

S'ils postulent pour plusieurs places vacantes différentes, ils doivent envoyer un mail séparé pour chaque candidature. Les candidats recevront un accusé de réception électronique par retour d'e-mail.

Indien zij voor meerdere verschillende vacante plaatsen postuleren, dienen zij voor elke kandidatuurstelling een afzonderlijke e-mail te sturen. De kandidaten krijgen per kerende een elektronische ontvangstmelding.

SERVICE PUBLIC FEDERAL JUSTICE

[C – 2021/41763]

Ordre judiciaire. — Places vacantes

La place néerlandophone suivante de secrétaire (m/f/x) (niveau B) pour l'Ordre judiciaire est déclarée vacante via promotion, il n'y aura pas d'épreuve complémentaire:

Secrétaire gestionnaire de dossiers principalement actif dans les processus primaires au parquet fédéral (néerlandophone): 1

Peuvent postuler aux places mentionnée ci-dessus les titulaires d'une attestation de réussite de la sélection comparative de promotion secrétaires pour le parquet fédéral (m/f/x) (BNG20099), organisée par SELOR pour l'Ordre judiciaire.

Pour les nominations et fonctions au sein de l'ordre judiciaire, les intéressés doivent être d'une conduite répondant aux exigences de la fonction visée et jouir des droits civils et politiques (article 287*quinquies* § 3 du Code judiciaire).

Ces conditions et les conditions de nomination reprises dans le Code judiciaire, doivent être remplies au moment de la clôture du dépôt des candidatures.

Les candidats doivent avoir la nationalité belge au moment de la nomination.

Le classement des candidats à la sélection comparative de promotion sert pour les nominations.

Les candidatures à une nomination dans l'Ordre judiciaire doivent être adressées dans un délai de 20 jours calendrier à partir de la publication de la vacance au *Moniteur belge* (article 287*sexies* du Code judiciaire) et ce via « Mon Selor » (www.selor.be).

La procédure de sélection se déroulera entièrement par voie électronique. Toute candidature incomplète ou qui ne respecte pas la procédure électronique sera déclarée irrecevable.

FEDERALE OVERHEIDS DIENST JUSTITIE

[C – 2021/41763]

Rechterlijke Orde. — Vacante betrekkingen

Volgende Nederlandstalige plaats van secretaris (m/v/x) (niveau B) voor de Rechterlijke orde worden vacant verklaard voor benoeming via bevordering, er wordt geen bijkomende proef georganiseerd :

Secretaris dossierbeheerder hoofdzakelijk ingeschakeld in de primaire processen bij het federaal parket (Nederlandstalig) : 1

Voor bovenvermelde plaatsen kan men zich kandidaat stellen wanneer men in het bezit is van een attest van slagen in de vergelijkende selectie voor bevordering van secretarissen bij het federaal parket (m/v/x) (BNG20099), georganiseerd door SELOR voor de Rechterlijke Orde.

Voor de ambten en de functies binnen de rechterlijke orde, moeten de betrokkenen een gedrag hebben dat in overeenstemming is met de eisen van de beoogde betrekking en de burgerlijke en politieke rechten genieten (art. 287*quinquies* § 3 van het Gerechtelijk Wetboek).

Aan deze vereisten en de benoemingsvooraarden opgenomen in het Gerechtelijk Wetboek, moet worden voldaan op het ogenblik van het afsluiten van de termijn voor kandidatuurstelling.

De kandidaten worden geacht Belg te zijn op het ogenblik van benoeming.

De rangschikking van de kandidaten in de vergelijkende bevorde ringsselectie geldt als volgorde voor benoeming.

De kandidaturen voor een benoeming bij de Rechterlijke Orde dienen gesteld te worden binnen een termijn van 20 kalenderdagen na bekendmaking van de vacature in het *Belgisch Staatsblad* (art.287*sexies* van het gerechtelijk wetboek) via "Mijn Selor" (www.selor.be).

De selectieprocedure wordt volledig elektronisch gevoerd. Elke onvolledige kandidaatstelling of inschrijving die niet verloopt volgens de elektronische inschrijvingsprocedure zal onontvankelijk verklaard worden.

SERVICE PUBLIC FEDERAL JUSTICE

[C – 2021/30853]

D directive commune contraignante des Ministres de la Justice et de l'Intérieur relative aux règles d'accès des membres des services de police à la banque de données nationale générale, aux banques de données de base, particulières et techniques

A Mesdames et Messieurs les Bourgmestres,

Au Commissaire général de la police fédérale.

