des données de la B.N.G. (exécution de l'article 44/11/12, § 2, *c)* de la loi sur la fonction de police).

Il se peut en effet que les données de la B.N.G. utiles dans le cadre des missions de renseignement soient enregistrées dans une banque de données gérée par un service de renseignement et de sécurité.

Le projet d'arrêté prévoit que les données émanant de la B.N.G. doivent être contextualisées lorsqu'elles sont enregistrées dans une banque de données gérées par un service de renseignement et de sécurité. Cela signifie que le service de renseignement et de sécurité concerné doit établir un lien entre la donnée de la B.N.G. et une menace qu'il est lui-même chargé de surveiller dans le cadre de ses compétences légales.

Les banques de données des services de sécurité et de renseignement dans lesquelles sont enregistrées des données de la B.N.G. doivent être entourées de garanties assurant un niveau de sécurité similaire à celui qui est en vigueur pour la B.N.G.

Il va par ailleurs de soi que conformément à l'article 75 de la loi cadre en matière de protection des données les services de renseignement sont tenus avant d'utiliser de l'information de la B.N.G. enregistrées dans leurs banques de données de consulter à nouveau la B.N.G. afin de mettre à jour ces informations.

Met andere woorden, aan de kant van de politie zal elke transactie worden geregistreerd, zodat bevoegde personen kunnen zien dat VSSE of ADIV deze of gene gegevens heeft geraadpleegd zonder een agent van die instelling te identificeren. En aan de kant van de VSSE en ADIV wordt de identiteit van de agent die de verwerking heeft uitgevoerd aan de logbestanden gekoppeld. Dit is geen dubbel systeem van logbestanden, maar een continuüm van logbestanden met gedifferentieerde toegang tot loggegevens (met of zonder agentidentificatie).

Bovendien maakt dit systeem ook een volledige controle mogelijk van alle verwerkingen die in het kader van deze toegang worden uitgevoerd. De samenwerking tussen het Vast Comité I en het controleorgaan zal deze organen in staat stellen de controles die zij in het kader van hun opdracht uitvoeren, te optimaliseren, zoals momenteel het geval is voor de gemeenschappelijke gegevensbank Terrorist Fighters.

Deze samenwerking is volledig in overeenstemming met het samenwerkingsprotocol tussen de Belgische toezichthoudende autoriteiten op het vlak van dataprotectie

Het voornoemde artikel 47 organiseert de controle die kan worden uitgeoefend met betrekking tot de verwerkingen van persoonsgegevens uitgevoerd door de inlichtingen- en veiligheidsdiensten in externe gegevensbanken, zoals hier het geval is voor de A.N.G. De logbestanden van die verwerkingen van de inlichtingen- en veiligheidsdiensten, bepaald in artikel 6 van dit ontwerp, zijn toegankelijk voor de persoon aangewezen door de verwerkingsverantwoordelijke(n) voor de A.N.G. en voor de DPO aangewezen voor de A.N.G., enerzijds, en uiteraard voor de betrokken inlichtingen- en veiligheidsdienst, anderzijds. De toegang tot de logbestanden van de verwerkingen en de inhoud ervan is enkel toegestaan voor controledoeleinden. Een toegang voor andere doeleinden is niet uitgesloten in de wet van 30 juli 2018. Andere doeleinden dan controledoeleinden moeten dan verduidelijkt worden in een protocolakkoord.

Indien om de een of andere reden een raadpleging uitgevoerd door de inlichtingen- en veiligheidsdiensten problematisch blijkt te zijn, zal er een controle uitgevoerd worden in toepassing van artikel 47 van de wet van 30 juli 2018, en overleggen de persoon gedelegeerd door de verwerkingsverantwoordelijke(n) voor de A.N.G. en/of de functionaris gegevensbescherming voor de A.N.G. zo spoedig mogelijk met het diensthoofd van de betrokken inlichtingendienst en/of met de functionaris gegevensbescherming van deze dienst om de passende maatregelen te nemen. De modaliteiten van de controle uitgeoefend op basis van de logginggegevens staan beschreven in het hogergenoemde protocolakkoord.

Naast de controles die worden uitgevoerd in toepassing van het voormelde artikel 47, kan het Vast Comité I op elk moment en op elke plaats, op eigen initiatief of naar aanleiding van een klacht of verzoek ingediend door een particulier, controles uitvoeren in het kader van zijn bevoegdheden, enerzijds als orgaan van algemene controle op de werking van de inlichtingen- en veiligheidsdiensten (wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse) en anderzijds als toezichthoudende autoriteit voor de bescherming van gegevens die door de inlichtingen- en veiligheidsdiensten worden verwerkt.

Art. 7. Artikel 7 heeft betrekking op de geautomatiseerde verwerkingen die kunnen uitgevoerd worden op basis van de gegevens van de A.N.G. (uitvoering van artikel 44/11/12, §2, c) van de wet op het politieambt.

Het kan namelijk voorkomen dat nuttige gegevens van de A.N.G. in het kader van inlichtingen opdrachten geregistreerd worden in een door een inlichtingen- en veiligheidsdienst beheerde gegevensbank.

