

Mindestanzahl von Krediten enthält, erneut angewandt werden konnte. Daraus ergibt sich, dass nur der Vorteil von zwei zusätzlichen Einschreibungen für die Studierenden, die sich zu Beginn des akademischen Jahres 2024-2025 nach einer zweiten Einschreibung im ersten Zyklus neu orientiert haben, für sie eine berechnete Erwartung für das nächste akademische Jahr darstellt. Der Dekretgeber hat dieser berechtigten Erwartung ohne objektive und sachliche Rechtfertigung Abbruch getan.

B.11. Am 25. April 2025 hat die Ministerpräsidentin der Französischen Gemeinschaft im Parlament Folgendes erklärt:

« Mon cabinet a déjà donné la consigne aux commissaires et délégués du gouvernement auprès des établissements d'enseignement supérieur – universités, hautes écoles et écoles supérieures des arts (ESA) – de préserver les droits acquis par les étudiants, pour leur réorientation en 2024-2025, après deux inscriptions dans le premier cycle » (*Parl. Dok.*, Parlement der Französischen Gemeinschaft, Ausschuss für Haushalt, Hochschulwesen und Schulgebäude, 2024–2025, CRIC Nr. 76, S. 24).

Diese Richtlinie wurde anschließend in ihrer Fassung vom Mai 2025 den Hochschuleinrichtungen durch das Vereinigte Kollegium der Kommissare und Beauftragten der Regierung bei den Universitäten, den Hochschulen und den Kunsthochschulen mitgeteilt:

« [...] les étudiants de premier cycle ayant bénéficié de deux inscriptions supplémentaires pour rencontrer les différentes balises prévues à l'article 5 du présent Décret continueront à en bénéficier, à condition qu'ils se soient réorientés après une deuxième inscription au minimum, soit au début de l'année académique 2024-2025, soit au cours de cette même année. Ce droit sera cependant perdu en cas de nouvelle réorientation et/ou d'interruption » (« Vade-mecum du Collège réuni des Commissaires et Délégués du Gouvernement près les Universités, les Hautes Écoles et les Écoles supérieures des Arts », Mai 2025, S. 8).

B.12. Die angefochtenen Bestimmungen verstoßen gegen die Artikel 10 und 11 der Verfassung in Verbindung mit dem Grundsatz des berechtigten Vertrauens, indem sie keine Übergangsregelung für Studierende vorsehen, die sich zu Beginn des akademischen Jahres 2024-2025 nach einer zweiten Einschreibung im ersten Zyklus neu orientiert haben.

B.13.1. Der zweite Klagegrund betrifft anschließend die Situation der Studierenden, die sich 2024-2025 ein drittes Mal in einem ersten Ausbildungsweg eingeschrieben haben. Diese können sich zu Beginn des akademischen Jahres 2025-2026 nicht neu orientieren, weil sie in Anwendung von Artikel 5 § 2 des Dekrets vom 2. Dezember 2021, um finanzierbar zu sein, mindestens 50 Erstkredite ihres Kurses am Ende von höchstens drei Einschreibungen im Zyklus erwerben oder in Wert setzen müssen.

B.13.2. Im Gegensatz zu dem, was die klagende Partei behauptet, konnten sich die Studierenden, die sich 2024-2025 ein drittes Mal in einem ersten Ausbildungsweg eingeschrieben haben, nicht darauf verlassen, noch in den Vorteil einer Einschreibung zu gelangen, um sich 2025-2026 neu zu orientieren. Obwohl Artikel 2 des Dekrets vom 31. Mai 2024 sich tatsächlich auf diese Studierenden bezog, indem sie als « finanzierbar im Hinblick auf ihre Einschreibung im selben Kursus während des akademischen Jahres 2024-2025 » angesehen wurden, bezog sich Artikel 5 desselben Dekrets nämlich nicht auf sie, da dieser die sich neu orientierenden Studierenden betraf. Wie in B.10 erwähnt wurde, betraf das Dekret vom 31. Mai 2024 insbesondere diese Kategorie von Studierenden. Außerdem wies es eine zeitliche Begrenzung auf ein Jahr auf, bevor das Dekret vom 2. Dezember 2021, das die Bedingungen des Erwerbs oder der Inwertsetzung einer Mindestanzahl von Krediten enthält, erneut angewandt werden konnte.