Pour information à :

Mesdames et Messieurs les Procureurs généraux,

Madame et Messieurs les Gouverneurs de province,

Monsieur le Ministre-Président de la Région de Bruxelles-Capitale,

Monsieur le Procureur fédéral et Mesdames et Messieurs les Magistrats du parquet fédéral,

Mesdames et Messieurs les Commissaires d'arrondissement,

Monsieur le Président de la Commission Permanente de la police locale,

Mesdames et Messieurs les Chefs de corps de la police locale,

Madame et Messieurs les Présidents de l'Organe de contrôle de l'information policière, du Comité permanent de contrôle des services de police et de l'Inspection générale de la police fédérale et de la police locale.

Madame le Bourgmestre,

FEDERALE OVERHEIDS DIENST JUSTITIE

[C – 2021/30853]

Gemeenschappelijke bindende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de toegangsregels van de leden van de politiediensten tot de algemene nationale gegevensbank en de basis-, bijzondere en technische gegevensbanken

Aan de Dames en Heren Burgemeesters,

Aan de Commissaris-generaal van de federale politie.

Ter kennisgeving van:

De Dames en Heren Procureurs-generaal,

Mevrouw en Heren Provinciegouverneurs,

De Heer Minister-President van het Brussels Hoofdstedelijk Gewest,

De Heer Federaal procureur en de Dames en Heren Magistraten van het federaal parket,

Dames en Heren Arrondissementscommissarissen,

De Heer Voorzitter van de Vaste Commissie van de lokale politie,

De Dames en Heren Korpschefs van de lokale politie,

Mevrouw en Heren Voorzitters van het Controleorgaan op de politieke informatie, het Vast Comité van Toezicht op de politiediensten en de Algemene inspectie van de federale politie en van de lokale politie.

Mevrouw de Burgemeester,

Monsieur le Bourgmestre,

Monsieur le Commissaire général,

I. CADRE GENERAL

L'article 44/4, §3 de la loi sur la fonction de police (ci-après « LFP ») constitue la base légale pour la présente directive concernant les règles d'accès des membres des services de police à la Banque de Données Nationale Générale (ci-après « BNG »), aux banques de données de base, particulières et techniques.

Conformément à cet article, les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences et sans préjudice des compétences des autorités judiciaires, déterminent par directive générale et contraignante, publiée au *Moniteur belge*, les règles d'accès des membres des services de police aux banques de données visées à l'article 44/2, §§1^{er} et 3.

Pour ce qui concerne les données de police judiciaire, il y a lieu de se conformer également aux règles des autorités judiciaires et de procédure pénale, en particulier en ce qui concerne le secret de l'information et de l'instruction.

Le 22 mai 2019, la LFP a été modifiée à la lumière des nouvelles dispositions en matière de protection des données. Auparavant, les règles d'accès des membres des services de police ne devaient pas être publiées au *Moniteur belge*. De ce fait, les directives en la matière étaient incluses dans la partie non publiée de la circulaire MFO-3.

L'avis du Conseil des bourgmestres a été donné le 12 août 2020, celui de l'Organe de contrôle de l'information policière le 22 septembre 2020 et celui du Collège des Procureurs Généraux le 04 mars 2021.

II. LES REGLES D'ACCES A LA BNG ET AUX BANQUES DE DONNEES DE BASE, PARTICULIERES ET TECHNIQUES

Les membres des services de police ont un accès à la BNG, aux banques de données de base, particulières et techniques (ci-après « banques de données ») pour accomplir des missions de police administrative et de police judiciaire.

L'accès à ces banques de données et aux données qu'elles contiennent leur est octroyé parce qu'ils ont le besoin d'en connaître.

Pour cette raison, l'accès doit être nécessaire pour exécuter les tâches attribuées.

Les membres des services de police s'identifient et sont authentifiés préalablement à chaque accès aux banques de données et aux données qu'elles contiennent et chaque accès fait l'objet d'une journalisation¹.

Les chefs de corps, pour la police locale, le commissaire général, les directeurs généraux et les directeurs, pour la police fédérale, ci-après « l'autorité », décident pour les membres de leur personnel quels accès sont nécessaires pour exécuter les tâches qu'ils leur confient.

Pour déterminer si l'accès à une banque de données est nécessaire, l'autorité s'appuie sur les finalités définies dans la LFP pour cette catégorie de banque de données².

Si la tâche vise l'une des finalités, c'est que l'accès à la banque de données est nécessaire.

L'autorité sera particulièrement vigilante lorsqu'elle appliquera cette règle pour décider de donner l'accès aux données relatives aux enquêtes et à la gestion de celles-ci. En effet, cet accès se justifie pour les membres des services de police réellement engagés dans ces tâches spécialisées et pour cette raison il fait partie d'un profil spécifique.