Het ontwerpbesluit bepaalt dat gegevens van de A.N.G. in een context moeten worden geplaatst wanneer ze worden opgenomen in een gegevensbank die wordt beheerd door een inlichtingen- en veiligheidsdienst. Dit betekent dat de betreffende inlichtingen- en veiligheidsdienst een verband moet leggen tussen gegevens uit de A.N.G. en een dreiging die hij zelf in het kader van zijn wettelijke bevoegdheden in het oog moet houden.

De gegevensbanken van de inlichtingen- en veiligheidsdiensten waarin gegevens van de A.N.G. zijn geregistreerd moeten voorzien zijn van garanties die een veiligheidsniveau waarborgen dat vergelijkbaar is met dat van toepassing op de A.N.G.

Het spreekt vanzelf dat de inlichtingendiensten overeenkomstig artikel 75 van de kaderwet inzake gegevensbescherming verplicht zijn de A.N.G. opnieuw te raadplegen om de in hun databanken opgeslagen informatie bij te werken alvorens deze te gebruiken.

Art. 8. Enfin, en cas de violation de données ou d'incident en matière de sécurité, il revient à chaque service de renseignement et de sécurité de prendre immédiatement les mesures les plus appropriées pour mettre fin à cette violation ou incident. Il peut s'agir du retrait de l'accès de l'agent concerné, comme d'une limitation de son accès. Tout dépend de la violation ou de l'incident qui est constaté. Le cas échéant, le service de renseignement et de sécurité concerné prendra les mesures disciplinaires qui s'imposent. Il devra aussi évaluer si des suites pénales doivent être données conséquemment à la violation des règles en matière d'accès. Par incident de sécurité, il faut par exemple comprendre une coupure de l'accès à la B.N.G. ou la transmission indue de données de la B.N.G.

Cela étant, il va de soi que, même en cas d'incident de sécurité grave, l'accès des services de renseignement et de sécurité aux données de la B.N.G. ne peut être empêché. En effet, la combinaison des articles 14 et 20 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et 92 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel pose clairement le principe selon lequel il ne peut y avoir d'interruption dans la communication de données vers les services de renseignement et de sécurité. En fonction du type d'incident de sécurité, un moyen de communication autre que l'accès direct peut temporairement être utilisé, jusqu'à ce qu'il soit mis fin à l'incident de sécurité.

Afin de minimaliser les impacts que pourrait engendrer l'incident sur le bon déroulement des missions exécutées par les services de police ou de remédier aux impacts de la violation sur l'intégrité, la fiabilité ou la disponibilité de la B.N.G., en ce compris l'accès des services de renseignement et de sécurité à la B.N.G., une intervention rapide est souhaitable et il convient de communiquer le problème au gestionnaire de la B.N.G. et son délégué à la protection des données. En effet, une intervention technique et/ou fonctionnelle sera peut-être nécessaire.

Les modalités relatives à cette communication seront décrites dans le protocole d'accord entre chaque service de renseignement et de sécurité et la Direction de l'information policière et des moyens ICT de la police fédérale.

J'ai l'honneur d'être,

Sire,
de Votre Majesté,
le très respectueux
et très fidèle serviteur,

Donné à Bruxelles, 23 novembre 2023.

PHILIPPE

Par le Roi :

Le Ministre de la Justice,
P. VAN TIGCHELT

La Ministre de l'Intérieur,
A. VERLINDEN

La Ministre de la Défense,
L. DEDONDER

---

23 NOVEMBRE 2023. — Arrêté royal relatif à l'accès direct des services de renseignement et de sécurité aux données à caractère personnel et informations de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la loi sur la fonction de police du 5 août 1992, notamment l'article 44/11/12, § 1er, 1°, et § 2,

Vu l'avis de l'Inspecteur des Finances auprès de la police fédérale, donné le 23 décembre 2022 ;

Vu l'avis de l'Inspecteur des Finances auprès du ministre de la Justice, donné le 16 janvier 2023 ;

Vu l'accord de la Secrétaire d'Etat au Budget, donné le 1er février 2023 ;

Vu l'avis 73.145/2 du Conseil d'État, donné le 20 mars 2023, en application de l'article 84, § 1er, alinéa 1er, 2°, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973 ;

Vu l'avis de l'Organe de contrôle de l'information policière, donné le 25 avril 2023 ;

Art. 8. Bij veiligheidsincidenten of inbreuken in verband met gegevens neemt elke inlichtingen- en veiligheidsdienst onmiddellijk de meest geschikte maatregelen om een einde te maken aan dit incident of deze inbreuk. Die maatregelen kunnen betrekking hebben op zowel de intrekking als de beperking van de toegang van de betrokken agent. Alles hangt af van het incident of de inbreuk die werden vastgesteld. In voorkomend geval zal de betrokken inlichtingen- en veiligheidsdienst de nodige tuchtrechtelijke maatregelen nemen. De betrokken dienst zal tevens moeten bekijken of er strafrechtelijke gevolgen moeten worden gegeven aan de schending van de toegangsregels. Onder veiligheidsincident moet bijvoorbeeld een onderbreking van de toegang tot de A.N.G. of de ongepaste verzending van gegevens van de A.N.G. verstaan worden

