SERVICE PUBLIC FEDERAL INTERIEUR

[C − 2021/42602]

25 AVRIL 2021. — Arrêté royal relatif au nombre minimum de personnel et aux moyens organisationnels, techniques et d'infrastructure des entreprises de gardiennage, des services internes de gardiennage et des services de sécurité

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, les articles 32 et 89;

Vu l'arrêté royal du 14 mai 1991 relatif à l'équipement technique des entreprises de gardiennage et des services internes de gardiennage;

Vu l'arrêté royal du 20 mars 2017 relatif au nombre minimum de personnel et aux moyens organisationnels, techniques et d'infrastructure pour l'exercice de l'activité de gardiennage de gestion de centraux d'alarme;

Vu la communication à la Commission européenne, le 6 décembre 2018, en application de l'article 5 de la directive 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information;

Vu l'accord du Ministre du Budget, donné le 9 juillet 2020;

Vu l'avis de l'Inspecteur des Finances, donné le 16 juillet 2019;

Vu l'avis 66.700/2 du Conseil d'Etat, donné le 2 décembre 2019, en application de l'article 84, § 1er, alinéa 1er, 2°, des lois coordonnées sur le Conseil d'Etat, remplacé par la loi du 2 avril 2003;

Sur la proposition de Notre ministre de l'Intérieur,

Nous avons arrêté et arrêtons :

CHAPITRE 1er. — *Définitions*

Article 1er. Dans le cadre de l'application du présent arrêté, il convient d'entendre par :

1° la loi : la loi du 2 octobre 2017 réglementant la sécurité privée et particulière;

2° la loi-cadre STI: la loi du 17 août 2013 portant création du cadre pour le déploiement de systèmes de transport intelligents et modifiant la loi du 10 avril 1990 réglementant la sécurité privée et particulière;

3° le règlement UE 305/2013: le règlement délégué (UE) n° 305/2013 de la commission du 26 novembre 2012 complétant la Directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition harmonisée d'un service d'appel d'urgence (eCall) interopérable dans toute l'Union européenne;

4° temps de réaction : le temps qui s'écoule entre l'enregistrement d'un appel par un système de réception et la première action entreprise par un opérateur d'une centrale d'alarme;

5° administration : la Direction Sécurité privée de la Direction générale Sécurité et Prévention du Service public fédéral Intérieur;

6° dirigeant stratégique : la personne, telle que visée à l'article 2, 25°, de la loi, qui :

a) a la direction sur l'ensemble de l'entreprise de gardiennage ou du service interne de gardiennage ou de sécurité,

b) exerce une autorité sur tous les agents de gardiennage ou de sécurité de l'entreprise de gardiennage ou du service interne de gardiennage ou de sécurité ou

c) exerce une autorité sur d'autres dirigeants stratégiques ou opérationnels de l'entreprise de gardiennage ou du service interne de gardiennage ou de sécurité;

7° dirigeant opérationnel : la personne, telle que visée à l'article 2, 25°, de la loi, qui exerce une autorité sur plus de 15 agents de gardiennage ou de sécurité sans que cela n'implique les responsabilités d'un dirigeant stratégique;

8° contrat d'assurance de la protection juridique : contrat d'assurance tel que visé au chapitre 4 du titre III de la partie IV de la loi du 4 avril 2014 relative aux assurances;

9° organisme d'inspection: un organisme indépendant qui répond au moins aux critères de la norme EN-ISO/IEC 17020;

10° heures de bureau : la période entre 9 heures et 17 heures;

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN

[C − 2021/42602]

25 APRIL 2021. — Koninklijk besluit betreffende de minimumvereisten inzake personeel en organisatorische, technische en infrastructurele middelen van bewakingsondernemingen, interne bewakingsdiensten en veiligheidsdiensten

FILIP, Koning der Belgen,

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

Gelet op de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, artikelen 32 en 89;

Gelet op het koninklijk besluit van 14 mei 1991 betreffende de technische uitrusting van bewakingsondernemingen en interne bewakingsdiensten;

Gelet op het koninklijk besluit van 20 maart 2017 betreffende de minimumvereisten inzake personeel en organisatorische, technische en infrastructurele middelen voor de uitoefening van de bewakingsactiviteiten beheer van alarmcentrales;

Gelet op de mededeling aan de Europese Commissie, op 6 december 2018, met toepassing van artikel 5 van richtlijn 2015/1535 van het Europees parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij;

Gelet op het akkoord van de Minister van Begroting, gegeven op 9 juli 2020;

Gelet op het advies van de Inspecteur van Financiën, gegeven op 16 juli 2019;

Gelet op advies 66.700/2 van de Raad van State, gegeven op 2 december 2019, met toepassing van artikel 84, § 1, eerste lid, 2°, van de gecoördineerde wetten op de Raad van State, vervangen bij de wet van 2 april 2003;

Op de voordracht van Onze Minister van Binnenlandse Zaken,

Hebben Wij besloten en besluiten Wij :

HOOFDSTUK 1. — *Definities*

Artikel 1. In het kader van de toepassing van dit besluit wordt verstaan onder:

1° de wet: de wet van 2 oktober 2017 tot regeling van private en bijzondere veiligheid;

2° de ITS-kaderwet: de wet van 17 augustus 2013 tot creatie van het kader voor het invoeren van intelligente vervoerssystemen en tot wijziging van de wet van 10 april 1990 tot regeling van de private en bijzondere veiligheid;

3° de EU-verordening 305/2013: de gedelegeerde verordening (EU) Nr. 305/2013 van de commissie van 26 november 2012 tot aanvulling van de Richtlijn 2010/40/EU van het Europees Parlement en de Raad, wat de geharmoniseerde voorziening in de gehele Unie van een interoperabele eCall betreft;

4° reactietijd: de tijd die verloopt tussen de registratie van een oproep door een ontvangstsysteem en de eerste actie uitgevoerd door een operator van een alarmcentrale;

5° administratie: de Directie Private Veiligheid bij de Algemene Directie Veiligheid en Preventie bij de Federale Overheidsdienst Binnenlandse Zaken;

6° strategisch leidinggevende : de persoon, zoals bedoeld in artikel 2, 25°, van de wet, die :

a) de leiding heeft over het geheel van de bewakingsonderneming of interne bewakings- of veiligheidsdienst,

b) gezag uitoefent over alle bewakings- of veiligheidsagenten van de bewakingsonderneming of interne bewakings- of veiligheidsdienst of

c) gezag uitoefent over andere strategisch of operationeel leidinggevenden van de bewakingsonderneming of interne bewakings- of veiligheidsdienst;

7° operationeel leidinggevende: leidinggevend personeelslid dat gezag uitoefent over meer dan 15 bewakings- of veiligheidsagenten zonder dat dit verantwoordelijkheden inhoudt van een strategisch leidinggevende;