Pour déterminer si l'accès à une catégorie de données est nécessaire, l'autorité s'appuie sur les critères suivants :

1) la ou les catégorie(s) de personnes visées à l'article 44/5 de la LFP. Les catégories des témoins et des victimes sont examinées avec la plus grande rigueur.

2) le niveau d'évaluation des données³ sur la base de sa source, de la qualité de la donnée et de l'usage qui peut en être fait;

3) le niveau de validation des données. Les données sont soit validées, soit non validées.

Pour déterminer si l'accès aux données à caractère personnel relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la santé ou à la vie ou l'orientation sexuelle et si le traitement de données génétiques ou biométriques⁴ est justifié pour un membre des services de police, il est en outre vérifié qu'il appartient à l'une des catégories de personnes désignées par le responsable du traitement pour un tel accès ou traitement⁵.

Mijnheer de Burgemeester,

Mijnheer de Commissaris-generaal,

I. ALGEMEEN KADER

Het artikel 44/4, §3 van de wet op het politieambt (hierna "WPA") vormt de wettelijke basis voor de onderhavige richtlijn aangaande de toegangsregels voor de leden van de politiediensten tot de Algemene Nationale Gegevensbank (hierna "ANG"), tot de basis-, bijzondere en technische gegevensbanken.

Conform dit artikel bepalen de ministers van Binnenlandse Zaken en van Justitie, elk binnens hun bevoegdheden en onvermindert de bevoegdheden van de gerechtelijke overheden, bij algemene en bindende richtlijn gepubliceerd in het *Belgisch Staatsblad*, de toegangsregels voor de leden van de politiediensten tot de gegevensbanken bedoeld in artikel 44/2, §§ 1 en 3.

Wat de gegevens van gerechtelijke politie betreft, moeten de regels van de gerechtelijke overheden en strafprocedure ook worden nageleefd, inzonderheid wat betreft het geheim van het opsporings- en het gerechtelijk onderzoek.

Op 22 mei 2019 werd de WPA gewijzigd in het licht van de nieuwe bepalingen inzake gegevensbescherming. Voordien dienden de toegangsregels van de leden van de politiediensten niet gepubliceerd te worden in het *Belgisch Staatsblad*. De richtlijnen ter zake werden aldus opgenomen in het niet gepubliceerde deel van de omzendbrief MFO-3.

Het advies van de raad van burgemeesters werd op 12 augustus 2020 uitgebracht, dat van het Controleorgaan op de politieën informatie op 22 september 2020 en dat van het College van procureurs-generaal op 04 maart 2021.

II. DE TOEGANGSREGELS TOT DE ANG EN DE BASIS-, BIJZONDERE EN TECHNISCHE GEGEVENSBANKEN.

De leden van de politiediensten hebben toegang tot de ANG, de basis-, bijzondere en technische gegevensbanken (hierna "gegevensbanken") om opdrachten van bestuurlijke en gerechtelijke politie te vervullen.

De toegang tot deze gegevensbanken en tot de gegevens die zij bevatten wordt hun verleend omdat zij de nood hebben om er kennis van te nemen.

Om deze reden moet de toegang noodzakelijk zijn om de toegekende taken uit te voeren.

De leden van de politiediensten worden voorafgaandelijk elke toegang tot de gegevensbanken en de gegevens die ze bevatten geïdentificeerd en gauthentiseerd en elke toegang wordt gelogd¹.

De korpschef, voor de lokale politie, de commissaris-generaal, de directeurs-generaal en directeurs, voor de federale politie, hierna "de overheid", beslissen voor de leden van hun personeel welke toegang noodzakelijk is om de hun toevertrouwde taken uit te voeren.

Om te bepalen of een toegang tot een gegevensbank noodzakelijk is, steunt de overheid zich op de doeleinden bepaald in de WPA voor deze categorie van gegevensbank².

Als de taak één van de doeleinden beoogt, dan is de toegang tot de gegevensbank noodzakelijk.

De overheid zal bijzonder waakzaam zijn bij de toepassing van deze regel wanneer zij besluit toegang te verlenen tot gegevens in verband met onderzoeken en het beheer daarvan. Deze toegang is immers gerechtvaardigd voor leden van de politiediensten die zich daadwerkelijk met deze gespecialiseerde taken bezighouden en maakt om die reden deel uit van een specifiek profiel.

Om te bepalen of een toegang tot een categorie van gegevens noodzakelijk is, steunt de overheid zich op de volgende criteria:

1) de categorie(en) van personen bedoeld in artikel 44/5 van de WPA. De categorieën van getuigen en slachtoffers worden met grote omzichtigheid onderzocht.

2) het evaluatienniveau van de gegevens³ op basis van hun bron, van de kwaliteit van het gegeven en het gebruik dat ervan kan worden gemaakt;

4) het validatienniveau van de gegevens. De gegevens zijn ofwel gevalideerd, ofwel niet gevalideerd.