B.13.3. Demzufolge hat das Dekret vom 31. Mai 2024 für die Studierenden, die sich 2024-2025 ein drittes Mal in einem ersten Ausbildungsweg eingeschrieben haben, zu keinem Zeitpunkt die berechnete Erwartung entstehen lassen, sich 2025-2026 neu orientieren zu können, weshalb das Nichtvorhandensein einer Übergangsregelung für sie nicht gegen die Artikel 10, 11 und 24 § 4 der Verfassung verstößt.

Aus diesen Gründen:

Der Gerichtshof

1. erklärt die Artikel 53 und 67 des Programmdekrets der Französischen Gemeinschaft vom 11. Dezember 2024 « zur Festlegung verschiedener Bestimmungen in Bezug auf Unterricht, Schulgebäude, Forschung und Kultur » für nichtig, insofern sie keine Übergangsregelung für Studierende vorsehen, die sich zu Beginn des akademischen Jahres 2024-2025 nach einer zweiten Einschreibung im ersten Zyklus neu orientiert haben;

2. weist die Klage im Übrigen zurück.

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 25. Juni 2026.

Der Kanzler,

Frank Meererschaut

Der Präsident,

Pierre Nihoul

FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER
EN FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN

[2026/202297]

15 SEPTEMBER 2026. — Koninklijk besluit tot wijziging van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België

VERSLAG AAN DE KONING

Sire,

Het ontwerp van koninklijk besluit dat wij ter ondertekening aan Uwe Majesteit voorleggen beoogt de wijziging van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, ter uitvoering van de artikelen 37, 107, tweede lid, en 108 van de Grondwet, en van artikel 4, eerste lid van Verordening (EU) 2025/38 van het Europees Parlement en de Raad van 19 december 2024 tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren en tot wijziging van Verordening (EU) 2021/694 (hierna de "Verordening cybersolidariteit").

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE
ET SERVICE PUBLIC FEDERAL INTERIEUR

[2026/202297]

15 SEPTEMBRE 2026. — Arrêté royal modifiant l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cyberécurité Belgique

RAPPORT AU ROI

Sire,

Le projet d'arrêté royal que nous avons l'honneur de soumettre à la signature de Votre Majesté vise à modifier l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cyberécurité Belgique, en exécution des articles 37, 107, alinéa 2, et 108 de la Constitution et de l'article 4, alinéa 1^{er} du Règlement (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694 (ci-après le « Règlement sur la cybersolidarité »).

De Verordening cybersolidariteit is in januari 2025 in werking getreden. Artikel 4, eerste lid, bepaalt dat elke lidstaat die besluit deel te nemen aan het Europees waarschuwingssysteem voor cyberveiligheid, een nationale cyberhub moet aanwijzen.

Het is belangrijk dat België deelneemt aan dit Europees waarschuwingssysteem voor cyberveiligheid, om de opsporing, analyse en verwerking van gegevens over cyberdreigingen en de preventie van incidenten in ons land te verbeteren.

Artikel 108 van de Grondwet bepaalt dat de Koning de verordeningen maakt en de besluiten neemt die voor de uitvoering van de wetten nodig zijn.

In het kader van zijn veiligheidsbeleid, voorziet het federaal regeerakkoord 2025-2029 van de regering in een logische hergroepering van alle veiligheidsbevoegdheden bij de Minister van Veiligheid en Binnenlandse Zaken.

Het CCB staat momenteel onder het gezag van de Eerste Minister en geniet administratieve en logistieke ondersteuning van de FOD Kanselarij van de Eerste Minister.

Dit ontwerp van koninklijk besluit heeft tot doel de uitvoering van de Verordening cybersolidariteit, door het CCB als nationale cyberhub aan te wijzen.