8° rechtsbijstandverzekering : verzekeringsovereenkomst zoals bedoeld in deel 4, titel III, hoofdstuk 4 van de wet van 4 april 2014 betreffende de verzekeringen;

9° inspectieinstelling: een onafhankelijke instelling die minstens voldoet aan de criteria van de norm EN-ISO/IEC 17020;

10° kantooruren: de periode tussen 9 uur en 17 uur;

11° jour ouvrable : tous les jours autres que le samedi, le dimanche et les jours fériés légaux;

12° ministre : le ministre de l'Intérieur;

13° système d'alarmes pour les biens : système d'alarme destiné à prévenir ou constater des délits contre des biens;

14° sécurité de l'information : protection de la confidentialité, de l'intégrité et de la disponibilité de l'information;

15° Règlement Général sur la Protection des Données : le 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 (règlement général sur la protection des données);

16° infrastructure : un bâtiment, une partie de bâtiment ou une structure permanente ou temporaire qui est utilisé par une entreprise ou un service pour soutenir son fonctionnement général.

CHAPITRE 2. — *Conditions pour l'exercice d'activités de gardiennage*

Art. 2. § 1er. Les entreprises de gardiennage et les services internes de gardiennage et de sécurité ayant moins de 50 agents de gardiennage ou de sécurité disposent d'au moins un dirigeant stratégique.

Les entreprises de gardiennage et les services internes de gardiennage et de sécurité ayant 50 agents de gardiennage ou de sécurité ou plus disposent d'au moins deux dirigeants stratégiques.

La détermination du nombre d'agents dans une entreprise ou un service au sens des premier et deuxième alinéas se base sur le nombre total d'agents qui doivent disposer d'une carte d'identification valable au sein de l'entreprise ou du service concerné.

§ 2. Pour les entreprises de gardiennage, en personne physique, au moins la personne physique concernée est un dirigeant stratégique.

Pour les entreprises de gardiennage, en personne morale, au minimum les personnes suivantes sont, selon le cas, des dirigeants stratégiques :

- les gérants;

- les administrateurs délégués, ainsi que les autres administrateurs qui sont habilités, eu égard aux dispositions des statuts de l'entreprise, à engager cette dernière, seuls ou avec d'autres administrateurs.

Pour les services internes de gardiennage et de sécurité, au minimum les personnes qui exercent la direction fonctionnelle de l'ensemble du service sont des dirigeants stratégiques.

§ 3. Si le seul dirigeant stratégique d'une entreprise de gardiennage autorisée ou d'un service interne de gardiennage ou de sécurité autorisé quitte l'entreprise ou le service, l'entreprise ou le service est tout de même réputé satisfaire à la condition minimale de personnel prévue dans le présent article, si les conditions suivantes sont cumulativement remplies :

1° le départ du seul dirigeant stratégique est la conséquence de :

- la rupture unilatérale du contrat de travail à durée indéterminée par l'entreprise ou le service pour motif grave ou

- la rupture unilatérale du contrat de travail à durée indéterminée sans délai de préavis par le dirigeant stratégique lui-même ou

- le décès de l'intéressé;

2° l'administration a été informée par e-mail, dans les cinq jours ouvrables, de la situation visée au 1° et des coordonnées de la personne qui est désignée comme remplaçant au sein de l'entreprise ou du service.

L'entreprise de gardiennage ou le service interne de gardiennage ou de sécurité doit à nouveau disposer d'un dirigeant stratégique dans les six mois suivant la date de début de la situation visée au 1° de l'alinéa 1er.

Art. 3. Sans préjudice d'autres exigences plus strictes prévues par la loi ou ses arrêtés d'exécution, chaque entreprise de gardiennage, service interne de gardiennage ou de sécurité doit, par activité pour laquelle il demande l'autorisation, disposer d'au moins un membre du personnel répondant aux conditions de formations correspondantes, telles que requises pour l'activité concernée en application de l'article 61, 4°, de la loi.

11° werkdag: elke dag andere dan een zaterdag, een zondag of een wettelijke feestdag;

12° minister: de minister van Binnenlandse Zaken;

13° goederenalarmsysteem : alarmsysteem bestemd om misdrijven tegen goederen te voorkomen of vast te stellen;

14° veiligheid van de informatie : bescherming van de vertrouwelijkheid, de integriteit en de beschikbaarheid van de informatie;

15° de Algemene Verordening Gegevensbescherming: de Verordening (EU) 2016/679 van het Europees Parlement en de Raad 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 (algemene verordening gegevensbescherming);

16° infrastructuur : een gebouw, een deel van een gebouw of een tijdelijke of permanente structuur die door een onderneming of dienst wordt gebruikt ter ondersteuning van haar algemene werking.

HOOFDSTUK 2. — *Vereisten voor de uitoefening van bewakingsactiviteiten*

Art. 2. § 1. De bewakingsondernemingen en de interne bewakings- en veiligheidsdiensten met minder dan 50 bewakings- of veiligheidsagenten beschikken over minstens één strategisch leidinggevende.

De bewakingsondernemingen en de interne bewakings- en veiligheidsdiensten met 50 of meer bewakings- of veiligheidsagenten beschikken over minstens twee strategisch leidinggevenden.

Het bepalen van het aantal agenten binnen een onderneming of dienst in de zin van het eerste en tweede lid, wordt gebaseerd op het totaal aantal agenten dat binnen de betrokken onderneming of dienst over een geldige identificatiekaart dient te beschikken.

§ 2. Voor de bewakingsondernemingen, natuurlijk persoon, is minstens de betrokken natuurlijke persoon strategisch leidinggevende.

Voor de bewakingsondernemingen, rechtspersoon, zijn minstens, naar gelang het geval, volgende personen strategisch leidinggevenden:

- de zaakvoerders;

- de afgevaardigde bestuurders, alsmede de andere bestuurders die ingevolge de bepalingen van de statuten van de onderneming, gemachtigd zijn om, alleen of samen met andere bestuurders, de onderneming te binden.

Voor de interne bewakings- en veiligheidsdiensten zijn minstens de personen die de functionele leiding uitoefenen over het geheel van de dienst strategisch leidinggevenden.

§ 3. Indien de enige strategisch leidinggevende van een vergunde bewakingsonderneming of van een vergunde interne bewakings- of veiligheidsdienst de onderneming of dienst verlaat, wordt de onderneming of dienst toch geacht te voldoen aan de in dit artikel voorziene minimale personeelsvoorwaarde, indien volgende voorwaarden cumulatief vervuld zijn:

1° het vertrek van de enige strategisch leidinggevende is het gevolg van :

- de eenzijdige beëindiging van de arbeidsovereenkomst van onbepaalde duur door de onderneming of dienst omwille van een dringende reden of

- de eenzijdige beëindiging van de arbeidsovereenkomst van onbepaalde duur zonder opzeggingstermijn door de strategisch leidinggevende zelf of

- het overlijden van de betrokkene;

2° de administratie werd binnen de vijf werkdagen per e-mail in kennis gesteld van de situatie bedoeld onder 1° en van de contactgegevens van de persoon die als waarnemer wordt aangeduid binnen de onderneming of dienst.