Het spreekt echter voor zich dat ook bij een ernstig veiligheidsincident de toegang van de inlichtingen- en veiligheidsdiensten tot de gegevens van de A.N.G. niet kan worden verhinderd. De combinatie van de artikelen 14 en 20 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en 92 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens poneert immers duidelijk het principe dat er geen onderbreking mag zijn in de mededeling van gegevens aan de inlichtingen- en veiligheidsdiensten. In functie van het type veiligheidsincident kan tijdelijk een ander communicatiemiddel dan rechtstreekse toegang gebruikt worden tot er een einde is gemaakt aan het veiligheidsincident.

Om de gevolgen die het incident zou kunnen hebben op de goede uitvoering van de opdrachten door de politiediensten te beperken of om de gevolgen van de inbreuk op de integriteit, betrouwbaarheid of beschikbaarheid van de A.N.G. te verhelpen, met inbegrip van de toegang tot de A.N.G. door de inlichtingen- en veiligheidsdiensten, is een snelle interventie wenselijk en wordt het probleem meegedeeld aan de beheerder van de A.N.G. en zijn functionaris gegevensbescherming. Een technische en/of functionele interventie kan immers nodig zijn.

De modaliteiten met betrekking tot deze mededeling worden beschreven in het protocolakkoord tussen elke inlichtingen- en veiligheidsdienst en de Directie van de politionele informatie en de ICT-middelen van de federale politie.

Ik heb de eer te zijn,

Sire,
van Uwe Majesteit,
de zeer eerbiedige
en zeer getrouwe dienaar,

Gegeven te Brussel, 23 november 2023.

FILIP

Van Koningswege :

De Minister van Justitie,
P. VAN TIGCHELT

De Minister van Binnenlandse Zaken
A. VERLINDEN

De Minister van Defensie,
L. DEDONDER

---

23 NOVEMBER 2023. — Koninklijk besluit betreffende de rechtstreekse toegang van de inlichtingen- en veiligheidsdiensten tot de persoonsgegevens en de informatie van de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de wet op het politieambt van 5 augustus 1992, inzonderheid op artikel 44/11/12, § 1, 1° en § 2,

Gelet op het advies van de Inspecteur van Financiën bij de federale politie, gegeven op 23 december 2022;

Gelet op het advies van de Inspecteur van Financiën bij de minister van Justitie, gegeven op 16 januari 2023;

Gelet op het akkoord van de Staatsecretaris voor Begroting, gegeven op 1 februari 2023;

Gelet op het advies 73.145/2 van de Raad van State, verleend op 20 maart 2023, met toepassing van het artikel 84, § 1, eerste lid, 2°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Gelet op het advies van het Controleorgaan op de politionele informatie verleend op 25 april 2023;

Vu l'avis du Comité Permanent R, en sa qualité d'Autorité de contrôle compétente, donné le 9 juin 2023 ;

Vu l'exemption d'analyse d'impact visée à l'article 8, § 2, 1° de la loi du 15 décembre 2013 portant des dispositions diverses concernant la simplification administrative ;

Considérant la loi organique sur les services de renseignement et de sécurité du 30 novembre 1998, notamment les articles 7, 8, 11, 13, 14, 20, 21, et 36 ;

Considérant la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 30 juillet 2018, notamment les titres II et III ;

Sur la proposition des Ministres de l'Intérieur, de la Justice et de la Défense, et de l'avis des Ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

Article 1er. Pour l'application du présent arrêté, il faut entendre par :

1° « la loi sur la fonction de police » : la loi du 5 août 1992 relative à la fonction de police ;

2° « la B.N.G. » : la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police ;

3° « la loi du 30 novembre 1998 » : la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;

4° « le Comité permanent R » : le Comité permanent de contrôle des services de renseignement et de sécurité visé dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace ;

5° « la loi du 30 juillet 2018 » : la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

6° « la journalisation » : le mécanisme permettant la traçabilité des consultations de données effectués dans la B.N.G.

Art. 2. § 1er. Dans l'intérêt de l'exercice de leurs missions visées dans la loi du 30 novembre 1998 ou pour l'exécution de toutes autres missions qui leur sont confiées par ou en vertu de la loi, les agents des services de renseignement et de sécurité ont un accès direct à l'ensemble des informations et des données à caractère personnel de la B.N.G., visées à l'article 44/5 de la loi sur la fonction de police.

§ 2. Lorsque cet accès direct s'effectue sur la base de critères préétablis, il fait l'objet d'une décision écrite motivée du dirigeant du service de renseignement et de sécurité concerné ou de son délégué. En cas d'urgence, le dirigeant du service ou son délégué peut décider verbalement de procéder à l'accès sur la base de critères préétablis. Cette décision verbale est confirmée par une décision écrite, le premier jour ouvrable qui suit la date de la décision verbale.

La décision du dirigeant du service ou de son délégué et sa motivation sont transmises au Comité permanent R dans les meilleurs délais.