Ten tweede beoogt dit ontwerp van koninklijk besluit ook te verzekeren dat het CCB over de nodige operationele onafhankelijkheid beschikt om zijn toezichthoudende taken uit te voeren in overeenstemming met de vereisten van de NIS2-wet.

Ten slotte heeft dit ontwerp van koninklijk besluit tot doel de aanpak die in het federaal regeerakkoord is beschreven, te concretiseren. Dit houdt in dat het CCB onder het gezag van de Minister van Veiligheid en Binnenlandse Zaken wordt geplaatst en administratieve en logistieke ondersteuning kan krijgen van de FOD Binnenlandse Zaken.

Artikel 1

Dit artikel wijzigt artikel 1 van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België teneinde het CCB onder het gezag van de Minister van Veiligheid en Binnenlandse Zaken te plaatsen, en de verwijzing naar de Federale Overheidsdienst Kanselarij van de Eerste Minister te vervangen door de Federale Overheidsdienst Binnenlandse Zaken.

Artikel 2

Dit artikel wijzigt artikel 2 van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België teneinde de verwijzing naar de Federale Overheidsdienst Kanselarij van de Eerste Minister te vervangen door de Federale Overheidsdienst Binnenlandse Zaken en om paragraaf 2 op te heffen.

Artikel 2, § 1 van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België stelt het CCB in staat beroep te doen op de administratieve en logistieke ondersteuning van de FOD Kanselarij van de Eerste Minister, aangezien het CCB onder het gezag van de Eerste Minister ressorteert.

Vanaf het moment dat het CCB onder het gezag van de Minister van Veiligheid en Binnenlandse Zaken wordt geplaatst, dient het CCB een beroep te doen op de administratieve en logistieke ondersteuning van de FOD Binnenlandse Zaken, aangezien dit de FOD is die onder het gezag van de Minister van Binnenlandse zaken valt, overeenkomstig artikel 1 van het koninklijk besluit van 14 januari 2002 houdende de oprichting van de Federale Overheidsdienst Binnenlandse Zaken.

Artikel 2, § 2 van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België bepaalt dat, in het specifieke kader van de toepassing van artikel 4 van het koninklijk besluit van 7 november 2000 houdende oprichting en samenstelling van de organen die gemeenschappelijk zijn aan iedere federale overheidsdienst, het CCB als een operationele dienst van de Federale Overheidsdienst Kanselarij van de Eerste Minister wordt beschouwd.

Echter, in het kader van de NIS2-wet heeft het CCB een inspectiedienst opgericht om de toezichthoudende taken uit te voeren die zijn vastgelegd in deze wet.

Overeenkomstig artikelen 44 en 64 van de NIS2-wet, moet de inspectiedienst zijn taken onafhankelijk uitoefenen ten opzichte van de entiteiten die hij controleert, met inbegrip van de overheidsinstanties die onder het toepassingsgebied van de NIS2-wet vallen (waaronder de FOD Kanselarij van de Eerste Minister en de FOD Binnenlandse Zaken).

Artikel 2, § 2 van het koninklijk besluit moet derhalve worden opgeheven, zodat het CCB niet als een operationele dienst van andere overheidsinstanties beschouwd wordt en elk risico van belangenconflict tussen de inspectietaken van het CCB en de beslissingen van de betrokken overheidsinstanties wordt vermeden.

Le Règlement sur la cybersolidarité est entré en vigueur en janvier 2025. Il prévoit en son article 4, alinéa 1^{er} que chaque État Membre qui décide de participer au système européen d'alerte en matière de cybersécurité doit désigner un cyberpôle national.

Il est important pour la Belgique de participer à ce système européen d'alerte en matière de cybersécurité, pour améliorer la détection, l'analyse et le traitement des données relatives aux cybermenaces et la prévention des incidents dans notre pays.

L'article 108 de la Constitution prévoit que le Roi fait les règlements et arrêtés nécessaires pour l'exécution des lois.