Binnen de zes maanden na de datum van aanvang van de situatie bedoeld onder 1° van het eerste lid, dient de bewakingsonderneming of de interne bewakings- of veiligheidsdienst terug te beschikken over een strategisch leidinggevende.

Art. 3. Onverminderd andere hogere vereisten in de wet of haar uitvoeringsbesluiten, dient elke bewakingsonderneming, interne bewakings- of veiligheidsdienst, per activiteit waarvoor ze de vergunning aanvraagt, te beschikken over minstens één personeelslid dat voldoet aan de opleidingsvoorwaarden die, in uitvoering van artikel 61, 4°, van de wet, specifiek vereist zijn voor de betreffende activiteit.

Pour toute mission de gardiennage qu'elle exerce, chaque entreprise de gardiennage doit pouvoir fournir le nombre minimum de membres du personnel et de moyens nécessaire pour garantir la continuité des activités à exercer.

Art. 4. Les infrastructures des entreprises de gardiennage, services internes de gardiennage et services de sécurité sont au minimum protégées par :

1° un système d'alarme pour les biens qui fonctionne correctement;

2° un système de contrôle d'accès.

Les entreprises de gardiennage ont l'obligation supplémentaire de relier le système d'alarme visé à l'alinéa 1er, 1°, à une centrale d'alarme autorisée.

Art. 5. Les données de service concernant le personnel, les données concernant d'éventuels clients et les lieux où les activités professionnelles sont exercées ainsi que toutes autres données confidentielles sont conservées à un siège d'exploitation de l'entreprise de gardiennage ou de l'entreprise qui organise le service interne de gardiennage ou de sécurité, ayant été notifié à l'administration.

Art. 6. Aux endroits tels que visés à l'article 5, les entreprises de gardiennage, les services internes de gardiennage et les services de sécurité disposent d'un local séparé fermé à clé où les documents et données visés dans cet article sont conservés.

Art. 7. Les entreprises de gardiennage et les services internes de gardiennage et de sécurité disposent d'un système de sécurisation des documents et données visés à l'article 5 qui est adapté au mode de conservation.

Le système de sécurité doit empêcher que des personnes non autorisées ne puissent accéder à ces dossiers et données.

L'infrastructure informatique pour la conservation digitale des données est protégée contre tout risque connu d'intrusion individuelle et contre l'accès non autorisé aux informations qu'elle contient. A cet effet, elle est sécurisée de manière à ce que toute forme d'intrusion individuelle ou d'accès non autorisé aux fichiers soit détectée. Dans le cas d'une telle détection, les contremesures nécessaires, parmi lesquelles les alertes, doivent immédiatement pouvoir être prises. Ce système de sécurisation fonctionne de manière autonome vis-à-vis des systèmes informatiques utilisés pour la conservation digitale des données.

Art. 8. Les entreprises de gardiennage et services internes de gardiennage et de sécurité établissent et mettent en œuvre un plan de sécurité de l'information adapté au contexte de l'entreprise et conforme aux dispositions de la loi, du présent arrêté et du Règlement Général sur la Protection des Données.

L'entreprise de gardiennage ou le service interne forme ses collaborateurs aux dispositions de ce plan de sécurité de l'information, les sensibilise à l'importance du respect des procédures et prévoit un dispositif de mesures et sanctions applicables en cas de non- respect des procédures.

Ce plan de sécurité de l'information comprendra entre autres:

- des procédures assurant la protection des informations contenues dans les messages électroniques;

- des procédures assurant une protection contre la perte de données;

- des procédures assurant une protection contre les logiciels malveillants (anti-virus à jour, firewall,...);

- une politique de gestion de l'accès des utilisateurs limitant l'accès aux systèmes et services aux utilisateurs autorisés et prévenant un accès non autorisé;

- une politique relative aux mots de passe adéquate;

- des procédures protégeant l'accès aux serveurs;

- des procédures protégeant l'accès au réseau;

- des procédures de protection des postes de travail;

- des procédures relatives à la classification des informations d'après leur valeur ou leur caractère critique ou sensible en cas de modification ou de divulgation non autorisée et aux conséquences de la classification.

Art. 9. Les entreprises de gardiennage et les services internes de gardiennage et de sécurité disposent d'un numéro de téléphone général auquel un représentant de l'entreprise ou du service peut être joint les jours ouvrables pendant les heures de bureau.

Elke bewakingsonderneming dient gedurende elke bewakingsopdracht die ze uitvoert het minimum aantal personeelsleden en middelen te kunnen leveren noodzakelijk om de continuïteit van de uit te oefenen activiteiten te garanderen.

Art. 4. De infrastructuren van bewakingsondernemingen, interne bewakingsdiensten en veiligheidsdiensten zijn minimaal beveiligd door middel van:

1° een correct functionerend goederenalarmsysteem;

2° een systeem van toegangscontrole.

De bewakingsondernemingen hebben de bijkomende verplichting om het alarmsysteem zoals bedoeld in het eerste lid, 1°, aan te sluiten op een vergunde alarmcentrale.

Art. 5. De dienstgegevens over personeel, de gegevens over eventuele klanten en plaatsen waar de beroepsactiviteiten worden uitgeoefend en alle andere vertrouwelijke gegevens worden bewaard op een bij de administratie aangemelde exploitatiezetel van de bewakingsonderneming of van de onderneming die de interne bewakings- of veiligheidsdienst organiseert.

Art. 6. Op de plaatsen bedoeld in artikel 5 beschikken de bewakingsondernemingen, de interne bewakings- en veiligheidsdiensten over een afzonderlijk afgesloten lokaal waar de documenten en gegevens bedoeld in dit artikel bewaard worden.

Art. 7. De bewakingsondernemingen en de interne bewakings- en veiligheidsdiensten beschikken over een aan de bewaringswijze aangepast systeem voor het beveiligen van de gegevens en documenten bedoeld in artikel 5.

Het beveiligingssysteem moet voorkomen dat personen die daartoe niet gerechtigd zijn toegang kunnen verkrijgen tot deze dossiers en gegevens.