La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, une liste des accès ponctuels est communiquée une fois par mois au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans des conditions qui ne respectent pas les dispositions légales.

§ 3. Le dirigeant de chaque service de renseignement et de sécurité désigne les agents autorisés à accéder aux données et informations dans la B.N.G., dans la mesure où celles-ci sont utiles dans l'exercice de leur fonction ou de leur mission.

Le dirigeant du service concerné tient en permanence à la disposition du Comité permanent R la liste nominative des agents désignés, avec indication de leur titre et de leur fonction. Le dirigeant du service concerné tient la liste à jour.

§ 4. Les agents désignés conformément au paragraphe 3 suivent une formation préalablement à l'obtention de l'accès direct dont les modalités pratiques sont déterminées dans un protocole d'accord entre chaque service de renseignement et de sécurité et la Direction de l'information policière et des moyens ICT de la police fédérale.

Gelet op het advies van het Vast Comité I; in haar hoedanigheid van bevoegde toezichthoudende autoriteit, verleend op 9 juni 2023;

Gelet op de vrijstelling van impactanalyse bedoeld in artikel 8, §2, 1° van de wet van 15 december 2013 houdende diverse bepalingen inzake administratieve vereenvoudiging;

Gelet op de wet houdende regeling van de inlichtingen- en veiligheidsdiensten wet van 30 november 1998, inzonderheid op de artikelen 7,8, 13, 20, 21, et 36;

Gelet op de wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens van 30 juli 2018, inzonderheid op de titels II et III ;

Op de voordracht van de Ministers van Binnenlandse Zaken, van Justitie en van Defensie en op het advies van de in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij :

Artikel 1. Voor de toepassing van dit besluit, wordt verstaan onder:

1° "de wet op het politieambt": de wet van 5 augustus 1992 op het politieambt;

2° "de A.N.G.": de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt;

3° "de wet van 30 november 1998": de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

4° "het Vast Comité I": het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

5° "de wet van 30 juli 2018": de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

6° "de logbestanden": het mechanisme dat toelaat de in de A.N.G. uitgevoerde raadplegingen op te sporen.

Art. 2. § 1. In het belang van de uitoefening van hun opdrachten bedoeld in de wet van 30 november 1998 of voor de uitoefening van alle andere opdrachten die hun worden toevertrouwd door of krachtens de wet, hebben de agenten van de inlichtingen- en veiligheidsdiensten een rechtstreekse toegang tot alle informatie en persoonsgegevens van de A.N.G. bedoeld in artikel 44/5 van de wet op het politieambt.

§ 2. Wanneer deze rechtstreekse toegang wordt verleend op basis van vooraf vastgestelde criteria, is een met redenen omkleed schriftelijk besluit van het diensthoofd van de inlichtingen- en veiligheidsdienst of zijn gedelegeerde vereist. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde mondeling beslissen om over te gaan tot de toegang op basis van vooraf vastgestelde criteria. Deze mondelinge beslissing wordt op de eerste werkdag die volgt op de datum van de mondelinge beslissing bevestigd door een schriftelijke beslissing.

De beslissing van het diensthoofd of zijn gedelegeerde wordt met de motivering van deze beslissing zo spoedig mogelijk aan het Vast Comité I betekend.

De beslissing kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek inlichtingenonderzoek. In dit geval wordt een lijst van de gerichte toegangen een maal per maand aan het Vast Comité I doorgegeven. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke bepalingen voldoen.

§ 3. Het diensthoofd van elke inlichtingen- en veiligheidsdienst wijst de agenten aan die gemachtigd zijn om toegang te hebben tot de gegevens en informatie in de A.N.G., voor zover deze nuttig zijn in de uitoefening van hun functie of opdracht.

Het betrokken diensthoofd houdt te allen tijde de nominatieve lijst van de aangewezen agenten, met vermelding van hun titel en functie, ter beschikking van het Vast Comité I. Het betrokken diensthoofd houdt de lijst bij.

§ 4. Voordat de overeenkomstig paragraaf 3 aangewezen agenten rechtstreekse toegang krijgen, volgen zij een opleiding waarvan de praktische modaliteiten worden vastgelegd in een protocolakkoord tussen elke inlichtingen- en veiligheidsdienst en de Directie van de politionele informatie en de ICT-middelen van de federale politie.

§ 5. La possession d'une habilitation de sécurité de niveau « très secret », telle que visée par la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, dans le chef des agents des services de renseignement et de sécurité, répond aux exigences de fiabilité, du milieu et des antécédents des agents visés à l'article 44/11/12, § 2, *g)* de la loi sur la fonction de police.

Art. 3. Les agents visés à l'article 2 s'engagent par écrit à veiller à la sécurité et à la confidentialité des données auxquelles ils ont accès. Cet engagement est versé dans leur dossier personnel.

Ils sont en outre soumis au secret professionnel tel que visé à l'article 36 de la loi du 30 novembre 1998.