Om te bepalen of een toegang tot persoonsgegevens betreffende de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakvereniging, de gezondheid, seksueel gedrag of seksuele gerichtheid en indien de verwerking van genetische of biometrische gegevens⁴ gerechtvaardigd is voor een lid van de politiediensten, moet bovendien worden nagegaan dat deze behoort tot de categorieën van personen aangesteld door de verwerkingsverantwoordelijke voor een dergelijke toegang of verwerking⁵.

Pour déterminer le droit d'accès nécessaire, l'autorité considère le traitement de données à réaliser : une consultation (lecture) simple ou sur la base de paramètres, un enregistrement (écriture), un transfert, une validation, une modification, un archivage, un effacement ou tout autre traitement de données.

Afin de permettre une prise de décision en connaissance de cause, des directives internes à la police intégrée contiennent, pour les banques de données et les applications techniques, les informations suivantes :

- 1) les finalités;
- 2) les catégories de personnes visées à l'article 44/5 de la LFP;
- 3) le niveau d'évaluation des données;
- 4) le niveau de validation des données;
- 5) le profil requis pour y accéder;
- 6) les droits d'accès et ce qu'ils permettent.

Ces directives sont tenues à la disposition de l'Organe de contrôle de l'information policière.

L'application de ces règles vise à individualiser les accès des membres des services de police.

L'autorité décide pour les membres de son personnel pour quelle durée l'accès est accordé. Une tâche temporaire ne nécessite pas un accès permanent. Par exemple, en cas de détachement ou de réaffectation dans une autre zone de police, l'accès à l'ISLP de la zone est accordé pendant la durée du détachement ou de la réaffectation. En revanche un accès à la BNG peut être permanent et rester actif aussi longtemps que le membre des services de police est engagé dans des missions de police judiciaire ou de police administrative dans la mesure où la BNG est la banque de données dont l'ensemble des services de police ont besoin pour exercer leurs missions.

L'autorité s'assure que les membres de son personnel ont les connaissances requises pour accéder aux banques de données et aux données qu'elles contiennent ainsi que pour effectuer les activités de traitement prévues pour le droit d'accès octroyé.

L'autorité dispose d'une politique d'accès traduisant les règles en fonction de la situation locale dont elle est responsable. Pour l'accès aux banques de données particulières et techniques locales, le responsable du traitement peut déroger à certaines règles de la présente pour autant que l'objectif à atteindre par la règle ne soit pas ou très peu impacté. Il s'agit par conséquent de poursuivre le même objectif mais en utilisant d'autres moyens. Dans ce cas, il faut être en mesure d'en motiver la raison et de la conserver afin de pouvoir expliquer son approche en cas de contrôle par les services compétents. Il s'agit en premier lieu de l'Organe de contrôle de l'information policière.

Les accès des membres des services à la BNG, aux banques de données de base, particulières et techniques sont donc encadrés par la présente directive, par des directives internes à la police intégrée et par la politique d'accès de l'autorité. Chaque niveau est ainsi impliqué et prend les responsabilités qui lui incombent pour permettre la bonne application des règles d'accès et la bonne gestion de ceux-ci.

III. LA GESTION DES ACCES

Les règles sont mises en œuvre dans le cadre d'une gestion globale des accès avec des procédures et des systèmes de gestion des accès.

Les procédures de demande et d'autorisation d'accès font l'objet de directives internes à la police intégrée. Celles-ci sont tenues à la disposition de l'Organe de contrôle de l'information policière.

Sauf dérogation dûment justifiée, la gestion des accès est supportée par un système de permissions basé sur des rôles. C'est le registre central des profils et des accès.

Pour les banques de données particulières et techniques locales, le registre est organisé localement par le responsable du traitement et respecte les mêmes règles.

Le registre a pour objectif de :

- 1) contenir les décisions portant sur les accès et les profils des membres des services de police;
- 2) connaître en permanence les accès et profils qui leur sont individuellement octroyés;
- 3) rendre compte globalement ou individuellement sur les accès et les profils. Il s'agit notamment de tenir à la disposition de l'Organe de contrôle de l'information policière les profils d'accès et l'identification des personnes ayant accès.

L'enregistrement des décisions, des accès et des profils et leur mise à jour dans le registre central se fait localement au niveau le plus proche de la décision. L'autorité peut décider de déléguer cette tâche.

Om het recht tot noodzakelijke toegang te bepalen, neemt de overheid de te bereiken verwerking van gegevens in beschouwing: eenvoudige raadpleging of raadpleging op grond van parameters (lezen), registratie (schrijven), overdracht, validatie, wijziging, archivering, uitwisseling of enige andere verwerking van gegevens.