De informatica-infrastructuur voor de digitale bewaring van gegevens is beschermd tegen elk bekend risico van individuele indringing en tegen ongeoorloofde toegang tot de informatie die ze bevat. Daartoe is ze beveiligd op een wijze zodat iedere vorm van individuele indringing of ongeoorloofde toegang tot de bestanden wordt gedetecteerd. In geval van een dergelijke detectie, dienen onmiddellijk de nodige tegenmaatregelen, waaronder alarmeringen, genomen te kunnen worden. Dit beveiligingssysteem functioneert autonoom ten aanzien van de informaticasystemen gebruikt voor de digitale bewaring van deze gegevens.

Art. 8. De bewakingsondernemingen en interne bewakings- en veiligheidsdiensten zorgen voor het opstellen en het uitvoeren van een informatieveiligheidsplan dat aangepast is aan de context van de onderneming en dat conform de bepalingen van de wet, van dit besluit en van de Algemene Verordening Gegevensbescherming is.

De bewakingsonderneming of de interne dienst leert haar medewerkers de bepalingen van dit informatieveiligheidsplan aan, sensibiliseert hen voor het belang van de inachtneming van de procedures en voorziet in een dispositief van maatregelen en sancties die van toepassing zijn in geval van niet-naleving van de procedures.

Dit informatieveiligheidsplan zal onder andere het volgende omvatten:

- procedures voor de bescherming van de informatiegegevens in elektronische berichten;

- procedures voor de bescherming tegen het verlies van gegevens;

- procedures voor de bescherming tegen malware (bijgewerkte antivirus, firewall,...);

- een beleid inzake het beheer van de toegang van de gebruikers waarbij de toegang tot de systemen en diensten voorbehouden wordt voor de gemachtigde gebruikers en een niet-gemachtigde toegang voorkomen wordt;

- een geschikt beleid met betrekking tot wachtwoorden;

- procedures voor de bescherming van de toegang tot de servers;

- procedures voor de bescherming van de toegang tot het netwerk;

- procedures voor de bescherming van de werkposten;

- procedures met betrekking tot de classificatie van de informatiegegevens volgens hun waarde of hun kritieke of gevoelige aard in geval van wijziging of niet-toegestane verspreiding en met betrekking tot de gevolgen van de classificatie.

Art. 9. De bewakingsondernemingen en de interne bewakings- en veiligheidsdiensten beschikken over een algemeen telefoonnummer waar men op de werkdagen tijdens de kantooruren een vertegenwoordiger van de onderneming of dienst kan bereiken.

Art. 10. Les entreprises de gardiennage et les services internes de gardiennage et de sécurité disposent d'une connexion et de l'équipement nécessaire pour pouvoir recevoir, conserver et envoyer des documents par e-mail.

Ils disposent également d'une adresse mail générale fonctionnelle à laquelle ils peuvent être contactés.

Cette adresse mail peut être utilisée comme point de contact électronique unique pour les communications avec l'entreprise ou le service concerné.

L'entreprise ou le service est supposé avoir pris connaissance du contenu de chaque communication que l'administration envoie par le biais de cette adresse mail.

Art. 11. Les entreprises de gardiennage et services internes de gardiennage et de sécurité disposent d'une propre procédure écrite pour la réception, l'enregistrement, l'analyse et le traitement de plaintes qu'ils doivent appliquer.

Cette procédure prévoit au moins que :

1° le plaignant reçoit, au plus tard dans les cinq jours ouvrables après réception de la plainte par l'entreprise ou le service, un accusé de réception contenant les coordonnées de la personne et/ou du service qui traitera la plainte;

2° une réponse doit avoir été notifiée au plaignant endéans les deux mois à dater de la réception de la plainte.

Art. 12. Les entreprises de gardiennage et les services internes de gardiennage et de sécurité peuvent uniquement faire appel à des agents de gardiennage ou de sécurité pour lesquels une assurance protection juridique a été souscrite permettant à ces agents de faire valoir leurs droits s'ils ont subi, en tant que victime d'un acte de violence, des dommages matériels ou physiques dans l'exercice de leurs activités.

CHAPITRE 3. — *Conditions pour l'exercice de l'activité de gardiennage "gestion de centrales d'alarme"*

Art. 13. Les conditions prévues au chapitre 2 sont applicables aux activités de gardiennage 'gestion de centrales d'alarme' sauf lorsqu'il y est expressément dérogé dans les dispositions qui suivent.

Pour l'application du présent chapitre, il convient d'entendre par centrale d'alarme l'entreprise visée à l'article 2, 23°, de la loi.

Si l'appel d'urgence tel que visé à l'article 2, 23°, *c)*, de la loi est un eCall privé, au sens de la loi-cadre STI, la centrale d'alarme est une centrale telle que visée à l'article 2, *d)* du règlement UE n° 305/2013.

Art. 14. Les locaux où une centrale d'alarme assure un contrôle à distance des entrées et des sorties ou reçoit et traite des signaux provenant de systèmes d'alarme destinés à constater des situations d'alarme suite à des délits contre des personnes ou des biens sont, outre ce qui est prévu à l'article 4:

1° surveillés de manière périphérique par vidéosurveillance;

2° équipés d'un système d'alarme pour les biens et pour les personnes qui, en plus d'être raccordé à la propre centrale d'alarme, l'est aussi à une autre centrale d'alarme qui fonctionne de manière autonome par rapport à la propre centrale d'alarme;

3° pourvus de plafonds et de parois dont l'extérieur est conçu pour résister à une effraction.

Art. 15. Les obligations visées aux articles 4 à 7 inclus ne s'appliquent pas aux centrales d'alarme qui sont exclusivement autorisées pour la réception et le traitement des signaux provenant de systèmes d'alarme destinés à constater des incendies, des fuites de gaz, des explosions ou des situations d'urgence de manière générale.

L'obligation visée à l'article 12 ne s'applique pas aux centrales d'alarme.

Art. 16. La centrale d'alarme dispose de l'équipement, des installations et des procédures nécessaires sur le plan informatique et de la communication pour :

1° recevoir, localiser, et analyser en temps réel les signaux, appels, images, données d'identification et de localisation des biens et des personnes surveillés par elle, vérifier leur véracité et les transférer aux centrales de gestion des appels d'urgence 112 ou aux services de police, le tout conformément à la réglementation en vigueur;

2° au cas où la réglementation en vigueur le prévoit, signaler électroniquement les systèmes d'alarme des utilisateurs raccordés chez elle;

Art. 10. De bewakingsondernemingen en de interne bewakings- en veiligheidsdiensten beschikken over een verbinding en de nodige uitrusting om documenten per e-mail te kunnen ontvangen, te bewaren en te versturen.

Ze beschikken tevens over een algemeen functioneel e-mailadres waarop ze gecontacteerd kunnen worden.

Dit e-mailadres kan door de administratie als uniek elektronisch contactpunt aangewend worden voor communicatie met de betreffende onderneming of dienst.