Dans le cadre de sa politique de sécurité, l'Accord de coalition fédérale 2025-2029 du gouvernement prévoit un regroupement logique de toutes les compétences en matière de sécurité auprès du Ministre de la Sécurité et de l'Intérieur.

Le CCB est actuellement placé sous l'autorité du Premier Ministre et bénéficie de l'appui administratif et logistique de la part du SPF Chancellerie du Premier Ministre.

Le présent projet d'arrêté royal a pour objectif d'exécuter le Règlement sur la cybersolidarité en Belgique, en désignant le CCB comme cyberpôle national.

Le présent projet d'arrêté royal vise également à assurer que le CCB dispose de l'indépendance opérationnelle nécessaire pour qu'il puisse exécuter ses tâches de supervision dans le respect des exigences de la loi NIS2.

Enfin, le présent projet d'arrêté royal a comme but de concrétiser la démarche décrite dans l'accord de coalition fédéral. Cela implique que le CCB soit placé sous l'autorité du Ministre de la Sécurité et de l'Intérieur et puisse bénéficier de l'appui administratif et logistique du SPF Intérieur.

Article 1^{er}

Cet article modifie l'article 1^{er} de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique afin de placer le CCB sous l'autorité du Ministre de la Sécurité et de l'Intérieur, et de remplacer la mention du Service Public Fédéral Chancellerie du Premier Ministre par celle du Service Public Fédéral Intérieur.

Article 2

Cet article modifie l'article 2 de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique afin de remplacer la mention du Service Public Fédéral Chancellerie du Premier Ministre par celle du Service Public Fédéral Intérieur et afin d'abroger le paragraphe 2.

L'article 2, § 1^{er}, de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique permet au CCB de faire appel à l'appui administratif et logistique du SPF Chancellerie du Premier Ministre étant donné que le CCB est placé sous l'autorité du Premier Ministre.

A partir du moment où le CCB est placé sous l'autorité du Ministre de la Sécurité et de l'Intérieur, le CCB devrait faire appel à l'appui administratif et logistique du SPF Intérieur car il s'agit du SPF placé sous l'autorité du Ministre de l'Intérieur, conformément à l'article 1^{er} de l'arrêté royal du 14 janvier 2002 portant création du Service public fédéral Intérieur.

L'article 2, § 2, de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique prévoit que, dans le cadre spécifique de l'application de l'article 4 de l'arrêté royal du 7 novembre 2000 portant création et composition des organes communs à chaque service public fédéral, le CCB est considéré comme un service opérationnel du SPF Chancellerie du Premier Ministre.

Cependant, dans le cadre de la loi NIS2, le CCB s'est muni d'un service d'inspection afin d'assurer les missions de supervision établies par cette loi.

Or, conformément aux articles 44 et 64 de la loi NIS2, le service d'inspection doit exercer ses tâches de manière indépendante vis-à-vis des entités qu'il supervise, en ce compris les autorités de l'administration publique tombant dans le champ d'application de la loi NIS2 (dont le SPF Chancellerie du Premier Ministre et le SPF Intérieur).

Il convient dès lors d'abroger l'article 2, § 2, de l'arrêté royal, de manière à ce que le CCB ne soit pas considéré comme service opérationnel auprès d'autres autorités de l'administration publiques et d'éviter tout risque de conflit d'intérêts entre les missions d'inspection du CCB et les décisions prises par les autorités concernées.

Artikel 3

Overeenkomstig artikel 4 van de Verordening cybersolidariteit, dienen de lidstaten een nationale cyberhub aan te wijzen indien ze besluiten deel te nemen aan het Europees waarschuwingssysteem voor cyberbeveiliging (opgericht in artikel 3 van dezelfde Verordening).

Dit waarschuwingssysteem betreft een pan-Europees infrastructuur-netwerk bestaande uit nationale en landsgrensoverschrijdende cyberhubs die zich op vrijwillige basis aansluiten, om de ontwikkeling van geavanceerde capaciteiten te ondersteunen waarmee de Unie haar opsporings-, analyse- en gegevensverwerkingscapaciteiten met betrekking tot cyberdreigingen en de preventie van incidenten in de Unie kan verbeteren.

