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 politionele 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 Politionele 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 Politionele 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]

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 OVERHEIDSDIENST 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 politionele 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 LEGAL ET CHAMP D'APPLICATION

L'article 44/4, §2 de la loi sur la fonction de police (ci-après « LFP ») constitue la base légale pour la présente directive contraignante, portant sur les 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 la banque de données nationale générale, les banques de données de base, les banques de données particulières, les banques de données communes et les banques de données techniques visées à l'article 44/2 de la LFP.

Bien que la présente directive traite en principe du contexte nécessaire pour la sécurité des systèmes opérationnels, cela n'exclut pas que, en complément de la LFP et du titre 2 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (ci-après « la loi sur la protection des données » ou « LPD »), également le Règlement Général sur la Protection des Données[1] et le titre 1 de la LPD s'appliquent à certaines mesures prises en vertu de la présente directive.

La présente directive est applicable aux services de police au sens de l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré structuré à deux niveaux.

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 7 janvier 2021.

II. INTRODUCTION

Pour exécuter leurs missions, les services de police utilisent de plus en plus les nouvelles technologies d'information et de communication.

Dans une société où une attention croissante est accordée à la sécurité des informations et à la protection des données à caractère personnel, les risques inévitablement liés aux traitements de ces informations et données par les services de police doivent être correctement encadrés et couverts en adoptant les mesures techniques et organisationnelles nécessaires.

La LFP prévoit que les ministres de la Justice et de l'Intérieur adoptent par le biais d'une directive contraignante les mesures nécessaires à cette fin. Pour déterminer ces mesures, nous nous sommes inspirés des « Baseline Information Security Guidelines » (BSG) du Centre pour la Cybersécurité Belgique. Nous souhaitons que ces lignes directrices constituent le cadre de référence pour la politique de sécurité de l'information et les plans de sécurité des services de police.

Les mesures contenues dans la présente directive visent à permettre aux services de police, qui ont des niveaux de maturité différents en matière de sécurité de l'information, d'augmenter leur niveau au fur et à mesure en utilisant la méthode éprouvée du PDCA (Plan-Do-Check-Act) et de renforcer la gestion des risques qui y est associée, d'assurer la continuité des activités policières, de prévenir la fuite d'informations, d'assurer la sécurité de son personnel et des citoyens et de renforcer ainsi la confiance de la société à leur égard.

Cette progressivité permet également de maintenir la continuité des activités policières opérationnelles tenant compte des moyens disponibles.

La présente directive définit les mesures minimales que les services de police doivent respecter lors de l'élaboration, l'implémentation et l'évaluation de la politique de sécurité de l'information, ainsi que les plans de sécurité et les procédures et processus qui concrétiseront la présente directive.

La mise en œuvre progressive de la présente directive, ainsi que la définition des priorités, seront reprises dans la politique de sécurité de l'information, dans les plans de sécurité (voir ci-dessous), dans des notes internes à la police intégrée et/ou moyennant une mise à jour des fiches de la directive du 14 juin 2002 des Ministres de la Justice et de l'Intérieur (MFO-3) relative à la gestion de l'information de police judiciaire et de police administrative, lesquelles sont destinées aux services opérationnels.

Les chefs de corps pour la police locale et le commissaire général, les directeurs généraux et les directeurs pour la police fédérale sont les garants de la bonne exécution de ces directives en ce qui concerne les banques de données visées à l'article 44/2, §§ 1er et 3 LFP. Le cas échéant, une concertation entre les acteurs compétents en particulier le commissaire général, les directeurs généraux, les directeurs, les chefs de corps, le gestionnaire fonctionnel et le délégué à la protection des données compétent est fortement recommandée.

Mijnheer de Burgemeester,

Mijnheer de Commissaris-generaal,

I. WETTELIJK KADER EN TOEPASSINGSGEBIED

Het artikel 44/4 §2 van de wet op het politieambt (hierna "WPA") vormt de wettelijke basis voor de onderhavige dwingende richtlijn die betrekking heeft op 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 Algemene Nationale Gegevensbank, in de basisgegevensbanken, in de bijzondere gegevensbanken, in de gemeenschappelijke gegevensbanken en in de technische gegevensbanken, bedoeld in artikel 44/2 van de WPA, te verzekeren.

Hoewel de onderhavige richtlijn in principe handelt over de noodzakelijke context voor de beveiliging van de operationele systemen, sluit dit evenwel niet uit dat, naast de WPA en titel 2 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna "gegevensbeschermingswet" of "GBW" genoemd), ook de Algemene Verordening Gegevensbescherming[1] en titel 1 van de GBW van toepassing zijn op bepaalde maatregelen die genomen worden in uitwerking van de onderhavige richtlijn.

Onderhavige richtlijn is van toepassing op de politiediensten, zoals bedoeld in artikel 2, 2° van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.

Het advies van de Raad van burgemeesters werd op 12 augustus 2020 uitgebracht, dat van het Controleorgaan op de politionele informatie op 22 september 2020 en dat van het College van procureursgeneraal op 7 januari 2021.

II. INLEIDING

Bij de uitvoering van hun opdrachten maken de politiediensten steeds vaker gebruik van nieuwe informatie- en communicatietechnologieën.

In een maatschappij waar er steeds meer aandacht is voor de veiligheid van informatie en de bescherming van persoonsgegevens, dienen de risico's die onvermijdelijk verbonden zijn aan een dergelijke informatie- en gegevensverwerking door de politiediensten goed te worden omkaderd en afgedekt door het nemen van de nodige technische en organisatorische maatregelen.