De onderneming of dienst wordt geacht kennis te hebben genomen van de inhoud van elke berichtgeving die de administratie via dit e-mailadres verstuurt.

Art. 11. De bewakingsondernemingen en interne bewakings- en veiligheidsdiensten beschikken over een eigen schriftelijke procedure voor de ontvangst, registratie, analyse en behandeling van klachten die zij dienen toe te passen.

Deze procedure voorziet minstens dat:

1° de klager uiterlijk binnen de vijf werkdagen, na ontvangst van de klacht door de onderneming of dienst, een ontvangstbevestiging krijgt met vermelding van de contactgegevens van de persoon en/of de dienst die de klacht zal behandelen;

2° een inhoudelijk antwoord aan de klager dient genotificeerd te worden binnen de twee maanden na ontvangst van de klacht.

Art. 12. De bewakingsondernemingen en de interne bewakings- en veiligheidsdiensten kunnen enkel gebruik maken van bewakings- of veiligheidsagenten waarvoor een rechtsbijstandsverzekering werd afgesloten die deze agenten in staat stelt hun rechten te doen gelden wanneer zij, als slachtoffer van een gewelddaad, materiële of lichamelijke schade hebben opgelopen in het kader van de uitoefening van hun activiteiten.

HOOFDSTUK 3. — *Vereisten voor de uitoefening van de bewakingsactiviteit "beheer van alarmcentrales"*

Art. 13. De voorwaarden bedoeld in hoofdstuk 2 zijn van toepassing op de bewakingsactiviteiten 'beheer van alarmcentrales' tenzij wanneer daarvan uitdrukkelijk afgeweken wordt in de volgende bepalingen.

Voor de toepassing van dit hoofdstuk wordt met een alarmcentrale bedoeld de onderneming zoals bedoeld in artikel 2, 23°, van de wet.

Indien de noodoproep zoals bedoeld in artikel 2, 23°, c, van de wet een particuliere eCall uitmaakt, in de zin van de ITS-wet, is de alarmcentrale een centrale zoals bedoeld in artikel 2, *d)* van de EU-verordening 305/2013.

Art. 14. De lokalen waar een alarmcentrale afstandscontrole van toegangen en uitgangen verzekert of signalen ontvangt en verwerkt afkomstig van alarmsystemen die bestemd zijn om alarmsituaties ingevolge misdrijven tegen personen of goederen vast te stellen, zijn, naast wat voorzien is in artikel 4:

1° periferisch bewaakt door videotoezicht;

2° uitgerust met een goederen- en persoonsalarmsysteem dat, naast op de eigen alarmcentrale, ook aangesloten is op een andere alarmcentrale dewelke autonoom functioneert ten aanzien van de eigen alarmcentrale;

3° voorzien van plafonds en wanden waarvan de buitenkant inbraakwerend is.

Art. 15. De verplichtingen bedoeld in de artikels 4 tot en met 7 zijn niet van toepassing op alarmcentrales die uitsluitend vergund zijn voor het ontvangen en het verwerken van signalen afkomstig van alarmsystemen bestemd om brand, gaslekken, ontploffingen of noodsituaties in het algemeen vast te stellen.

De verplichting bedoeld in artikel 12 is niet van toepassing op alarmcentrales.

Art. 16. De alarmcentrale beschikt over de nodige uitrusting, voorzieningen en procedures op het gebied van informatica- en communicatie die haar in staat stellen om:

1° signalen, oproepen, beelden, identificatie- en lokalisatiegegevens van de door haar bewaakte goederen en personen in reële tijd zowel te ontvangen, te lokaliseren als te analyseren en deze te verifiëren op hun waarachtigheid en door te melden aan de beheercentrales van noodoproepen 112 of de politiediensten, dit alles conform de vigerende regelgeving;

2° in geval de vigerende regelgeving hierin voorziet, de alarmsystemen van de bij haar aangesloten gebruikers, elektronisch aan te melden;

3° dans le cas visé à l'article 13, alinéa 3, la centrale d'alarme doit également satisfaire aux conditions minimales telles que visées à l'article 3, 1 à 6 inclus du règlement UE 305/2013.

Art. 17. L'infrastructure informatique où sont traitées les données d'une centrale d'alarme qui assure un contrôle à distance des entrées et des sorties ou reçoit et traite des signaux provenant de systèmes d'alarme destinés à constater des situations d'alarme suite à des délits contre des personnes ou des biens, est protégée conformément aux dispositions de l'article 7, troisième alinéa.

Art. 18. La centrale d'alarme dispose d'un journal de bord numérique où chaque alarme, signal ou appel entrant et chaque opération sont enregistrés.

Les données enregistrées dans le journal de bord numérique sont conservées pendant deux ans.

Art. 19. La centrale d'alarme dispose d'une ligne téléphonique réservée au traitement d'appels téléphoniques provenant des services de police et de secours et des centrales de gestion des appels d'urgence 112.

Art. 20. La centrale d'alarme dispose des opérateurs nécessaires pour assurer ses activités en continu avec au moins 2 opérateurs. Pour ce faire, elle possède l'équivalent d'au moins 11 opérateurs en service à temps plein.

Art. 21. La centrale d'alarme dispose des moyens techniques et des opérateurs nécessaires afin de réaliser, sur une base annuelle, les temps de réaction minimums suivants :

1° pour entamer la gestion des alarmes provenant de systèmes d'alarme destinés à constater des situations d'alarme suite à des délits contre des biens : 80% en moins de 180 secondes; 98,5% en moins de 240 secondes;

2° pour entamer la gestion des alarmes provenant de systèmes d'alarme destinés à constater des situations d'alarme suite à des délits contre des personnes, des incendies, des fuites de gaz, des explosions ou des situations d'urgence de manière générale : 80% en moins de 30 secondes; 98,5% en moins de 60 secondes;

3° pour répondre aux appels téléphoniques provenant des services de police et de secours et des centrales de gestion des appels d'urgence 112 : 80% en moins de 30 secondes et 98,5% en moins de 60 secondes;

4° pour répondre aux appels téléphoniques autres que ceux visés au 3° : 80% en moins de 60 secondes.

La centrale d'alarme peut, sur la base des données du journal de bord numérique visé à l'article 18, prouver que, par année civile, ces temps de réaction minimums sont réalisés.

Art. 22. La centrale d'alarme dispose des moyens, des procédures et des équipements nécessaires pour garantir la continuité de ses activités. Pour ce faire, elle dispose au moins :

1° des dispositifs d'urgence au niveau informatique, de l'approvisionnement en énergie et de la communication, qui garantissent le fonctionnement de la centrale pendant au moins 72 heures;

2° d'un plan d'urgence d'avertissement des clients, des utilisateurs, des services de police et de secours, si la centrale d'alarme ne pourra pas fonctionner pendant 24 heures ou plus.