Om een besluitvorming met kennis van zaken mogelijk te maken, bevatten de interne richtlijnen voor de geïntegreerde politie de volgende informatie over gegevensbanken en technische toepassingen:

- 1) de doeleinden;
- 2) de categorieën van personen bedoeld in artikel 44/5 van de WPA;
- 3) het evaluatieniveau van de gegevens;
- 4) het validatieniveau van de gegevens;
- 5) het vereiste profiel om er toegang toe te krijgen;
- 6) het toegangsrechten en wat zij toelaten.

Deze richtlijnen worden ter beschikking gesteld van het Controleorgaan op de politieke informatie.

De toepassing van deze regels is bedoeld om de toegang voor leden van de politiediensten te individualiseren.

De overheid beslist voor de leden van haar personeel voor welke duur de toegang wordt verleend. Voor een tijdelijke taak is geen permanente toegang vereist. Bijvoorbeeld in geval van detaching of herplaatsing in een andere politiezone, dan zal de toegang tot ISLP van deze zone toegekend worden voor de duur van deze detaching of herplaatsing. Anderzijds kan de toegang tot de ANG permanent zijn en actief blijven zolang het personeelslid van de politiedienst gerechtelijke of bestuurlijke politieopdrachten uitvoert, voor zover de ANG de gegevensbank is die alle politiediensten nodig hebben om hun opdrachten uit te voeren.

De overheid zorgt ervoor dat haar personeelsleden over de nodige kennis beschikken om toegang te krijgen tot de gegevensbanken en de gegevens die deze bevatten evenals om de verwerkingsactiviteiten uit te voeren die zijn voorzien voor het verleende toegangsrecht.

De overheid beschikt over een toegangsbeleid dat de voorgeschreven regels weerspiegelt in overeenstemming met haar lokale situatie waarvoor zij verantwoordelijk is. Voor de toegang tot de bijzondere en de lokale technische gegevensbanken kan de verwerkingsverantwoordelijke van sommige van deze regels afwijken in zoverre dat het geen of zeer weinig invloed heeft op het te bereiken doel. Het gaat er bijgevolg om hetzelfde doel na te streven, maar door gebruik van andere middelen. In dit geval is het noodzakelijk om de reden hiervoor te kunnen verantwoorden en deze bij te houden teneinde hun aanpak te lichten in geval van een controle door de bevoegde diensten. Dit is in de eerste plaats het Controleorgaan op de politieke informatie.

De toegang van de leden van de diensten tot de ANG, tot de basisgegevensbanken, bijzondere gegevensbanken en technische gegevensbanken wordt dus geregeld door de onderhavige richtlijn, door interne richtlijnen van de geïntegreerde politie en door het toegangsbeleid van de overheid. Elk niveau is dus betrokken en neemt de verantwoordelijkheden op zich die nodig zijn om te zorgen voor de juiste toepassing van de toegangsregels en het goede beheer daarvan.

III. HET BEHEER VAN DE TOEGANGEN

De regels worden ingevoerd in het raam van een algemeen toegangsbeheer met procedures en systemen voor het beheer van de toegangen.

De procedures voor het aanvragen en verlenen van toegang maken het voorwerp uit van interne richtlijnen binnen de geïntegreerde politie. Deze worden ter beschikking gesteld van het Controleorgaan op de politieke informatie.

Tenzij naar behoren gemotiveerde uitzonderingen, wordt het toegangsbeheer ondersteund door een op rollen gebaseerd rechstensysteem. Dit is het centrale register van profielen in toegangen.

Voor de bijzondere en de lokale technische gegevensbanken wordt het register lokaal georganiseerd door de verwerkingsverantwoordelijke en volgt deze dezelfde regels.

Het doel van het register is om:

- 1) beslissingen te bevatten betreffende de toegang en de profielen van de leden van de politiediensten;
- 2) een permanent oog te hebben op de toegangen en profielen die individueel werden toegekend;
- 3) rekenschap af te leggen, globaal of individueel, aangaande de toegangen en de profielen. Met name om toegangsprofielen en de identificatie van personen met toegang ter beschikking te stellen van het Controleorgaan op de politieke informatie.

De registratie van beslissingen, de toegang en de profielen en hun actualisatie in het centrale register gebeurt lokaal op het niveau dat het dichtst bij de beslissing ligt. De overheid kan beslissen deze taak te delegeren.

Exceptionnellement, la direction qui gère et développe la BNG procède à l'enregistrement, par exemple, en raison de la sensibilité⁶ particulière des données ou lorsqu'il s'agit de donner un profil déterminé.