De WPA voorziet dat de ministers van Justitie en Binnenlandse Zaken hiervoor de nodige maatregelen bij dwingende richtlijn bepalen. Bij het bepalen van de onderhavige maatregelen hebben de ministers zich geïnspireerd op de "Baseline Information Security Guidelines" (BSG) van het Centrum voor Cyber Security Belgium. Het is de wens van de ministers dat deze Guidelines het referentiekader vormen voor het informatieveiligheidsbeleid en beveiligingsplannen van de politiediensten.

De maatregelen vervat in de onderhavige richtlijn dienen de politiediensten, die over verschillende maturiteitsniveaus beschikken inzake informatieveiligheid, onder meer in staat te stellen hun maturiteitsniveau stapsgewijs te verhogen aan de hand van de beproefde PDCA-methode (Plan-Do-Check-Act) en het hiermee gepaard gaande risicobeheer te versterken, de continuïteit van de politieactiviteiten te verzekeren, het lekken van informatie te voorkomen, de veiligheid van haar personeel en de burgers te verzekeren en zo het vertrouwen van de maatschappij ten opzichte van hen te versterken.

Deze progressiviteit beoogt ook de continuïteit van de operationele politieactiviteiten rekening houdend met de beschikbare middelen.

De onderhavige richtlijn bepaalt de minimale maatregelen waar de politiediensten rekening mee dienen te houden bij het opstellen, het implementeren en het evalueren van het informatieveiligheidsbeleid, evenals de beveiligingsplannen en de procedures en processen die de onderhavige richtlijn zullen concretiseren.

De progressieve implementatie van de onderhavige richtlijn evenals de bepaling van de prioriteiten, zullen worden hernomen in het informatieveiligheidsbeleid, de beveiligingsplannen (zie onder), in interne nota's van de geïntegreerde politie en/of middels een bijwerking van de fiches van de richtlijn van 14 juni 2002 van de Ministers van Justitie en van Binnenlandse Zaken (MFO-3) betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie, die bestemd zijn voor de operationele diensten.

De korpschefs voor de lokale politie en de commissaris-generaal, de directeurs-generaal en de directeurs voor de federale politie staan borg voor de goede uitvoering van deze richtlijnen voor wat de gegevensbanken bedoeld in artikel 44/2, §§ 1 en 3 WPA, betreft. In voorkomend geval, wordt een overleg tussen de bevoegde actoren, in het bijzonder de commissaris-generaal, de directeurs-generaal, de directeurs, de korpschefs, de functioneel beheerder en de bevoegde functionaris voor de gegevensbescherming sterk aanbevolen.

III. LES MESURES MINIMALES DE PROTECTION

1) La politique de sécurité de l'information et les plans de sécurité

Les services de police doivent disposer d'une politique actualisée et uniforme en matière de sécurité de l'information, ci-après « la politique de sécurité de l'information », validée par le « comité de coordination de la police intégrée »[2] (ci-après le CCGPI) après avis du « comité information et ICT »[3].

En tenant compte de la politique de sécurité de l'information, des plans de sécurité sont ensuite établis, qui contiennent les mesures techniques et organisationnelles de sécurité de l'information à mettre en œuvre. Ces plans de sécurité, ainsi que les procédures et processus qui concrétiseront la présente directive, sont validés par la hiérarchie compétente, à savoir le Comité de direction pour la police fédérale et le Chef de Corps pour les zones de police, après avis du délégué à la protection des données compétent.

La politique de sécurité de l'information et les plans de sécurité, ainsi que les procédures et les processus qui concrétiseront la présente directive, doivent être évalués régulièrement.

Conformément à l'article 244 LPD, les services de police transmettent à l'Organe de contrôle de l'information policière (ci-après le « COC ») la politique en matière de sécurité de l'information ainsi que les plans de sécurité.

2) Organisation de la sécurité de l'information

Les services de police prévoient un système de gestion des risques en matière de sécurité de l'information et identifient les rôles et responsabilités des différents acteurs concernés par la sécurité de l'information.

Le délégué à la protection des données compétent est également chargé du suivi de la politique de sécurité des informations et de l'implémentation du(des) plan(s) de sécurité.

Afin de s'assurer que toutes les mesures organisationnelles soient appliquées, les services de police informent leur personnel et les tiers opérant sous leur responsabilité. La politique de sécurité et les plans de sécurité devront être disponibles et consultables par les personnes devant les appliquer. L'accès à toute l'information n'est néanmoins pas nécessaire pour atteindre cet objectif.

Les services de police développent, approuvent et communiquent des procédures et des bonnes pratiques pour la sécurité de l'information qui concrétiseront la présente directive.

Des procédures sont établies pour chaque utilisateur et en particulier pour ceux qui ont accès à des données avec une sensibilité particulière ou à des systèmes critiques.

Ces procédures portent sur les thèmes suivants :

- le contrôle d'accès / la gestion des autorisations ;

- le retrait des droits ;

- la confidentialité des données ;

- l'accès physique aux bâtiments et aux infrastructures ;

- les systèmes d'accès et la confidentialité des données d'accès ;

- les mesures permettant de déterminer l'utilisation correcte des outils de travail mis à disposition (tels que les appareils mobiles, le télétravail, les informations classifiées, etc.) ;

- les mesures qui sont prises pour contrôler les activités (accès, destruction de stockage, accès à distance, journalisation).

Ces thèmes sont détaillés ci-dessous.

Les services de police élaborent des procédures détaillant les règles d'accès aux données et informations, ayant ou non une sensibilité particulière, ainsi que le contrôle mis en place pour s'assurer du respect de ces règles.

Les services de police définissent les règles et mesures de sécurité pour l'utilisation des supports média mobiles et pour l'accès et la gestion des informations à distance (p.e. télétravail). Des procédures qui concrétiseront la présente directive sont prévues à cet effet.