Leden 2 en 3 van artikel 4 van de Verordening cybersolidariteit preciseren dat een nationale cyberhub één centrale entiteit dient te zijn die optreedt onder het gezag van een lidstaat. De nationale cyberhub kan een CSIRT zijn, of, in voorkomend geval, een nationale cybercrisisbeheerautoriteit of een andere bevoegde autoriteit die is aangewezen of ingesteld op grond van artikel 8, eerste lid, van Richtlijn (EU) 2022/2555 (hierna de "NIS2-richtlijn"), of een andere entiteit.

Overweging 25 van de Verordening cybersolidariteit preciseert ook dat het Europees waarschuwingssysteem voor cyberbeveiliging een civiel project is, maar waarbij ook de cyberdefensiegemeenschap baat kan hebben.

Het is belangrijk dat België deelneemt aan dit Europees waarschuwingssysteem voor cyberbeveiliging, om zo opsporings-, analyse- en gegevensverwerking met betrekking tot cyberdreigingen en de preventie van incidenten voor ons land te versterken.

Een formele aanwijzing van een nationale cyberhub is vereist, zodat België kan deelnemen aan Europese projecten.

Het CCB is, op basis van de NIS2-wet en het koninklijk besluit van 9 juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, reeds aangeduid als de nationale autoriteit voor cyberbeveiliging, het nationale CSIRT, de nationale autoriteit voor cybercrisisen, en de bevoegde autoriteit overeenkomstig artikel 8, eerste lid van de NIS2-richtlijn.

Artikel 4

Dit artikel vervangt elke vermelding van de woorden "Eerste Minister" door de woorden "Minister van Veiligheid en Binnenlandse Zaken" in artikelen 5 (rechtstreekse informatie-uitwisseling tussen de directeur-generaal en de Eerste Minister), 6 (vaststelling van de functieomschrijving en het competentieprofiel voor de managementfuncties van het CCB), 12 tot en met 14 (verlenging, evaluatie, hernieuwing van het mandaat van de directeur-generaal en de adjunct-directeur-generaal) en 16 (einde van het bovengenoemde mandaat) van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België.

Vanaf het moment dat het CCB onder het gezag van de Minister van Veiligheid en Binnenlandse Zaken wordt geplaatst, neemt deze laatste alle taken op zich die zijn vastgelegd in het bovengenoemde koninklijk besluit van 10 oktober 2014 en die tot nu toe in het kader van dit koninklijk besluit bij de Eerste Minister berustten.

Artikel 5

Dit artikel bepaalt de inwerkingtreding van dit besluit op 1 januari 2027, met uitzondering van artikel 3.

Het CCB plaatsen onder het gezag van de Minister van Veiligheid en Binnenlandse zaken en bij de Federale Overheidsdienst Binnenlandse Zaken vereist praktische wijzigingen. Dit besluit bepaalt de datum van inwerkingtreding zodat de administratie voldoende tijd heeft om een dergelijke overdracht voor te bereiden en zodat deze wijziging samenvalt met het begin van een nieuw begrotingsjaar.

Het doel van artikel 3 is echter de aanwijzing van het CCB als nationale Cyberhub. Deze aanwijzing moet niet op 1 januari 2027 wachten. Het principe dat het artikel in werking treedt tien dagen na de bekendmaking van dit besluit wordt dus behouden.

Article 3

Conformément à l'article 4 du Règlement sur la cybersolidarité, les États membres doivent désigner un cyberpôle national s'ils décident de participer au système d'alerte en matière de cybersécurité (mis en place à l'article 3 du même Règlement).

Ce système d'alerte est un réseau paneuropéen d'infrastructures composé de cyberpôles nationaux et transfrontaliers qui le rejoignent sur une base volontaire, pour soutenir le développement de capacités avancées permettant à l'Union d'améliorer ses capacités de détection, d'analyse et de traitement des données relatives aux cybermenaces et à la prévention des incidents dans l'Union.