Art. 4. § 1er. Le conseiller en sécurité de l'information et le délégué à la protection des données de chaque service de renseignement et de sécurité sont chargés :

1° d'inclure dans la politique de sécurité un volet relatif aux :

a) règles de sécurité à appliquer par les agents visés à l'article 2 en matière d'accès ;

b) règles applicables aux communications visées à l'article 5 ;

c) mesures à prendre en interne afin de pouvoir détecter et mettre fin à un incident de sécurité ou une violation de données tels que visés à l'article 8.

2° des contacts avec le Comité permanent R pour ce qui concerne les traitements des données issues de la B.N.G.

§ 2. Les modalités fonctionnelles et techniques des accès sont spécifiées dans le protocole d'accord visé à l'article 2, § 4. Ces modalités sont transmises au Comité permanent R.

§ 3. Chaque service de renseignement et de sécurité veille à ce que les stations de travail qui accèdent directement à la B.N.G. soient sécurisées par des mesures adéquates et ce, en tous lieux où l'accès est possible.

Ces mesures sont détaillées dans le protocole d'accord visé à l'article 2, § 4.

§ 4. Les conseillers en sécurité de l'information des services de renseignement et de sécurité et les délégués à la protection des données désignés respectivement pour la B.N.G. et par les services de renseignement et de sécurité sont consultés lors de l'élaboration des mesures visées au paragraphe 3.

§ 5. Les agents visés à l'article 2 enregistrent la motivation pour chaque consultation directe des données et informations dans la B.N.G. en vue d'un éventuel contrôle ultérieur. Cette motivation doit être conforme aux missions légales du service de renseignement et de sécurité concerné.

§ 6. Chaque service de renseignement et de sécurité vérifie à échéances régulières la conformité des consultations des données et informations de la B.N.G. effectuées par les agents visés à l'article 2 et en dresse un rapport. Une copie de ce rapport est adressée au Comité permanent R.

Art. 5. Conformément aux articles 19 et 20 de la loi du 30 novembre 1998, les services de renseignement et de sécurité peuvent, dans le cadre strict de leurs missions légales, communiquer à une autorité publique les données et informations de la B.N.G. qu'ils ont préalablement contextualisées.

Art. 6. Toutes les consultations réalisées dans la B.N.G. par les services de renseignement et de sécurité font l'objet d'une journalisation. Les données de cette journalisation sont conservées pendant 30 ans à partir du traitement réalisé.

Les données et informations de la journalisation visée à l'alinéa 1er sont conservées auprès de la direction qui gère les accès à la B.N.G. et au sein de chaque service de renseignement et de sécurité, chacun en ce qui le concerne.

La journalisation des consultations des services de renseignement et de sécurité dans la B.N.G. effectuée par la direction qui gère les accès à la B.N.G. permet d'assurer la traçabilité de la consultation réalisée par le service de renseignement et de sécurité dans la B.N.G.

§ 5. Het bezitten van een veiligheidsmachtiging van het niveau "zeer geheim", zoals bedoeld in de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, beantwoordt in hoofde van de agenten van de inlichtingen- en veiligheidsdiensten aan de vereisten van betrouwbaarheid, omgeving en antecedenten van de agenten bedoeld in artikel 44/11/12, §2, g) van de wet op het politieambt.

Art. 3. De agenten bedoeld in artikel 2 verbinden zich er schriftelijk toe te waken over de veiligheid en de vertrouwelijkheid van de gegevens waartoe ze toegang hebben. Deze verbintenis wordt toegevoegd aan hun persoonlijk dossier.

Daarnaast zijn zij gehouden tot het beroepsgeheim zoals bedoeld in artikel 36 van de wet van 30 november 1998.

Art. 4. § 1. De informatieveiligheidsconsulent en de functionaris voor gegevensbescherming van elke inlichtingen- en veiligheidsdienst zijn verantwoordelijk voor:

1° het opnemen in het veiligheidsbeleid van een luik met betrekking tot:

a) veiligheidsregels die moeten worden toegepast door de agenten bedoeld in artikel 2 inzake toegang;

b) regels die van toepassing zijn op de mededelingen bedoeld in artikel 5;

c) maatregelen die intern genomen moeten worden teneinde een veiligheidsincident of een inbreuk in verband met gegevens zoals bedoeld in artikel 8 te kunnen opsporen en er een einde aan te maken.

2° de contacten met het Vast Comité I met betrekking tot de verwerking van de gegevens uit de A.N.G.

§ 2. De functionele en technische nadere regels van de toegang worden bepaald in het protocolakkoord bedoeld in artikel 2, § 4. Die nadere regels worden aan het Vast Comité I meegedeeld.

§ 3. Elke inlichtingen- en veiligheidsdienst zorgt ervoor dat de werkstations die een rechtstreekse toegang tot de A.N.G. verlenen, beveiligd zijn met passende maatregelen en dit op alle plaatsen waar toegang mogelijk is.

Die maatregelen worden uitvoerig beschreven in het protocolakkoord bedoeld in artikel 2, §4.