3) La sécurité concernant les ressources humaines

Les services de police établissent une politique relative à la gestion des membres du personnel et collaborateurs externes en matière de sécurité de l'information et de protection des données. Des procédures couvrant les aspects suivants sont développées :

Avant le recrutement :

- procédures d'engagement et mesures y afférentes.

Pendant l'occupation de l'emploi :

- les modalités visant à l'adhésion de tous les collaborateurs internes et externes aux instructions internes de l'organisation.

III. DE MINIMALE BEVEILIGINGSMAATREGELEN

1) Het informatieveiligheidsbeleid en beveiligingsplannen

De politiediensten dienen te beschikken over een uniform en geactualiseerd beleid inzake informatieveiligheid, hierna "het informatieveiligheidsbeleid", dat wordt gevalideerd door het "coördinatiecomité van de geïntegreerde politie"[2] (hierna het CCGPI) na advies van het "comité informatie en ICT"[3].

Rekening houdende met het informatieveiligheidsbeleid, worden vervolgens de beveiligingsplannen opgesteld, die de te implementeren technische en organisatorische maatregelen bevatten inzake informatieveiligheid. Deze beveiligingsplannen, evenals de procedures en processen die de onderhavige richtlijn zullen concretiseren, worden gevalideerd door de bevoegde hiërarchie, zijnde het Directiecomité wat de federale politie betreft, en de korpschef wat de politiezones betreft, na advies van de betrokken functionaris voor de gegevensbescherming.

Het informatieveiligheidsbeleid en de veiligheidsplannen evenals de procedures en processen die de onderhavige richtlijn zullen concretiseren, dienen regelmatig te worden geëvalueerd.

De politiediensten maken conform artikel 244 van de GBW het beleid inzake informatieveiligheid evenals de beveiligingsplannen over aan het Controleorgaan op de politionele informatie (hierna het "COC").

2) De organisatie van de informatieveiligheid

De politiediensten voorzien een risicobeheersysteem inzake informatieveiligheid en identificeren de rollen en verantwoordelijkheden van de verschillende actoren betrokken bij de informatieveiligheid.

De bevoegde functionaris voor de gegevensbescherming is ook belast met de opvolging van het informatieveiligheidsbeleid en de implementatie van het beveiligingsplan of de beveiligingsplannen.

Om ervoor te zorgen dat alle organisatorische maatregelen worden uitgevoerd, informeren de politiediensten hun personeel en de derden die onder hun verantwoordelijkheid werken. Het veiligheidsbeleid en de beveiligingsplannen dienen beschikbaar en raadpleegbaar te zijn voor de personen die deze moeten toepassen. Een toegang tot alle informatie is echter niet nodig om dit doel te bereiken.

Procedures en goede praktijken voor de informatieveiligheid die de onderhavige richtlijn zullen concretiseren, worden door de politiediensten ontwikkeld, goedgekeurd en gecommuniceerd.

Er worden procedures vastgelegd voor elke gebruiker, in het bijzonder voor diegenen die toegang hebben tot gegevens met een bijzondere gevoeligheid of tot kritieke systemen.

Deze procedures hebben betrekking op de volgende onderwerpen:

- de toegangscontrole / het autorisatiebeheer;

- de intrekking van rechten;

- de vertrouwelijkheid van gegevens;

- de fysieke toegang tot gebouwen en infrastructuur;

- de toegangssystemen en vertrouwelijkheid van toegangsgegevens;

- de maatregelen om het juiste gebruik te bepalen van werkinstrumenten die ter beschikking gesteld worden (zoals mobiele apparaten, telewerk, de geclassificeerde informatie, etc.);

- de maatregelen die genomen worden om de activiteiten te controleren (toegang, vernietiging van opslag, toegang op afstand, logbestanden).

Deze onderwerpen worden hieronder toegelicht.

De politiediensten leggen procedures vast houdende de regels voor de toegang tot de gegevens en de informatie, met al dan niet een bijzondere gevoeligheid, evenals de controle die voorzien wordt om de naleving van deze regels te verzekeren.

De politiediensten bepalen regels en veiligheidsmaatregelen voor het gebruik van mobiele informatiedragers en voor de toegang tot en het beheer van informatie op afstand (vb. telewerken). Procedures die de onderhavige richtlijn zullen concretiseren, worden hiervoor voorzien.

3) De veiligheid inzake het personeelsbeheer

De politiediensten stellen een beleid op voor het beheer van de personeelsleden en de externe medewerkers inzake informatieveiligheid en gegevensbescherming. Er worden procedures ontwikkeld die betrekking hebben op de volgende aspecten:

Voor de aanwerving:

- aanwervingsprocedures en bijbehorende maatregelen.

Tijdens de tewerkstelling:

- modaliteiten die voorzien dat alle personeelsleden en externe medewerkers zich dienen te houden aan de interne instructies van de organisatie.

Après la résiliation ou la modification de la relation de travail :

- les responsabilités et les obligations relatives à la sécurité de l'information et à la protection des données demeurent après la résiliation ou le changement d'emploi et ces conditions doivent être clairement communiquées et intégrées dans le processus de gestion des collaborateurs (internes ou externes).

Un contrat de confidentialité est conclu avec toute personne n'étant pas soumise au statut des membres de la police intégrée et ayant accès aux systèmes d'information des services de police.

4) Sensibilisation, formation & communication

Les services de police prévoient une formation continue des membres du personnel et des collaborateurs externes en ce qui concerne la politique de sécurité de l'information et de protection des données.