Les données à caractère personnel relatives aux membres des services de police sont automatiquement mises à jour dans le registre par la connexion avec la source authentique pour la gestion du personnel de la police intégrée. La mise à jour garantit notamment que les membres du personnel partis à la retraite n'aient plus d'accès aux banques de données.

La gestion des accès est un processus dynamique avec des mises à jour régulières de sorte que seuls les accès nécessaires soient actifs. Nous chargeons en plus chaque autorité de vérifier au moins une fois par an que les données du registre sont toujours à jour. Les accès doivent en effet rester nécessaires et autorisés. Les contrôles et mises à jour sont importants, par exemple, parce que les tâches d'un membre des services de police ont changé.

IV. LES PROFILS

Pour des raisons techniques et logiques liées aux processus de travail, des profils sont créés. Ils rendent uniforme la correspondance entre des tâches et les accès nécessaires pour les exécuter.

Un profil est conforme à la loi s'il peut être démontré que, lors de sa détermination, il a été tenu compte des règles d'accès développées au point II.

L'autorité décide pour les membres de son personnel quel profil est nécessaire pour exécuter les tâches qu'elle leur confie.

De ce fait, elle donne l'autorisation de l'accès.

Comme les profils peuvent évoluer en fonction du travail policier et de la technologie, ils sont déterminés dans des directives internes à la police intégrée. Celles-ci sont tenues à la disposition de l'Organe de Contrôle de l'information policière.

V. L'IDENTIFICATION, L'AUTHENTIFICATION ET LA JOURNALISATION (LOGGING)

La règle d'identification et d'authentification vaut pour chaque accès aux banques de données et aux données qu'elles contiennent.

L'identification vérifie techniquement que celui qui se connecte afin d'accéder aux banques de données est bien un membre des services de police et que son autorité hiérarchique a autorisé cet accès.

La garantie que l'on est un membre des services de police est donnée en consultant la source authentique pour la gestion du personnel de la police intégrée.

L'authentification garantit techniquement que le membre des services de police qui s'est identifié et dispose de l'accès requis est bien le membre du personnel réellement concerné.

L'authentification multifacteur⁷ est la norme pour les solutions informatiques déployées postérieurement à la présente directive.

L'identifiant et le moyen d'authentification sont strictement personnels.

L'accès aux banques de données et le traitement de données qu'elles contiennent font l'objet d'une journalisation (logging) qui établit, a posteriori, qui a eu accès et a fait quel traitement, de quelle donnée, quand et, formulé de façon compréhensible, pourquoi.

Une consultation irrégulière peut constituer une infraction pénale, entraînant la rédaction d'un procès-verbal et est donc également susceptible de constituer une transgression disciplinaire.

Lorsque le traitement est une communication de données, la journalisation établit aussi les systèmes qui les ont communiquées, les catégories de destinataires des données à caractère personnel, et, si possible, l'identité des destinataires de ces données.

Sauf dérogation dûment justifiée, la journalisation est supportée par un système appelé « registre central des loggings ».

Pour les banques de données particulières et techniques locales, le registre est organisé localement par le responsable du traitement et respecte les mêmes règles.

Les données de journalisation sont conservées dans le registre pendant :

- 1) 30 ans à partir du traitement dans la BNG;
- 2) 15 ans à partir du traitement dans les banques de données de base;
- 3) 10 ans, au minimum, à partir du traitement dans les banques de données particulières. Le responsable du traitement peut décider de prolonger ce délai de maximum 20 ans en motivant sa décision.
- 4) 10 ans à partir du traitement dans les banques de données techniques.

Bij wijze van uitzondering, voert de directie die de ANG beheert en ontwikkelt de registratie uit, bijvoorbeeld, wegens de bijzondere gevoeligheid⁶ van de gegevens of wanneer het om een bepaald profiel gaat.

De persoonsgegevens van de leden van de politiediensten worden automatisch bijgewerkt in het register door verbinding te maken met de authentieke bron voor het personeelsbeheer van de geïntegreerde politie. De bijwerking zorgt er met name voor dat personeelsleden die met pensioen zijn gegaan geen toegang meer hebben tot de gegevensbanken.

Toegangsbeheer is een dynamisch proces met regelmatige updates, zodat alleen de noodzakelijke toegangen actief zijn. Bovendien dragen wij elke autoriteit op ten minste eenmaal per jaar na te gaan of de gegevens in het register nog actueel zijn. De toegangen moeten noodzakelijk en geautoriseerd blijven. Controles en bijwerkingen zijn belangrijk, bijvoorbeeld omdat de taken van een lid van de politiediensten zijn veranderd.

IV. DE PROFIELEN

Om technische en logische redenen gebonden aan de werkprocessen worden er profielen aangemaakt. Ze uniformiseren de overeenstemming tussen de taken en de noodzakelijke toegangen.