Art. 23. Les centrales d'alarme qui traitent des appels d'urgence qui sont un eCall privé au sens de la loi-cadre STI, satisfont aux dispositions du présent arrêté et à la norme EN 16454.

Si la norme EN16454 contient des dispositions plus strictes que celles prévues dans le présent arrêté, les règles les plus strictes sont d'application.

CHAPITRE 4. — *Evaluation de la conformité*

Art. 24. Les entreprises de gardiennage, les services internes de gardiennage et les services de sécurité doivent, pour l'obtention ou le renouvellement d'une autorisation, prouver la conformité aux dispositions du présent arrêté par le biais d'un rapport de contrôle de la conformité remis par un organisme d'inspection désigné par le ministre.

A cette fin, ils introduisent eux-mêmes une demande auprès de l'organisme d'inspection.

Art. 25. L'évaluation de la conformité réalisée par l'organisme d'inspection porte sur le respect par l'entreprise de gardiennage, le service interne de gardiennage ou le service de sécurité concerné des articles 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 16 à 23 inclus. Le cas échéant, l'évaluation de la conformité porte également sur le respect des normes auxquelles doivent répondre les centraux d'appel, telles que fixées par le Roi en exécution de l'article 89 de la loi.

3° in het geval, bedoeld in artikel 13, derde lid, dient de alarmcentrale bovendien te voldoen aan de minimale vereisten zoals bedoeld in artikel 3, 1 tot en met 6 van de EU-verordening 305/2013.

Art. 17. De informatica-infrastructuur waar gegevens worden verwerkt van een alarmcentrale die afstandscontrole van toegangen en uitgangen verzekert of signalen ontvangt en verwerkt afkomstig van alarmsystemen die bestemd zijn om alarmsituaties ingevolge misdrijven tegen personen of goederen vast te stellen, is beschermd overeenkomstig hetgeen bepaald is in artikel 7, derde lid.

Art. 18. De alarmcentrale beschikt over een digitaal logboek waarin elk binnenkomend alarm, signaal of oproep en elke operatorhandeling is geregistreerd.

De gegevens opgenomen in het digitaal logboek worden gedurende twee jaar bewaard.

Art. 19. De alarmcentrale beschikt over een gereserveerde telefoonlijn voor de behandeling van telefonische oproepen, afkomstig van politie- en hulpdiensten en beheercentrales van noodoproepen 112.

Art. 20. De alarmcentrale beschikt over de nodige operatoren om haar activiteiten op een volcontinue wijze te verzekeren met minstens 2 operatoren. Hiertoe heeft ze minstens een equivalent van 11 voltijdse operatoren in dienst.

Art. 21. De alarmcentrale beschikt over de nodige technische middelen en operatoren teneinde, op jaarbasis, volgende minimale reactietijden te realiseren:

1° voor de aanvang van de behandeling van alarmen afkomstig van alarmsystemen die bestemd zijn om alarmsituaties ingevolge misdrijven tegen goederen vast te stellen: 80% in minder dan 180 seconden; 98,5 % in minder dan 240 seconden;

2° voor de aanvang van de behandeling van alarmen, afkomstig van alarmsystemen die bestemd zijn om alarmsituaties ingevolge misdrijven tegen personen, brand, gaslekken, ontploffingen of noodsituaties in het algemeen vast te stellen : 80% in minder dan 30 seconden; 98,5 % in minder dan 60 seconden;

3° voor het beantwoorden van telefonische oproepen afkomstig van politie- en hulpdiensten en de beheercentrales van noodoproepen 112 : 80% in minder 30 seconden en 98,5 % in minder 60 seconden;

4° voor het beantwoorden van telefonische oproepen, andere dan deze bedoeld onder 3°: 80% in minder dan 60 seconden.

De alarmcentrale kan op basis van de gegevens uit het digitaal logboek, bedoeld in artikel 18, aantonen dat, per kalenderjaar deze minimale reactietijden zijn gerealiseerd.

Art. 22. De alarmcentrale beschikt over de nodige middelen, procedures en materialen om de continuïteit van haar activiteiten te waarborgen. Daartoe beschikt ze minstens:

1° over noodvoorzieningen inzake informatica, energiebevoorrading en communicatie die de werking van de alarmcentrale waarborgt gedurende minstens 72 uur;

2° een noodplan van verwittiging van klanten, gebruikers, politie- en hulpdiensten indien de alarmcentrale niet kan functioneren gedurende 24 uur of langer.

Art. 23. De alarmcentrales die noodoproepen behandelen die een particuliere eCall in de zin van de ITS-kaderwet uitmaken, voldoen aan de bepalingen van dit besluit en de norm EN 16454.

In geval de norm EN16454 strengere bepalingen bevat dan deze voorzien in dit besluit, gelden deze strengere bepalingen.

HOOFDSTUK 4. — *Conformiteitsbeoordeling*

Art. 24. De bewakingsondernemingen, interne bewakings- en veiligheidsdiensten dienen, voor het bekomen of het vernieuwen van een vergunning, de conformiteit aan de bepalingen uit dit besluit aan te tonen door middel van een verslag van conformiteitsbeoordeling afgeleverd door een door de minister aangewezen inspectieinstelling.

Hiervoor dienen ze zelf een aanvraag in bij de inspectieinstelling.

Art. 25. De conformiteitsbeoordeling uitgevoerd door de inspectieinstelling heeft betrekking op de naleving van de artikels 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 16 tot en met 23 door de betreffende bewakingsonderneming, interne bewakingsdienst of veiligheidsdienst. Desgevallend heeft de conformiteitsbeoordeling ook betrekking op de naleving van de normen waaraan de oproepcentrales dienen te voldoen, zoals bepaald door de Koning in uitvoering van de artikel 89 van de wet.

Dans le cas visé à l'article 13, alinéa 3, l'évaluation de la conformité se fonde également, en vertu du règlement UE n° 305/2013, sur la norme EN 16454 ("Intelligent transport systems – eSafety – eCall end to end conformance testing").

Art. 26. L'organisme d'inspection transmet, dans les 14 jours qui suivent la fin de l'évaluation de la conformité, l'original de son rapport au mandant et un duplicata à l'administration.

Le rapport de contrôle de la conformité visé à l'alinéa 1er est établi conformément au modèle fixé par le ministre.

Art. 27. Le rapport visé à l'article 26 est uniquement valable si :

1° l'évaluation de la conformité qu'il contient a trait à la situation actuelle, à la date d'introduction de la demande d'autorisation ou de renouvellement d'autorisation, des moyens organisationnels, techniques et d'infrastructure;

2° à la date d'introduction de la demande d'obtention ou de renouvellement de l'autorisation, il ne date pas de plus de 6 mois.