Les services de police prévoient un plan de formation afin que tous les membres du personnel et collaborateurs externes, reçoivent la formation nécessaire et qu'ils soient informés des modifications apportées aux directives et procédures concernant :

- la sécurité de l'information et la protection de la vie privée ;

- les mesures applicables à l'exercice de leurs fonctions ;

- leur rôle et leur responsabilité à cet égard.

Les services de police développent un programme de sensibilisation ayant les objectifs suivants :

- conscientiser les membres du personnel et les collaborateurs externes à la sécurité de l'information et à la protection de la vie privée (en mettant l'accent sur les données à caractère personnel) ;

- expliquer clairement les responsabilités respectives de l'autorité hiérarchique, d'un service spécifique, du collaborateur et des personnes chargées du contrôle de l'application des mesures de sécurité.

Les sessions doivent être répétées régulièrement afin que les nouveaux collaborateurs soient inclus assez tôt dans le programme.

Pour chaque collaborateur, l'information doit être :

o compréhensible;

o appropriée pour l'exercice de sa fonction ;

o toujours accessible de manière simple et facile.

5) La gestion des actifs[4]

Afin de garantir la sécurité des systèmes traitant de l'information opérationnelle, les services de police établissent l'inventaire de leurs actifs essentiels, quels que soient leurs types (informations, données, applications, réseaux, processus, systèmes, etc)[5]. L'inventaire est une liste non-exhaustive et évolutive, qui sera complétée au fur et à mesure, afin d'assurer une amélioration continue en utilisant le cycle PDCA mentionné ci-dessus. Il s'agit d'augmenter progressivement le niveau de maturité des services de police.

Chaque actif sera détaillé et tous les éléments seront repris et tenus à jour afin de bénéficier d'une cartographie correcte de l'architecture des systèmes et de l'information de l'organisation.

Un responsable fonctionnel est identifié pour chaque élément de cet inventaire et sa tâche est précisée dans le plan de sécurité concerné.

Les services de police veillent à mettre en place une procédure de gestion des actifs de l'information en tenant compte de l'importance des données de l'organisation.

6) Le contrôle d'accès

Pour les services de police, les règles relatives à l'accès aux données et informations dans les banques de données policières sont contenues dans la directive ministérielle visée à l'article 44/4, §3 LFP.

Pour l'accès aux autres actifs ICT essentiels, les services de police définissent les règles d'accès dans des procédures distinctes qui concrétiseront la présente directive.

Un processus qui garantit l'identification de l'utilisateur lorsque celui-ci souhaite exercer ses tâches est mis en place. Les actifs ICT essentiels ne sont accessibles que via un identifiant individuel et unique.

7) La cryptographie

Les services de police protègent adéquatement les données et l'information lors de leur stockage, de leur transport et de leur utilisation.

Na beëindiging of verandering van dienstverband:

- verantwoordelijkheden en verplichtingen voor informatiebeveiliging en gegevensbescherming blijven bestaan na beëindiging of verandering van dienstverband en deze voorwaarden moeten duidelijk worden gecommuniceerd en geïntegreerd in het werknemersmanagementproces (intern of extern).

Met alle personen die toegang hebben tot de informatiesystemen van de politiediensten en die niet onderworpen zijn aan het statuut van de personeelsleden van de geïntegreerde politie, wordt een vertrouwelijkheidsovereenkomst afgesloten.

4) Sensibilisering, opleiding & communicatie

De politiediensten voorzien in een permanente opleiding van de personeelsleden en de externe medewerkers met betrekking tot het informatieveiligheids- en gegevensbeschermingsbeleid.

De politiediensten voorzien een opleidingsplan, opdat alle personeelsleden en externe medewerkers, de nodige opleiding krijgen en op de hoogte worden gehouden van aanpassingen aan de richtlijnen en procedures betreffende:

- de informatieveiligheid en de bescherming van het privéleven;

- de maatregelen die van toepassing zijn bij de uitoefening van hun functies;

- hun rol en verantwoordelijkheid daarin.

De politiediensten ontwikkelen een sensibiliseringsprogramma met de volgende doelstellingen:

- de personeelsleden en de externe medewerkers bewust maken van de informatieveiligheid en de bescherming van het privéleven (met focus op persoonsgegevens);

- duidelijk uitleggen welke de verantwoordelijkheden zijn van de hiërarchische overheid, van een specifieke dienst, van de medewerkers en van de personen belast met de controle van de toepassing van de veiligheidsmaatregelen.

De sessies dienen op geregelde tijdstippen te worden herhaald, zodat ook nieuwe medewerkers tijdig opgenomen worden in het programma.

De informatie moet voor elk van de medewerkers:

o verstaanbaar zijn;

o aangepast aan de uitoefening van zijn/haar functie;

o steeds op een eenvoudige, vlotte manier toegankelijk zijn.

5) Het beheer van de activa[4]

Teneinde de veiligheid te verzekeren van de systemen die operationele gegevens verwerken, stellen de politiediensten de inventaris op van hun essentiële activa, ongeacht de categorie ervan (informatie, gegevens, applicaties, netwerken, processen, systemen enz.)[5]. De inventaris is een niet-exhaustieve en evolutieve lijst, die stapsgewijs aangevuld zal worden, teneinde een voortdurende verbetering te kunnen voorzien gebruikmakend van de hiervoor vermelde PDCA-cyclus. Het doel is om het maturiteitsniveau van de politiediensten geleidelijk te verhogen.

Alle activa dienen in detail beschreven te worden en alle elementen ervan worden bijgehouden en geactualiseerd om zodoende te beschikken over een correct beeld van de informatie- en systeemarchitectuur van de organisatie.

Een functionele verantwoordelijke wordt geïdentificeerd voor elk element van deze inventaris en in het betrokken beveiligingsplan wordt zijn taak duidelijk omschreven.