§ 4. De informatieveiligheidsconsulenten van de inlichtingen- en veiligheidsdiensten en de functionarissen voor gegevensbescherming, respectievelijk aangewezen voor de A.N.G. en door de inlichtingen- en veiligheidsdiensten, worden geraadpleegd bij het uitwerken van de maatregelen bedoeld in paragraaf 3.

§ 5. De agenten bedoeld in artikel 2, §2 registreren de motivering voor elke rechtstreekse raadpleging van de gegevens en informatie in de A.N.G. Die motivering moet overeenstemmen met de wettelijke opdrachten van de betrokken inlichtingen- en veiligheidsdienst.

§ 6. Elke inlichtingen- en veiligheidsdienst gaat op regelmatige tijdstippen de conformiteit na van de raadplegingen van de gegevens en informatie van de A.N.G. uitgevoerd door de agenten bedoeld in artikel 2 en stelt hiervan een verslag op. Een kopie van dit verslag wordt toegezonden aan het Vast Comité I.

Art. 5. Overeenkomstig de artikelen 19 en 20 van de wet van 30 november 1998 kunnen de inlichtingen- en veiligheidsdiensten binnen het strikte kader van hun wettelijke opdrachten de vooraf door hen gecontextualiseerde gegevens en informatie van de A.N.G. aan een publieke overheid meedelen.

Art. 6. Alle door de inlichtingen- en veiligheidsdiensten uitgevoerde raadplegingen in de A.N.G. maken het voorwerp uit van de logbestanden. De logbestanden worden bewaard gedurende 30 jaar vanaf de datum van verwerking.

De gegevens en informatie uit de in lid 1 bedoelde logbestanden worden bewaard bij de directie die de toegang tot de A.N.G. beheert en binnen elke inlichtingen- en veiligheidsdienst elk voor zover het hem betreft.

De logbestanden van de verwerkingen die door de inlichtingen- en veiligheidsdiensten in de A.N.G. worden uitgevoerd door de directie die de toegang tot de A.N.G. beheert, waarborgt de traceerbaarheid van de raadpleging door de inlichtingen- en veiligheidsdienst in de A.N.G..

Conformément à l'article 47 de la loi du 30 juillet 2018 et à l'article 3 de l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998, les données de journalisation permettant l'identification des agents des services de renseignement et de sécurité qui consultent la B.N.G. ainsi que la motivation de chaque consultation, ne sont enregistrées, conservées et accessibles que dans la journalisation effectuée par le service de renseignement et de sécurité concerné.

La journalisation visée à l'alinéa 3 est uniquement accessible à la personne déléguée par les responsables du traitement de la B.N.G. et au délégué à la protection des données désigné pour la B.N.G., pour remplir une finalité de contrôle et ce, conjointement avec le responsable du traitement des traitements du service de renseignement et le délégué à la protection des données du service de renseignement et de sécurité concerné.

Le traitement des données de la journalisation visée aux alinéas 3 et 4 aux fins de contrôle est détaillé dans le protocole d'accord visé à l'article 2, § 4.

La journalisation et les mesures de sécurité y afférentes visées à l'alinéa 4 sont mises à la disposition du Comité permanent R dans le cadre de ses missions de contrôle.

Art. 7. Pour autant que cela soit utile, les données et informations de la B.N.G., contextualisées dans le cadre des missions des services de renseignement et de sécurité sont enregistrées par le service de renseignement et de sécurité concerné dans la documentation visée à l'article 13 de la loi du 30 novembre 1998.

Préalablement à toute utilisation, les services de renseignement et de sécurité vérifient dans la B.N.G. que ces données et informations enregistrées dans leur documentation respective sont à jour.

Cette documentation fait l'objet de garanties assurant au minimum un niveau de sécurité similaire à celui qui est en vigueur pour la B.N.G.

Art. 8. Sans préjudice des articles 61 et 89 de la loi du 30 juillet 2018, en cas d'incident en matière de sécurité de l'information ou de violation de données à caractère personnel, le service de renseignement et de sécurité concerné prend les mesures nécessaires dans les meilleurs délais afin d'en limiter les conséquences.

En outre, si l'incident présente un risque pour l'exécution des missions légales des services de police ou requiert l'intervention de la direction qui gère les accès à la B.N.G. ou si la violation a un impact sur l'intégrité, la fiabilité ou la disponibilité de la B.N.G., le service de renseignement et de sécurité concerné en informe immédiatement la direction qui gère les accès à la B.N.G. et le délégué à la protection des données désigné pour la B.N.G.

Les modalités de cette communication sont détaillées dans le protocole d'accord visé à l'article 2, § 4.

Art. 9. Le ministre ayant l'Intérieur dans ses attributions, le ministre ayant la Justice dans ses attributions et le ministre ayant la Défense dans ses attributions sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

Donné à Bruxelles,

PHILIPPE

Par le Roi :

Le Ministre de la Justice,
P. VAN TIGCHELT

La Ministre de l'Intérieur,
A. VERLINDEN

La Ministre de la Défense,
L. DEDONDER

Overeenkomstig artikel 47 van de wet van 30 juli 2018 en artikel 3 van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998, worden de logbestanden die de identificatie mogelijk maken van agenten van inlichtingen- en veiligheidsdiensten die de A.N.G. raadplegen alsook de motivering van elke raadpleging, enkel geregistreerd, bewaard en toegankelijk gemaakt in de logbestanden uitgevoerd door de betrokken inlichtingen- en veiligheidsdienst.