Les alinéas 2 et 3 de l'article 4 du Règlement sur la cybersolidarité précisent qu'un cyberpôle national doit être une entité unique agissant sous l'autorité d'un État membre. Le cyberpôle national peut être un CSIRT ou, le cas échéant, une autorité nationale de gestion des crises cyber ou une autre autorité compétente désignée ou établie en vertu de l'article 8, alinéa 1^{er}, de la directive (UE) 2022/2555 (ci-après la « directive NIS2 »), ou une autre entité.

Le considérant 25 du Règlement sur la cybersolidarité précise également que le système européen d'alerte en matière de cybersécurité est un projet civil, mais qui peut aussi profiter à la communauté de cyberdéfense.

Il est important que la Belgique participe à ce système européen d'alerte en matière de cybersécurité, pour améliorer la détection, l'analyse et le traitement des données relatives aux cybermenaces et la prévention des incidents dans notre pays.

Pour que la Belgique puisse participer aux projets européens, il faut qu'un cyberpôle national soit formellement désigné.

Le CCB a déjà été désigné, en vertu de la loi NIS2 et de l'arrêté royal du 9 juin 2024 exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, comme l'autorité nationale en matière de cybersécurité, le CSIRT national, l'autorité nationale en matière de crises cybers, et l'autorité compétente conformément à l'article 8, alinéa 1^{er}, de la directive NIS2.

Article 4

Cet article remplace chaque itération des mots « Premier Ministre » par les mots « Ministre de la Sécurité et de l'Intérieur » dans les articles 5 (partage d'information direct du directeur général au Premier Ministre), 6 (établissement de la description de fonction et du profil de compétences pour les fonctions de management du CCB), 12 à 14 (prolongation, évaluation, suite donnée au mandat de directeur général et directeur général adjoint), et 16 (fin du mandat précité), de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique.

A partir du moment où le CCB est placé sous l'autorité du Ministre de la Sécurité et de l'Intérieur, ce dernier endosse toutes les tâches prévues par l'arrêté royal du 10 octobre 2014 précité qui étaient jusqu'ici dévolues au Premier Ministre dans le cadre de cet arrêté royal.

Article 5

Cet article fixe l'entrée en vigueur de l'arrêté au 1^{er} janvier 2027, à l'exception de l'article 3.

Placer le CCB sous l'autorité du Ministre de la Sécurité et de l'Intérieur et auprès du SPF Intérieur nécessite des changements d'ordre pratique. Cet arrêté fixe son entrée en vigueur afin de s'assurer que l'administration ait suffisamment de temps pour préparer un tel transfert, et afin de faire coïncider ce changement avec le début d'un nouvel exercice budgétaire.

Cependant, l'objectif de l'article 3 est la désignation du CCB comme cyberpôle national. Cette désignation ne doit pas attendre le 1^{er} janvier 2027, le principe général de l'entrée en vigueur dix jours après celui de la publication de l'arrêté est donc maintenu pour cet article.

Artikel 6

Dit artikel belast de Eerste Minister en de Minister bevoegd voor Veiligheid en Binnenlandse zaken met de uitvoering van dit besluit, ieder wat hem betreft.

Dit is de strekking van het besluit dat we U ter ondertekening voorleggen.

Ik heb de eer te zijn,

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

De Eerste Minister,
B. DE WEVER

De Minister van Veiligheid en Binnenlandse Zaken,
B. QUINTIN

15 SEPTEMBER 2026. — Koninklijk besluit tot wijziging van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België

FILIP, Koning der Belgen,

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

Gelet op de Verordening (EU) 2025/38 van het Europees Parlement en de Raad van 19 december 2024 tot vaststelling van de maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren en tot wijziging van de Verordening (EU) 2021/694;

Gelet op de Grondwet, artikelen 37, 107, tweede lid, en 108;

Gelet op het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, gewijzigd bij de koninklijke besluiten van 8 september 2015, 16 februari 2022 en 16 oktober 2022;