Een profiel is in overeenstemming met de wet als kan worden aangetoond dat bij de bepaling ervan rekening werd gehouden met de in punt II ontwikkelde toegangsregels.

De overheid beslist voor haar personeelsleden welk profiel noodzakelijk is om de taken die ze aan hen toevertrouwt uit te voeren.

Hierdoor geeft ze de toestemming voor de toegang.

Omdat de profielen kunnen evolueren in functie van het politieën werk, zijn ze in interne richtlijnen van de geïntegreerde politie bepaald. Deze richtlijnen worden ter beschikking gesteld van het Controleorgaan op de Politieën Informatie.

V. IDENTIFICATIE, AUTHENTICATIE EN LOGBESTANDEN (LOGGING)

De identificatie- en authenticatieregel is van toepassing op elke toegang tot de gegevensbanken en de gegevens die ze bevatten.

Met de identificatie wordt technisch nagegaan of de persoon die verbinding maakt om toegang tot de gegevensbanken te hebben, effectief lid is van de politiediensten en of zijn of haar hiërarchische overheid deze toegang heeft goedgekeurd.

De garantie dat men een personeelslid van de politiediensten is, wordt gegeven door het raadplegen van de authentieke bron voor het personeelsbeheer van de geïntegreerde politie.

Authenticatie garandeert technisch gezien dat het lid van de politiediensten die zich heeft geïdentificeerd en de vereiste toegang heeft, wel degelijk het juiste lid is.

De multifactor⁷ authenticatie is de standaard voor IT-oplossingen die na deze richtlijn worden geïmplementeerd.

De identificatiecode en de wijze van authenticatie zijn strikt persoonlijk.

De toegang tot de gegevensbanken en de verwerking van de gegevens die daarin zijn opgenomen, maken het voorwerp uit van een logbestand (logging), waarbij a posteriori wordt vastgesteld wie toegang heeft gehad en welke verwerking heeft uitgevoerd, van welke gegevens, wanneer en, begrijpelijk geformuleerd, waarom.

Een onregelmatige raadpleging kan een strafbaar feit vormen, dat leidt tot de opstelling van een proces-verbaal, en kan dus ook een tuchtrechtelijke overtreding inhouden.

Wanneer de verwerking een mededeling van gegevens is, worden in het logbestand ook de systemen vastgesteld die de gegevens hebben meegedeeld, de categorieën ontvangers van de persoonsgegevens en, indien mogelijk, de identiteit van de ontvangers van deze gegevens.

Tenzij er een naar behoren gerechtvaardigde afwijking wordt gemaakt, wordt het logbestand ondersteund door een systeem dat "het centraal register van de logbestanden" wordt genoemd.

Voor de bijzondere en lokale technische gegevensbanken wordt het register lokaal georganiseerd door de verwerkingsverantwoordelijke en volgt dezelfde regels.

De logbestanden worden in het register bewaard voor een periode van:

- 1) 30 jaar na verwerking in de ANG;
- 2) 15 jaar na verwerking in de basisgegevensbanken;
- 3) ten minste 10 jaar na verwerking in de bijzondere gegevensbanken. De verwerkingsverantwoordelijke kan besluiten deze periode te verlengen tot maximaal 20 jaar, mits motivatie van deze beslissing.
- 4) 10 jaar na verwerking in de technische gegevensbanken.

La journalisation est utilisée uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle par les services de police, de garantie de l'intégrité et de la sécurité des données à caractère personnel, à des fins de procédures pénales et à des fins de surveillance par l'Organe de contrôle de l'information policière ou par d'autres instances de contrôle.

L'accès au registre des loggings est réglé par des procédures internes garantissant la nécessité, la proportionnalité et la sécurité de l'accès. Celles-ci sont soumises à l'avis de l'Organe de contrôle de l'information policière.

Les procédures de demande de données de la journalisation et le traitement des demandes font l'objet de directives internes à la police intégrée. Celles-ci sont tenues à la disposition de l'Organe de contrôle de l'information policière.

Notes

¹ Le point V définit ces notions et leurs objectifs.

² Pour la BNG à l'article 44/7; les banques de données de base à l'article 44/11/2 §1er; les banques de données particulières à l'article 44/11/3 §2; les banques de données techniques à l'article 44/11/3 septies.

³ Les niveaux d'évaluation des données sont déterminés dans des directives non publiées.

⁴ Il s'agit des catégories particulières de données à caractère personnel visées à l'article 34 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

⁵ Il s'agit de l'application de l'article 44/1 §2, alinéa 3 de la loi sur la fonction de police.

⁶ La sensibilité pourrait par exemple concerner des données biométriques ou encore des données relatives à la santé.