De in het derde lid bedoelde logbestanden zijn enkel toegankelijk voor de persoon gedelegeerd door de verwerkingsverantwoordelijken van de A.N.G. en de voor de A.N.G. aangewezen functionaris voor gegevensbescherming om tegemoet te komen aan controledoeleinden, en dit gezamenlijk met de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming van de betrokken inlichtingen- en veiligheidsdienst.

De verwerking van de gegevens van de in het derde en vierde lid bedoelde logbestanden voor controledoeleinden wordt uitvoerig beschreven in het in artikel 2, § 4 bedoelde protocolakkoord.

De logbestanden en de daarmee samenhangende beveiligingsmaatregelen bedoeld in het vierde lid worden ter beschikking gesteld van het Vast Comité I in het kader van zijn toezichthoudende opdrachten.

Art. 7. Voor zover nuttig worden de gegevens en informatie van de A.N.G., die steeds gecontextualiseerd zijn in het kader van de opdrachten van de inlichtingen- en veiligheidsdiensten, geregistreerd door de betrokken inlichtingen- en veiligheidsdienst in de documentatie bedoeld in artikel 13 van de wet van 30 november 1998.

Voorafgaand aan elk gebruik controleren de inlichtingen- en veiligheidsdiensten in de A.N.G. of de gegevens en informatie in hun respectieve documentatie actueel zijn.

Die documentatie moet op zijn minst voorzien zijn van garanties die een veiligheidsniveau waarborgen dat vergelijkbaar is met dat van toepassing op de A.N.G.

Art. 8. Onverminderd de artikelen 61 en 89 van de wet van 30 juli 2018, neemt de betrokken inlichtingen- en veiligheidsdienst bij incidenten op het gebied van informatieveiligheid of inbreuken in verband met persoonsgegevens zo spoedig mogelijk de noodzakelijke maatregelen om de gevolgen ervan te beperken.

Als het incident bovendien een risico inhoudt voor de uitoefening van de wettelijke opdrachten van de politiediensten of een tussenkomst vereist van de directie die de toegangen tot de A.N.G. beheert of indien de inbreuk een impact heeft op de integriteit, de betrouwbaarheid of de beschikbaarheid van de A.N.G., deelt de betrokken inlichtingen- en veiligheidsdienst dit onmiddellijk mee aan de directie die de toegangen tot de A.N.G. beheert en aan de voor de A.N.G. aangewezen functionaris voor gegevensbescherming.

De modaliteiten van deze mededeling worden uitvoerig beschreven in het protocolakkoord bedoeld in artikel 2, § 4.

Art. 9. De minister bevoegd voor Binnenlandse Zaken, de minister bevoegd voor Justitie en de minister bevoegd voor Defensie zijn, ieder wat hem of haar betreft, belast met de uitvoering van dit besluit.

Gegeven te Brussel, 23 november 2023.

FILIP

Van Koningswege :

De Minister van Justitie,
P. VAN TIGCHELT

De Minister van Binnenlandse Zaken
A. VERLINDEN

De Minister van Defensie,
L. DEDONDER

Protocole Réciprocité entre la Sûreté de l'Etat et la Police intégrée dans le cadre de l'accès direct de la Sûreté de l'Etat à la Banque de données Nationale Générale. : principes généraux

Suite à la mise en place d'un accès effectif à la B.N.G. de la Police intégrée pour la VSSE, comme prévu par l'article 14, alinéa 4 de la loi des services de renseignement et de sécurité et l'article 44/11/8*bis* LFP, une réciprocité en termes de communication d'informations doit être octroyée (cf. alinéa 2 de la même disposition LFP) afin d'assurer un équilibre dans la collaboration entre les deux autorités et de faciliter l'échange d'informations et la coordination des enquêtes concernant les entités reprises en BNG. Il s'agira également d'assurer un échange d'expertise respective.

Cela signifie que la VSSE fournit, d'une part, des données à la police de sa propre initiative et, d'autre part, répond aux demandes d'information de la police de la manière la plus appropriée.

[...]

Relation Zones de Police – VSSE :

Dans ce cadre, la VSSE a mis sur pied une section spécialisée pour gérer les relations avec ses partenaires belges. Cette section [...] chargés de veiller à la création et au maintien d'une relation de confiance entre la VSSE et les acteurs locaux tels que les Zones de Police Locale. [...] ils doivent, d'une part, assurer la transmission des informations pertinentes de la VSSE vers ces Zones de Police et, d'autre part, être le relais pour leurs questions et demandes adressées à la VSSE. Il s'agit dès lors d'assurer un flux bidirectionnel des informations qui permettra de faciliter la coordination des enquêtes et assurer que l'information pertinente se trouve au bon endroit.

[...]