Gelet op het advies van de Inspecteur van Financiën geaccrediteerd bij de Federale Overheidsdienst Kanselarij van de Eerste Minister, gegeven op 9 december 2025;

Gelet op het advies van de Inspecteur van Financiën geaccrediteerd bij de Federale Overheidsdienst Binnenlandse zaken, gegeven op 13 mei 2026;

Gelet op de akkoordbevinding van de Minister van Begroting, gegeven op 25 juni 2026;

Op de voordracht van de Eerste Minister, van de Minister van Veiligheid en Binnenlandse Zaken en op het advies van de in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij:

Artikel 1. Artikel 1 van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België wordt vervangen als volgt:

“Artikel 1. Bij de Federale Overheidsdienst Binnenlandse Zaken wordt het Centrum voor Cybersecurity België, hierna “CCB” genoemd, opgericht.

Het CCB staat onder het gezag van de Minister van Veiligheid en Binnenlandse Zaken.”.

Art. 2. In artikel 2 van hetzelfde besluit worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 worden de woorden “Kanselarij van de Eerste Minister” vervangen door de woorden “Binnenlandse Zaken”;

2° paragraaf 2 wordt opgeheven.

Art. 3. In hetzelfde besluit wordt een artikel *3quater* ingevoegd, luidende:

“Art. *3quater*. § 1. Het CCB wordt aangewezen als de nationale cyberhub als bedoeld in artikel 4 van de Europese Verordening (EU) 2025/38 van het Europees Parlement en de Raad van 19 december 2024 tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren en tot wijziging van Verordening (EU) 2021/694.

§ 2. Voor zover de taken die voortvloeien uit de verordening ook betrekking hebben op bevoegdheden van andere federale overheden of van gefedereerde entiteiten, ondersteunt het CCB de bevoegde administraties en werkt het nauw met ze samen, met inachtneming van de

Article 6

Cet article désigne le Premier Ministre et le Ministre qui a la Sécurité et l'Intérieur dans ses attributions comme étant chargés de l'exécution du présent arrêté, chacun en ce qui les concerne.

Telle est la teneur de l'arrêté que nous avons l'honneur de soumettre à Votre signature.

J'ai l'honneur d'être,

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

Le Premier Ministre,
B. DE WEVER

Le Ministre de la Sécurité et de l'Intérieur,
B. QUINTIN

15 SEPTEMBRE 2026. — Arrêté royal modifiant l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu le règlement (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694;

Vu la Constitution, les articles 37, 107, alinéa 2, et 108;

Vu l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, modifié par les arrêtés royaux des 8 septembre 2015, 16 février 2022 et 16 octobre 2022;

Vu l'avis de l'Inspecteur des Finances accrédité auprès du Service public fédéral Chancellerie du Premier Ministre, donné le 9 décembre 2025;

Vu l'avis de l'Inspecteur des Finances accrédité auprès du Service public fédéral Intérieur, donné le 13 mai 2026;

Vu l'accord du Ministre du Budget, donné le 25 juin 2026;

Sur la proposition du Premier Ministre, du Ministre de la Sécurité et de l'Intérieur, et de l'avis des Ministres qui ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

Article 1^{er}. L'article 1^{er} de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, est remplacé par ce qui suit :

“ Article 1^{er}. Auprès du Service public fédéral Intérieur est créé le Centre pour la Cybersécurité Belgique, ci-après dénommé “ CCB ”.

Le CCB est placé sous l'autorité du Ministre de la Sécurité et de l'Intérieur. ”.

Art. 2. A l'article 2 du même arrêté, les modifications suivantes sont apportées :

1° dans le paragraphe 1^{er}, les mots “ Chancellerie du Premier Ministre ” sont remplacés par le mot “ Intérieur ”;

2° le paragraphe 2 est abrogé.

Art. 3. Dans le même arrêté, il est inséré un article *3quater* rédigé comme suit :

“ Art. *3quater*. § 1^{er}. Le CCB est désigné comme cyberpôle national visé à l'article 4 du règlement européen (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694.