⁷ Authentification basée sur plusieurs facteurs ou « Multi-Factor Authentication » (M.F.A.) repose sur au moins deux des trois éléments suivants : un élément "connaissance" (quelque chose que seul l'utilisateur connaît), un élément "possession" (quelque chose que seul le signataire possède) et un élément "inhérence" (quelque chose que l'utilisateur est)

De logbestanden worden alleen gebruikt om de rechtmatigheid van de verwerking te controleren, voor zelfcontrole door de politiediensten, om de integriteit en de veiligheid van de persoonsgegevens te waarborgen en in het raam van strafrechtelijke procedures en voor toezichtdoeleinden door het Controleorgaan op de politieke informatie of andere toezichthoudende instanties.

De toegang tot de logbestanden wordt geregeld door middel van interne procedures die de noodzaak, de evenredigheid en de veiligheid van de toegang waarborgen. Deze zijn onderworpen aan het advies van het Controleorgaan op de Politieke Informatie.

De procedures voor het opvragen van logbestanden en de verwerking van verzoeken maken het voorwerp uit van interne richtlijnen van de geïntegreerde politie. Deze worden ter beschikking gesteld van het Controleorgaan op de Politieke Informatie.

Nota's

¹ Punt V definieert deze begrippen en hun doelstellingen.

² Voor de ANG op artikel 44/7; de basisgegevensbanken op artikel 44/11/2 §1er; de bijzondere gegevensbanken op artikel 44/11/3 §2; de technische gegevensbanken op artikel 44/11/3 septies.

³ De evaluatieniveaus van gegevens worden bepaald in niet gepubliceerde richtlijnen.

⁴ Het gaat over de bijzondere categorieën van personen bedoeld in artikel 34 van de wet dd 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

⁵ Het gaat over de toepassing van artikel 44/1 §2, lid 3 van de wet op het politieambt.

⁶ De gevoeligheid zou bij voorbeeld de biometrische gegevens of nog de gegevens in verband met de gezondheid kunnen betreffen.

⁷ Authenticatie gebaseerd op verschillende factoren of "Multi-Factor Authentication" (M.F.A.) is gebaseerd op ten minste twee van de volgende drie elementen: een element "kennis" (iets dat alleen de gebruiker weet), een element "bezit" (iets dat alleen de ondertekenaar heeft) en een element "hoedanigheid" (iets dat de gebruiker is)

SERVICE PUBLIC FEDERAL JUSTICE

[C – 2021/30854]

D directive contraignante commune des Ministres de la Justice et de l'Intérieur relative aux mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2 de la Loi sur la Fonction de Police

A Mesdames et Messieurs les Bourgmestres,

Au Commissaire général de la police fédérale.

Pour information à :

Mesdames et Messieurs les Procureurs généraux,

Madame et Messieurs les Gouverneurs de province,

Monsieur le Ministre-Président de la Région de Bruxelles-Capitale,

Monsieur le Procureur fédéral et Mesdames et Messieurs les Magistrats du parquet fédéral,

Mesdames et Messieurs les Commissaires d'arrondissement,

Monsieur le Président de la Commission Permanente de la police locale,

Mesdames et Messieurs les Chefs de corps de la police locale,

Madame et Messieurs les Présidents de l'Organe de contrôle de l'information policière, du Comité permanent de contrôle des services de police et de l'Inspection générale de la police fédérale et de la police locale.

Madame le Bourgmestre,

FEDERALE OVERHEIDS DIENST JUSTITIE

[C – 2021/30854]

Gemeenschappelijke dwingende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de maatregelen die nodig zijn om het beheer en de veiligheid, waaronder in het bijzonder de aspecten met betrekking tot de betrouwbaarheid, de vertrouwelijkheid, de beschikbaarheid, de traceerbaarheid en de integriteit van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2 van de Wet op het Politieambt, te verzekeren

Aan de Dames en Heren Burgemeesters,

Aan de Commissaris-generaal van de federale politie.

Ter kennisgeving van:

De Dames en Heren Procureurs-generaal,

Mevrouw en Heren Provinciegouverneurs,

De Heer Minister-President van het Brussels Hoofdstedelijk Gewest,

De Heer Federaal procureur en de Dames en Heren Magistraten van het federaal parket,

De Dames en Heren Arrondissementscommissarissen,

De Heer Voorzitter van de Vaste Commissie van de lokale politie,

De Dames en Heren Korpschefs van de lokale politie,

Mevrouw en Heren Voorzitters van het Controleorgaan op de politieke informatie, het Vast Comité van Toezicht op de politiediensten en de algemene inspectie van de federale politie en van de lokale politie.

Mevrouw de Burgemeester,