Relation Police Fédérale – VSSE :

A l'instar de ce qui est prévu ci-dessus pour les contacts entre les Zones de Police et la VSSE, les relations entre la Police fédérale et la VSSE sont aussi organisées via des points de contact privilégiés permettant d'assurer un flux d'information entre les deux partenaires le plus efficace et cohérent possible.

[...].

Pour la Police intégrée
Eric Snoeck

Pour la Sûreté de l'Etat
Francisca Bostyn

Protocol van wederkerigheid tussen de Staatveiligheid en de geïntegreerde Politie in het kader van de rechtstreekse toegang van de Staatveiligheid tot de Algemene Nationale Gegevensbank: algemene beginselen

Na de instelling van een effectieve toegang tot de A.N.G. van de geïntegreerde politie voor de VSSE, zoals bepaald in artikel 14, lid 4, van de wet op de inlichtingen- en veiligheidsdiensten en artikel 44/11/8 bis van de WPA, moet wederkerigheid op het gebied van de mededeling van informatie worden verleend (zie lid 2 van dezelfde bepaling van de WPA) teneinde te zorgen voor een evenwichtige samenwerking tussen beide overheden en teneinde de uitwisseling van informatie en de coördinatie van onderzoeken betreffende de in het ANG opgenomen entiteiten te vergemakkelijken. Deze uitwisseling zal tevens een uitwisseling van deskundigheid waarborgen.

Dit betekent dat de VSSE enerzijds op eigen initiatief gegevens aan de politie verstrekt en anderzijds op de meest geschikte wijze de verzoeken om informatie van de politie beantwoordt.

[...]

Relatie tussen de politiezones en de VSSE:

In dit kader heeft de VSSE een gespecialiseerde afdeling opgericht om de betrekkingen met haar Belgische partners te beheren. Deze afdeling [...] gelast met het creëren en onderhouden van een vertrouwensrelatie tussen de VSSE en lokale actoren zoals de lokale politiezones. [...] moeten zij enerzijds zorgen voor de overdracht van relevante informatie van de VSSE aan deze politiezones en anderzijds als doorgeefluik fungeren voor hun vragen en verzoeken aan de VSSE. Het doel is dus te zorgen voor een informatiestroom in twee richtingen die de coördinatie van de onderzoeken zal vergemakkelijken en ervoor zal zorgen dat de relevante informatie op de juiste plaats terechtkomt.

[...]

Verhouding Federale Politie - VSSE:

Naar het voorbeeld van wat hierboven is bepaald voor de contacten tussen de politiezones en de VSSE, worden ook de betrekkingen tussen de federale politie en de VSSE georganiseerd via bevoorrechte contactpunten die een zo efficiënt en coherent mogelijke informatiestroom tussen beide partners mogelijk maken.

[...].

Voor de Geïntegreerde Politie
Eric Snoeck

Voor de Veiligheid van de Staat
Francisca Bostyn

SERVICE PUBLIC FEDERAL JUSTICE

[C − 2023/48208]

17 DECEMBRE 2023. — Arrêté royal portant approbation du règlement d'ordre intérieur de l'auditorat établi auprès de la Chambre nationale des huissiers de justice en application de l'article 535 du Code judiciaire

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

Vu l'article 535, alinéa 4, du Code judiciaire, remplacé par la loi du 22 novembre 2022 ;

Sur la proposition du Ministre de la Justice,

Nous avons arrêté et arrêtons :

Article 1er. Le règlement d'ordre intérieur de l'auditorat, adopté par l'assemblée générale de la Chambre nationale des huissiers de justice le 19 septembre 2023 et qui est annexé au présent arrêté, est approuvé.

Art. 2. Le présent arrêté entre en vigueur le 1er janvier 2024.

Art. 3. Le ministre qui a la Justice dans ses attributions est chargé de l'exécution du présent arrêté.

Donné à Bruxelles, le 17 décembre 2023.

PHILIPPE

Par le Roi :

Le Ministre de la Justice,
P. VAN TIGCHELT

FEDERALE OVERHEIDSDIENST JUSTITIE

[C − 2023/48208]

17 DECEMBER 2023. — Koninklijk besluit houdende goedkeuring van het huishoudelijk reglement voor het auditoraat, vastgesteld bij de Nationale Kamer van Gerechtsdeurwaarders, in toepassing van artikel 535 van het Gerechtelijk Wetboek

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op artikel 535, vierde lid van het Gerechtelijk Wetboek, vervangen bij de wet van 22 november 2022;

Op de voordracht van de Minister van Justitie,

Hebben Wij besloten en besluiten Wij :

Artikel 1. Het huishoudelijk reglement voor het auditoraat, aangenomen door de algemene vergadering van de Nationale Kamer van Gerechtsdeurwaarders op 19 september 2023, dat bij dit besluit als bijlage is gevoegd, wordt goedgekeurd.

Art. 2. Dit besluit treedt in werking op 1 januari 2024.

Art. 3. De minister bevoegd voor Justitie is belast met de uitvoering van dit besluit.

Gegeven te Brussel, 17 december 2023.

FILIP

Van Koningswege :

De Minister van Justitie,
P. VAN TIGCHELT