De politiediensten zorgen ervoor dat er een procedure voor het beheer van de informatiemiddelen wordt uitgewerkt. Hierbij wordt rekening gehouden met het belang van de gegevens van de organisatie.

6) De toegangscontrole

Voor de politiediensten zijn de regels m.b.t. de toegang tot de gegevens en informatie in de politionele gegevensbanken vervat in de ministeriële richtlijn bedoeld in artikel 44/4, §3 WPA.

Voor de toegang tot de andere essentiële ICT-activa bepalen de politiediensten de toegangsregels in afzonderlijke procedures die de onderhavige richtlijn zullen concretiseren.

Er wordt een proces voorzien dat de identificatie van de gebruiker waarborgt wanneer deze zijn of haar taken wenst uit te oefenen. Essentiële ICT-activa zijn enkel toegankelijk via een individuele en unieke identificator.

7) Cryptografie

De politiediensten beschermen afdoende de gegevens en informatie tijdens de opslag, de overdracht en het gebruik ervan.

Comme décrit dans les articles 50 et 60 LPD, les données à caractère personnel doivent être protégées de manière appropriée pendant le stockage, le transport et l'utilisation de celles-ci. Le niveau de protection tient compte de l'analyse de risque avec, selon les besoins, des mesures de pseudonymisation ou de chiffrement des données ou de l'information, ou toute autre mesure permettant de garantir le niveau de protection approprié.

8) La sécurité physique

Les services de police sécurisent leurs infrastructures. Ils prennent les mesures de protection et de sécurisation afin de gérer l'accès des personnes autorisées aux bâtiments et aux locaux. Les mesures sont adaptées en fonction de la présence physique de personnes dans les locaux.

Les services de police protègent leurs données et leurs supports de données. Ils prennent des mesures préventives contre la perte, l'endommagement, le vol ou la compromission des actifs de l'organisation et contre une éventuelle interruption des activités de l'organisation.

9) La sécurité liée aux opérations

Les services de police mettent en œuvre des mesures spécifiques pour chaque actif essentiel : tout acte suspect ou tout incident est rapporté et investigué. Une trace du suivi de ces incidents est également conservée.

Les mesures techniques minimales qui doivent être prévues pour les moyens ICT des services de police[6], sont:

- un antimalware/antivirus actuel et à jour ;

- un système de détection et de blocage des intrusions ou des accès non autorisés ;

- une procédure de mise à jour des logiciels ;

- une gestion des incidents (y compris leur communication) ;

- des procédures de back-up et de continuité des activités (sécurité opérationnelle).

10) La sécurité de la communication des informations

Les services de police prennent des mesures spécifiques pour sécuriser la communication de l'information, afin d'éviter les accès non autorisés aux données et informations[7].

Si la loi le permet, les données et informations des services de police sont toujours consultées en retournant vers la banque de données d'origine avec un contrôle des autorisations prévues pour celle-ci. Des communications, des copies ou des extractions sont évitées. Si ce n'est absolument pas possible et qu'une communication de certaines données et informations des services de police doit malgré tout être effectuée, alors ces données communiquées doivent toujours avoir un caractère adéquat, pertinent et non excessif par rapport à la finalité de la communication et les mesures de sécurité nécessaires doivent toujours être prises.

11) Acquisition, développement et maintenance des systèmes d'information

Lors de l'achat, du développement (et test) et de la maintenance de systèmes, les services de police conçoivent et utilisent des processus et des procédures qui concrétiseront la présente directive pour protéger les informations et ce, aussi bien pendant la phase de développement que d'utilisation opérationnelle.

Les systèmes et les processus de traitement de données sont développés et conçus pour protéger par défaut les données et informations (art. 51, §2 LPD).

Si le recours à des données opérationnelles est indispensable pour le développement et la réalisation de tests, alors leur utilisation peut être exceptionnellement autorisée par le responsable du traitement après avis du comité information et ICT.

12) Relations avec les tiers (fournisseurs, autorités)

Les services de police définissent les relations avec les fournisseurs et les autorités.

Ces relations sont formalisées dans un document qui indique clairement, le cas échéant :

- qui est (sont) le(s) responsable(s) du traitement ;

- quelle partie est le sous-traitant ;

- comment les responsabilités sont réparties ;

- comment la protection des données est organisée, y compris :

o la sécurité et le comportement requis ;

o la gestion des incidents ;

o le signalement des violations ;

o le contact avec les autorités (ou non).

13) Le recours au cloud

Si les services de police font appel à des services de « cloud computing », ces derniers doivent se conformer aux mesures de sécurité requises, telles qu'elles sont définies dans la politique de sécurité de

Zoals beschreven in artikel 50 en 60 van de GBW moeten persoonsgegevens tijdens de opslag, de overdracht en het gebruik ervan adequaat worden beschermd. Het beschermingsniveau houdt rekening met de risicoanalyse en, indien nodig, worden pseudonimiserings- of versleutelingsmaatregelen voor de gegevens of informatie of elke andere maatregel die een passend beschermingsniveau waarborgt genomen.

8) De fysieke veiligheid

De politiediensten beveiligen hun infrastructuur. Zij nemen de beschermings- en beveiligingsmaatregelen om de toegangen te beheren van de personen die de gebouwen en lokalen mogen betreden. De maatregelen zijn aangepast in functie van de fysieke aanwezigheid van personen in de lokalen.

De politiediensten beschermen hun gegevens en hun gegevensdragers. Zij nemen preventieve maatregelen tegen verlies, schade, diefstal van of ongeoorloofde toegang tot de activa van de organisatie en tegen een eventuele onderbreking van de activiteiten van de organisatie.