Art. 28. L'administration peut à tout moment au cours de la période d'autorisation demander un rapport de contrôle de la conformité complémentaire à un organisme d'inspection afin de vérifier si l'entreprise de gardiennage ou le service interne de gardiennage ou de sécurité répond encore toujours aux normes minimales fixées dans le présent arrêté.

Art. 29. L'organisme d'inspection détruit toutes les données et documents récoltés à l'occasion de l'inspection dès que la décision concernant la demande d'autorisation ou de renouvellement d'autorisation est devenue définitive. Dans le cas visé à l'article 28, les données et documents sont détruits dès que l'administration a donné son autorisation à cet effet.

Art. 30. Les coûts liés à la mission de l'organisme d'inspection sont à charge du demandeur.

Art. 31. Pour être agréé comme organisme d'inspection par le ministre, l'organisme doit être établi dans l'Espace économique européen et adresser une demande à l'administration. Cette demande doit être accompagnée de la preuve que l'organisme est accrédité sur la base de la norme EN ISO/IEC 17020 par le système d'accréditation de l'Etat membre ou du pays membre de l'Association européenne de libre-échange dans lequel il est établi, conformément au règlement (CE) n° 765/2008 du Parlement européen et du Conseil et à l'article VIII.30 du Code de droit économique.

Pour être agréé en tant qu'organisme d'inspection, l'organisme doit satisfaire aux conditions suivantes :

- être un organisme d'inspection de type A, tel que visé dans la norme EN-ISO/IEC 17020. Il ne peut d'aucune manière avoir des intérêts dans le secteur de la sécurité privée et particulière;

- disposer d'au moins un inspecteur qui satisfait aux conditions visées à l'alinéa 5.

L'agrément visé à l'alinéa premier est valable cinq ans et peut être renouvelé pour une même durée.

Les organismes d'inspection et leurs inspecteurs réalisent leurs missions en totale impartialité et neutralité.

Les inspecteurs de l'organisme d'inspection désignés pour réaliser des inspections relatives au présent arrêté doivent au moins répondre aux conditions suivantes :

1° satisfaire à l'article 61, 1°, 2° et 5°, de la loi;

2° disposer des habilitations, attestations et avis nécessaires pour pouvoir effectuer la mission demandée, conformément à la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

3° ne pas avoir fait partie, au cours des cinq dernières années, du secteur de la sécurité privée et particulière ou d'une de ses organisations professionnelles ou représentatives des travailleurs;

4° ne pas avoir fait l'objet, au cours des cinq dernières années, d'une décision par laquelle il a été constaté qu'ils ne satisfaisaient pas aux conditions de sécurité visées à l'article 61, 6°, de la loi;

5° avoir connaissance du présent arrêté et, le cas échéant, de l'arrêté royal du 25 avril 2007 fixant les conditions d'installation, d'entretien et d'utilisation des systèmes d'alarme et de gestion de centraux d'alarme et de la norme EN 16454 ("Intelligent transport systems – eSafety – eCall end tot end conformance testing").

In het geval, bedoeld in artikel 13, derde lid, is, ingevolge de EU-verordening 305/2013, de conformiteitsbeoordeling tevens gebaseerd op de EN-norm 16454 ("Intelligent transport systems – eSafety – eCall end to end conformance testing").

Art. 26. De inspectieinstelling maakt, binnen de 14 dagen na het beëindigen van de conformiteitsbeoordeling, het origineel van haar verslag over aan de opdrachtgever en een duplicaat aan de administratie.

Het verslag van conformiteitsbeoordeling bedoeld in het eerste lid wordt opgesteld conform het model bepaald door de minister.

Art. 27. Het verslag bedoeld in artikel 26, is slechts geldig voor zover:

1° de conformiteitsbeoordeling die het bevat betrekking heeft op de, op datum van het indienen van de aanvraag tot het bekomen of de vernieuwing van de vergunning, actuele situatie van de organisatorische, technische en infrastructurele middelen;

2° het, op de datum van het indienen van de aanvraag tot het bekomen of de vernieuwing van de vergunning, niet ouder is dan zes maanden.

Art. 28. De administratie kan op elk moment tijdens de vergunningsperiode een bijkomend verslag van conformiteitsbeoordeling vragen aan een inspectieinstelling teneinde na te gaan of de bewakingsonderneming of de interne bewakings- of veiligheidsdienst nog steeds voldoet aan de minimumnormen bepaald in dit besluit.

Art. 29. De inspectieinstelling vernietigt alle gegevens en documenten die werden vergaard naar aanleiding van haar inspectie van zodra de beslissing omtrent de aanvraag tot vergunning of vernieuwing van de vergunning definitief geworden is. In het geval bedoeld in artikel 28 worden de gegevens en documenten vernietigd van zodra de administratie hiertoe haar toestemming gegeven heeft.

Art. 30. De kosten verbonden aan de opdracht van de inspectieinstelling zijn ten laste van de aanvrager.

Art. 31. Om als inspectieinstelling te worden erkend door de minister dient de instelling gevestigd te zijn binnen de Europese Economische Ruimte en een aanvraag te richten aan de administratie. Deze aanvraag moet vergezeld zijn van het bewijs dat de instelling geaccrediteerd is op basis van de norm EN ISO/IEC 17020 door het accreditatiesysteem van de lidstaat of het land van de Europese Vrijhandelsassociatie waarbinnen het is gevestigd, conform de verordening (EG) Nr. 765/2008 van het Europees Parlement en de Raad en artikel VIII.30 van het Wetboek van economisch recht.

Om te worden erkend als inspectieinstelling, moet de instelling voldoen aan volgende voorwaarden :

- een inspectieinstelling type A zijn, zoals bedoeld in de norm EN-ISO/IEC 17020. Deze mag op geen enkele wijze belangen hebben in de sector van de private en bijzondere veiligheid;

- beschikken over minstens één inspecteur die voldoet aan de voorwaarden bedoeld in het vijfde lid.

De in het eerste lid beoogde erkenning is vijf jaar geldig en kan worden vernieuwd voor een zelfde periode.

De inspectieinstellingen en hun inspecteurs voeren hun opdrachten volkomen onpartijdig en neutraal uit.

De inspecteurs van de inspectieinstelling die werden aangewezen om inspecties met betrekking tot dit besluit uit te voeren, moeten op zijn minst voldoen aan de volgende voorwaarden:

1°voldoen aan de bepalingen van artikel 61, 1°, 2° en 5°, van de wet;

2° beschikken over de nodige machtigingen, attesten of adviezen om, conform de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, de gevraagde opdracht te kunnen uitvoeren;

3° de voorbije vijf jaar geen deel hebben uitgemaakt van de sector van de private en bijzondere veiligheid of van één van haar beroeps- of werknemersorganisaties;

4° in de afgelopen vijf jaar niet het voorwerp hebben uitgemaakt van een beslissing waarbij werd vastgesteld dat zij aan veiligheidsvoorwaarden, bedoeld in artikel 61, 6°, van de wet, niet voldeden;

5° kennis hebben van dit besluit en, in voorkomend geval, van het koninklijk besluit tot wijziging van het koninklijk besluit van 25 april 2007 tot vaststelling van de voorwaarden voor installatie, onderhoud en gebruik van alarmsystemen en beheer van alarmcentrales en van de norm EN 16454 ("Intelligent transport systems – eSafety – eCall end tot end conformance testing").