9) De operationele veiligheid

De politiediensten nemen voor alle essentiële activa afzonderlijk specifieke maatregelen: elke verdachte handeling of elk incident wordt gemeld en onderzocht. Er wordt tevens een spoor bewaard van de opvolging van deze incidenten.

De minimale technische maatregelen die voor de ICT-middelen van de politiediensten genomen moeten worden[6], zijn:

- een anti-malware/antivirus: actueel en up-to-date;

- een detectie- en blokkeringssysteem voor inbraak of ongeoorloofde toegang;

- een procedure voor het bijwerken van software;

- een incident management (inclusief communicatie);

- back-up en business continuity (Operationele veiligheid) procedures.

10) De beveiliging van de mededeling van de informatie

De politiediensten nemen specifieke maatregelen om de mededeling van informatie te beveiligen, teneinde een ongeoorloofde toegang tot de gegevens en informatie te vermijden[7].

Indien toegelaten door de wet, worden de informatie en de gegevens van de politiediensten steeds geraadpleegd door terug te keren naar de oorspronkelijke gegevensbank met een controle van de daarvoor voorziene autorisaties. Mededelingen, kopieën of extracties worden vermeden. Indien dit absoluut niet mogelijk is en een mededeling van bepaalde informatie of gegevens van de politiediensten toch dient te gebeuren, dienen de meegedeelde gegevens steeds toereikend, ter zake dienend en niet overmatig te zijn rekening houdende met het doeleinde van de mededeling en dienen steeds de nodige veiligheidsmaatregelen voorzien te worden.

11) Aankoop, ontwikkeling en onderhoud van informatiesystemen

De politiediensten dienen bij de aankoop, de ontwikkeling (en testen) en het onderhoud van systemen, processen en procedures die de onderhavige richtlijn zullen concretiseren, op te stellen en te gebruiken om de informatie te beschermen, zowel in de ontwikkelingsfase als tijdens het operationeel gebruik ervan.

De systemen en processen voor gegevensverwerking worden ontworpen en ontwikkeld om de gegevens en informatie standaard (by default) te beschermen (art. 51, §2 GBW).

Indien het gebruik van operationele gegevens noodzakelijk is voor de ontwikkeling en de uitvoering van tests, dan kan het gebruik ervan door de verwerkingsverantwoordelijke uitzonderlijk worden toegestaan na advies van het comité informatie en ICT.

12) Betrekkingen met derden (leveranciers, overheden)

De politiediensten leggen de relaties met de leveranciers en de overheden vast.

Deze relaties worden geformaliseerd in een document, dat in voorkomend geval duidelijk aangeeft:

- wie de verwerkingsverantwoordelijke(n) is (zijn);

- welke partij de verwerker is;

- hoe de verantwoordelijkheden worden verdeeld;

- hoe de gegevensbescherming georganiseerd is; met inbegrip van:

o de veiligheid en de vereiste houding;

o het beheer van incidenten;

o de melding van inbreuken;

o het contact met de overheden (of niet).

13) Het gebruik van een "Cloud"

Indien politiediensten beroep doen op "cloud computing" diensten, voldoen deze aan de vereiste veiligheidsmaatregelen zoals hernomen in het informatieveiligheidsbeleid en, in voorkomend geval, in het

l'information et, le cas échéant, dans le plan de sécurité correspondant. Les dérogations aux principes énoncés dans la politique de sécurité de l'information doivent toujours être soumises à l'avis préalable du comité Information et ICT, et une décision du CCGPI est requise.

Des contrats et des documents sont rédigés afin de faire respecter les mesures de sécurité exigées.

Les rapports d'audit et les certifications des fournisseurs de services cloud ainsi que l'architecture de la solution « cloud » sont communiquées aux gestionnaires des systèmes compétents (à la DRI et dans la zone de police respective) afin qu'ils puissent vérifier au préalable si les mesures de sécurité requises sont respectées et/ou demander les adaptations nécessaires le cas échéant.

Il est exigé que les centres de données « cloud » et les facilités techniques qui y sont liées se situent sur le territoire de l'Union Européenne.

Dans les contrats et les documents, il est clairement établi qui est le responsable du traitement, quelle partie est le sous-traitant et comment les responsabilités sont réparties.

14) Gestion des incidents liés à la sécurité de l'information

Les services de police veillent à ce que les membres du personnel ainsi que les collaborateurs externes et d'autres personnes impliquées disposent d'une procédure permettant de signaler les activités suspectes.

Il s'agit d'une procédure permettant de rapporter, d'enregistrer et de gérer des violations potentielles ou présumées de données à caractère personnel ou de la sécurité des systèmes afin que les vulnérabilités puissent être traitées rapidement et de manière structurée.

Les services de police mettent également en place un plan de gestion tant pour des incidents en matière de sécurité de l'information que pour des violations de données à caractère personnel. Ce plan reprendra :

- les rôles et les responsabilités de tous les acteurs impliqués ;

- un registre interne des incidents contenant tous les incidents de sécurité signalés.

Les services de police veillent à ce que le membre du personnel qui signale un éventuel incident de sécurité n'en subisse pas de conséquences négatives.

15) Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Les services de police prévoient un système de protection garantissant la disponibilité des données et de l'information.

Les services de police prévoient la protection nécessaire de l'information et des données qu'ils traitent contre la perte, la modification ou la destruction non autorisée, soit par accident soit par acte malveillant.

Les services de police veillent à ce que la disponibilité et l'accès à des informations ou à des données soient rétablis rapidement après un incident physique ou technique.

Les services de police prévoient une solution afin d'assurer la continuité des applications utilisées. Dans cette solution, les codes de développement des applications seront au maximum conservés.