CHAPITRE 5. — *Dispositions finales*

Art. 32. L'arrêté royal du 14 mai 1991 relatif à l'équipement technique des entreprises de gardiennage et des services internes de gardiennage est abrogé.

Art. 33. L'arrêté royal du 20 mars 2017 relatif au nombre minimum de personnel et aux moyens organisationnels, techniques et d'infrastructure pour l'exercice de l'activité de gardiennage de gestion de centraux d'alarme est abrogé.

Art. 34. § 1er. Le présent arrêté entre en vigueur dix jours après sa publication au *Moniteur belge*, à l'exception de l'article 24 qui entre en vigueur six mois après la publication, au *Moniteur belge*, de la désignation du premier organisme d'inspection.

§ 2. Les entreprises de gardiennage et les services interne de gardiennage et de sécurité qui sont en possession, à la date d'entrée en vigueur du présent arrêté, d'une autorisation telle que visée à l'article 16 de la loi, disposent d'un délai de 6 mois après la publication du présent arrêté pour répondre aux obligations visées aux articles 2, § 1er, alinéa 2, 7 et 17.

Ils disposent d'un délai de deux mois après la publication du présent arrêté pour répondre aux obligations prévues aux articles 4 et 12.

Art. 35. Le ministre qui a l'Intérieur dans ses attributions est chargé de l'exécution du présent arrêté.

Donné à Bruxelles, le 25 avril 2021.

PHILIPPE

Par le Roi :

La Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau Démocratique,
A. VERLINDEN

HOOFDSTUK 5. — *Slotbepalingen*

Art. 32. Het koninklijk besluit van 14 mei 1991 betreffende de technische uitrusting van bewakingsondernemingen en interne bewakingsdiensten wordt opgeheven.

Art. 33. Het koninklijk besluit van 20 maart 2017 betreffende de minimumvereisten inzake personeel en organisatorische, technische en infrastructurele middelen voor de uitoefening van de bewakingsactiviteiten beheer van alarmcentrales wordt opgeheven.

Art. 34. § 1. Dit besluit treedt in werking tien dagen na de publicatie ervan in het *Belgisch Staatsblad*, met uitzondering van artikel 24 dat in werking treedt zes maanden na de publicatie van de aanstelling van de eerste inspectieinstelling in het *Belgisch Staatsblad*.

§ 2. De bewakingsondernemingen en de interne bewakings- en veiligheidsdiensten die op de datum van inwerkingtreding van dit besluit in het bezit zijn van een vergunning, zoals bedoeld in artikel 16 van de wet, beschikken over een termijn van 6 maanden na publicatie van dit besluit om tegemoet te komen aan de verplichtingen bedoeld in de artikels 2, § 1, tweede lid, 7 en 17.

Ze beschikken over een termijn van twee maanden na publicatie van dit besluit om tegemoet te komen aan de verplichtingen bedoeld in de artikels 4 en 12.

Art. 35. De minister bevoegd voor Binnenlandse Zaken is belast met de uitvoering van dit besluit.

Gegeven te Brussel, 25 april 2021.

FILIP

Van Koningswege :

De Minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing,
A. VERLINDEN

SERVICE PUBLIC FEDERAL INTERIEUR ET SERVICE PUBLIC FEDERAL JUSTICE

[C − 2021/21510]

11 JUILLET 2021. — Arrêté royal modifiant l'arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, l'article 93, § 3;

Vu l'arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale;

Vu l'avis de l'Inspecteur général des Finances, donné le 13 novembre 2020;

Vu l'accord de la Ministre de la Fonction publique, donné le 27 mai 2021;

Vu l'accord de la Secrétaire d'Etat au Budget, donné le 9 juin 2021;

Vu l'avis n° 68.116/2 du Conseil d'Etat, donné le 26 octobre 2020, en application de l'article 84, § 1er, alinéa 1er, 2°, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973;

Sur la proposition de la Ministre de l'Intérieur et du Ministre de la Justice,

Nous avons arrêté et arrêtons :

Article 1er. L'article 11, 2°, de l'arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale, remplacé par l'arrêté royal du 23 août 2014, est remplacé par ce qui suit :

"2° la direction centrale de la police technique et scientifique, dont le laboratoire doit être accrédité, pour ce qui concerne les activités en matière de données dactyloscopiques, conformément aux critères de la norme NBN EN ISO/IEC 17025, selon les procédures et conditions de l'accréditation telles que déterminées par l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité;".

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN EN FEDERALE OVERHEIDSDIENST JUSTITIE

[C − 2021/21510]

11 JULI 2021. — Koninklijk besluit tot wijziging van het koninklijk besluit van 14 november 2006 betreffende de organisatie en de bevoegdheden van de federale politie

FILIP, Koning der Belgen,

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

Gelet op de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, artikel 93, § 3;

Gelet op het koninklijk besluit van 14 november 2006 betreffende de organisatie en de bevoegdheden van de federale politie;

Gelet op het advies van de Inspecteur-generaal van Financiën, gegeven op 13 november 2020;

Gelet op de akkoordbevinding van de Minister van Ambtenarenzaken, d.d. 27 mei 2021;

Gelet op de akkoordbevinding van de Staatssecretaris voor Begroting, d.d. 9 juni 2021;

Gelet op advies nr. 68.116/2 van de Raad van State, gegeven op 26 oktober 2020, met toepassing van artikel 84, § 1, eerste lid, 2°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Op de voordracht van de Minister van Binnenlandse Zaken en van de Minister van Justitie,

Hebben Wij besloten en besluiten Wij :

Artikel 1. Artikel 11, 2°, van het koninklijk besluit van 14 november 2006 betreffende de organisatie en de bevoegdheden van de federale politie, vervangen bij het koninklijk besluit van 23 augustus 2014, wordt vervangen als volgt:

"2° de centrale directie van de technische en wetenschappelijke politie, waarvan het laboratorium voor wat betreft activiteiten inzake dactyloscopische gegevens geaccrediteerd moet zijn in overeenstemming met de criteria van de norm NBN EN ISO/IEC 17025 en dit volgens de procedures en voorwaarden voor accreditatie vastgelegd in het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling;".