16) Veille juridique

Les services de police suivent toutes les modifications législatives relatives à la sécurité de l'information et la protection des données, ainsi que les avis émis ou modifiés par les autorités ou organes compétents à ce sujet.

17) Evaluation des mesures de sécurité

Les services de police évaluent régulièrement la sécurité de l'information (entre autres conformément au cycle PDCA précité).

Les plans de sécurité doivent évoluer avec le temps. Ils peuvent être revus pour tenir compte :

- des changements dans les menaces et des leçons tirées suite à la gestion d'incidents ;

- des résultats d'analyses de risques, d'enquêtes de contrôle ou d'audits ;

- de changements de l'organisation ou du contexte juridique, réglementaire ou technologique.

Ces évolutions et adaptations sont suivies par le comité information et ICT et le comité de coordination de la police intégrée, avec les tâches principales suivantes :

- le suivi de l'exécution de la politique de sécurité et des plans de sécurité ;

- la mesure de l'évolution et du statut de sécurité de l'organisation ;

- la proposition de mises à jour ;

- la proposition de documents et directives complémentaires pour faciliter et rendre plus claire la mise en œuvre ;

- le suivi de l'évolution des documents techniques.

betrokken beveiligingsplan. Wanneer wordt afgeweken van de principes vastgelegd in het informatieveiligheidsbeleid dient steeds het voorafgaand advies van het comité informatie en ICT te worden ingewonnen en is een beslissing vereist van het CCGPI.

Contracten/documenten dienen als dusdanig te worden opgesteld, opdat de vereiste veiligheidsmaatregelen worden gerespecteerd.

Auditrapporten en certificeringen van cloud-dienstverleners, alsook de architectuur van de cloud-oplossing, worden aan de bevoegde systeembeheerders (bij DRI en in respectievelijke politiezone) gecommuniceerd, zodat zij voorafgaandelijk kunnen nagaan of deze voldoen aan de vereiste veiligheidsmaatregelen en/of desgewenst de nodige aanpassingen kunnen vragen.

Vereist is dat Cloud-datacenters en de bijbehorende technische faciliteiten zich op het grondgebied van de Europese Unie bevinden.

In contracten/documenten moet duidelijk worden vastgelegd wie de verwerkingsverantwoordelijke is, welke partij verwerker is en hoe de verantwoordelijkheden worden verdeeld.

14) Incident management aangaande informatieveiligheid

De politiediensten zorgen ervoor dat zowel personeelsleden als externe medewerkers en andere betrokken personen beschikken over een procedure die het mogelijk maakt om verdachte activiteiten te rapporteren.

Het gaat om een procedure om mogelijke of vermoedelijke inbreuken in verband met persoonsgegevens of in verband met de veiligheid van systemen te rapporteren, te registeren en te behandelen zodat kwetsbaarheden voortijdig en gestructureerd kunnen behandeld worden.

De politiediensten stellen eveneens een incidentenbeheersplan op, zowel voor informatieveiligheidsincidenten als inbreuken in verband met persoonsgegevens, dat:

- de rollen en verantwoordelijkheden van alle betrokken actoren vastlegt;

- een intern register voorziet waarin alle gemelde inbreuken op de beveiliging worden hernomen.

De politiediensten zorgen ervoor dat het personeelslid dat een mogelijk veiligheidsincident rapporteert hierdoor geen negatieve gevolgen ondervindt.

15) Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

De politiediensten voorzien een beschermingssysteem dat de beschikbaarheid van de gegevens en de informatie garandeert.

De politiediensten voorzien de nodige bescherming van de informatie en de gegevens die zij verwerken tegen verlies, ongeoorloofde wijziging of vernietiging, hetzij per ongeluk hetzij door een moedwillige handeling.

De politiediensten zorgen ervoor dat de beschikbaarheid van en toegang tot de informatie en de gegevens na een fysiek of technisch incident tijdig kan hersteld worden.

De politiediensten voorzien een oplossing, teneinde de continuïteit van de gebruikte toepassingen te verzekeren. In deze oplossing worden maximaal de ontwikkelcodes van de toepassingen bijgehouden.

16) Juridische monitoring

De politiediensten volgen alle wetswijzigingen inzake de informatieveiligheid en de gegevensbescherming op, evenals de door de bevoegde overheden of organen uitgebrachte of gewijzigde adviezen hieromtrent.

17) Evaluatie van de beveiligingsmaatregelen

De politiediensten evalueren op geregelde tijdstippen de informatiebeveiliging (onder andere conform de voornoemde PDCA-cyclus).

De beveiligingsplannen dienen mettertijd te evolueren. Ze kunnen met name worden herzien om rekening te houden met:

- veranderingen in bedreigingen en feedback als gevolg van incidentenbehandeling;

- de resultaten van risicoanalyses, controleonderzoeken of audits;

- veranderingen in organisatorische, juridische, regelgevende en technologische contexten.

Deze evoluties en aanpassingen worden opgevolgd door het comité informatie en ICT en het "coördinatiecomité van de geïntegreerde politie", met de volgende hoofdtaken:

- de opvolging van de uitvoering van het veiligheidsbeleid en de beveiligingsplannen;

- het meten van de voortgang en de beveiligingsstatus van de organisatie;

- het voorstellen van updates;

- het voorstellen van aanvullende documenten en richtsnoeren om de tenuitvoerlegging ervan te vergemakkelijken of te verduidelijken;

- de opvolging van de evolutie van de technische documenten.

IV. La méthodologie

Pour établir l'inventaire des actifs essentiels des services de police et l'analyse de risque pour chacun des actifs essentiels, les services de police peuvent s'inspirer de la méthodologie prévue dans les « Baseline Information Security Guidelines » du Centre pour la Cybersécurité Belgique.

Notes

[1] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

[2] Tel que visé à l'article 8*ter* de la loi du 7 décembre 1998 organisant un service de police intégré structuré à deux niveaux.

[3] Tel que visé à l'article 8sexies de la loi du 7 décembre 1998 organisant un service de police intégré structuré à deux niveaux.

[4] Pour la sécurité de l'information, on considère les actifs essentiels au sens large comme étant "toutes les ressources qui ont une valeur pour l'organisation et qui doivent être sécurisées". Cela ne se limite pas uniquement à l'infrastructure IT ou aux ressources matérielles, mais aussi aux personnes. Il peut également s'agir de ressources immatérielles, telles que des processus, des procédures, certaines méthodes de travail, des connaissances et des compétences, etc.

[5] Datacenter, systèmes d'accès, antivirus, ...

6 Comme décrit dans l'introduction, il s'agit d'une implémentation progressive en fonction du niveau de maturité.

[7] Il peut s'agir de mesures de sécurité prévues par un arrêté royal prévu par l'article 44/11/12 LFP réglementant un accès particulier ou un protocole de coopération en matière de communication de données avec un partenaire des services de la police.

IV. De methodologie

Voor het inventariseren van de essentiële activa van de politiediensten en de risicoanalyse voor elk van deze essentiële activa kunnen de politiediensten zich inspireren op de methodologie voorzien in de "Baseline Information Security Guidelines" van het Belgisch Centrum voor Cybersecurity.

Nota's

[1] Verordening (EU) 2016/679 van het Europees Parlement van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

[2] Zoals bedoeld in artikel 8*ter* van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.

[3] Zoals bedoeld in artikel 8sexies van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.

[4] Voor informatiebeveiliging worden de essentiële activa in brede zin beschouwd als 'alle middelen die een waarde hebben voor de organisatie en die moeten worden beveiligd'. Dit beperkt zich niet enkel tot IT-infrastructuur of tastbare middelen, maar ook tot mensen. Het kunnen bovendien ook ontastbare middelen zijn, zoals processen, procedures, bepaalde werkwijzen, kennis en expertise etc.

[5] Datacenter, toegangsystemen, antivirus, ...

[6] Zoals beschreven in de inleiding, gaat het om een progressieve implementatie ingevolge het maturiteitsniveau.

[7] Het kan onder meer gaan om veiligheidsmaatregelen die voorzien worden in een koninklijk besluit voorzien door artikel 44/11/12 WPA dat een bepaalde toegang regelt of een samenwerkingsprotocol inzake mededeling van gegevens aan een partner van de politiediensten.

AGENCE FEDERALE DE CONTROLE NUCLEAIRE

[C − 2021/41359]

7 MAI 2021. — Règlement technique fixant les critères et les modalités d'agrément des services de dosimétrie pour l'exécution d'analyses radiotoxicologiques

Vu la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire ;

Vu l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants, ci-après nommé " règlement général » ;

Considérant que, conformément à l'article 30.6.5, § 1er, du règlement général, l'Agence fédérale de Contrôle nucléaire fixe les critères et les modalités d'agrément des services de dosimétrie qui effectuent la dosimétrie externe ou des analyses radiotoxicologiques,

Arrête :

Article 1er. Champ d'application

Le présent règlement technique fixe les critères et les modalités d'agrément des services de dosimétrie qui effectuent des analyses radiotoxicologiques dans le cadre de la dosimétrie interne de personnes.

Art. 2. Définitions

§ 1er

Les définitions reprises à l'article 2 du règlement général s'appliquent également au présent règlement technique.

§ 2

En complément, pour l'application du présent règlement technique, on entend par :

1° BELAC : l'Organisme belge d'Accréditation, créé en vertu de la loi du 20 juillet 1990 concernant l'accréditation des organismes d'évaluation de la conformité ;

2° système de gestion de la qualité : ensemble d'éléments corrélés ou en interaction d'un organisme qui sont utilisés pour établir des politiques et des objectifs qualité, ainsi que les processus permettant d'atteindre ces objectifs ;

FEDERAAL AGENTSCHAP VOOR NUCLEAIRE CONTROLE

[C − 2021/41359]

7 MEI 2021. — Technisch reglement tot vaststelling van de criteria en de modaliteiten voor de erkenning van de dosimetrische diensten voor het uitvoeren van radiotoxicologische analyses

Gelet op de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor nucleaire controle;

Gelet op het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen, hierna het "algemeen reglement";

Overwegende dat ingevolge artikel 30.6.5, § 1, van het algemeen reglement, het Federaal Agentschap voor Nucleaire Controle de criteria en de modaliteiten bepaalt voor de erkenning van de dosimetrische diensten die externe dosimetrie of radiotoxicologische analyses uitvoeren,

Besluit :

Artikel 1. Toepassingsgebied

Dit technisch reglement stelt de criteria en de modaliteiten vast voor de erkenning van de dosimetrische diensten die radiotoxicologische analyses uitvoeren in het kader van interne dosimetrie van personen.

Art. 2. Definities

§ 1

De definities opgenomen in artikel 2 van het algemeen reglement zijn van toepassing op dit technisch reglement.

§ 2

Aanvullend voor de toepassing van dit technisch reglement wordt verstaan onder:

1° BELAC: de Belgische Accreditatie-instelling opgericht krachtens de wet van 20 juli 1990 betreffende de accreditatie van instellingen voor de conformiteitsbeoordeling;

2° kwaliteitsmanagement systeem: het geheel van samenhangende of interagerende elementen van een organisme die gebruikt worden voor het vastleggen van kwaliteitsbeleid en -doelstellingen, alsook de processen om deze objectieven te verwezenlijken;