§ 2. Dans la mesure où les tâches découlant du règlement portent également sur des domaines de compétence d'autres entités fédérales ou d'entités fédérées, le CCB soutient et coopère étroitement avec les

toepasselijke samenwerkingsakkoorden, overeenkomstig artikel 92bis van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

§ 3. Het CCB deelt alle relevante informatie met de federale overheden en de gefedereerde entiteiten, in uitvoering van de taken opgedragen in paragraaf 1.°.

Art. 4. In de artikelen 5, tweede en derde lid, 6, § 5, 12, § § 2 en 3, 13, 14, eerste lid, 16, en 19 van hetzelfde besluit, worden de woorden "Eerste Minister" vervangen door de woorden "Minister van Veiligheid en Binnenlandse Zaken".

Art. 5. Dit besluit treedt in werking op 1 januari 2027, met uitzondering van artikel 3, dat in werking treedt tien dagen na die van de bekendmaking van dit besluit.

Art. 6. De Eerste Minister en de minister bevoegd voor Veiligheid en Binnenlandse Zaken, zijn, ieder wat hem betreft, belast met de uitvoering van dit besluit.

Gegeven te Brussel, 15 september 2026.

FILIP

Van Koningswege:

De Eerste Minister,

B. DE WEVER

De Minister van Veiligheid en Binnenlandse Zaken,

B. QUINTIN

administrations compétentes, dans le respect des accords de coopération applicables, conformément à l'article 92bis de la loi spéciale du 8 août 1980 de réformes institutionnelles.

§ 3. Le CCB échange avec les entités fédérales et fédérées toutes les informations pertinentes, en exécution des tâches assignées au paragraphe 1^{er}.

Art. 4. Dans les articles 5, alinéas 2 et 3, 6, § 5, 12, § § 2 et 3, 13, 14, alinéa 1^{er}, 16, et 19 du même arrêté, les mots "Premier Ministre" sont chaque fois remplacés par les mots "Ministre de la Sécurité et de l'Intérieur".

Art. 5. Le présent arrêté entre en vigueur le 1^{er} janvier 2027, à l'exception de l'article 3 qui entre en vigueur dix jours après celui de la publication du présent arrêté.

Art. 6. Le Premier Ministre et le ministre qui a la Sécurité et l'Intérieur dans ses attributions sont, chacun en ce qui le concerne, chargés de l'exécution du présent arrêté.

Donné à Bruxelles, le 15 septembre 2026.

PHILIPPE

Par le Roi :

Le Premier Ministre,

B. DE WEVER

Le Ministre de la Sécurité et de l'Intérieur,

B. QUINTIN

FEDERALE OVERHEIDSDIENST MOBILITEIT EN VERVOER

[C – 2026/006560]

3 SEPTEMBER 2026. — Koninklijk besluit tot wijziging van het koninklijk besluit van 20 juli 2001 betreffende de inschrijving van voertuigen

VERSLAG AAN DE KONING

Sire,

Het ontwerp van koninklijk besluit dat U ter ondertekening van Uwe Majesteit wordt voorgelegd, strekt tot wijziging van het koninklijk besluit van 20 juli 2001 betreffende de inschrijving van voertuigen.

Artikelsgewijze bespreking

Artikel 1

Artikel 1 strekt ertoe een nieuw artikel 35/1 in te voeren in het koninklijk besluit van 20 juli 2001 betreffende de inschrijving van voertuigen. Dit artikel heeft tot doel de problematiek op te lossen met betrekking tot bepaalde gepersonaliseerde kentekenplaten die werden afgeleverd overeenkomstig artikel 23 van voornoemd koninklijk besluit. Het blijkt dat sommige combinaties van letters en cijfers, eenmaal in het verkeer gebracht, aanleiding geven tot klachten omdat zij als aanstootgevend worden beschouwd. In deze context kan redelijkerwijs niet worden aanvaard dat een burger blijft rondrijden met een kentekenplaat die aanstootgevende tekens bevat. De schrapping vormt dan ook een ultimum remedium ten aanzien van een burger die heeft geweigerd gebruik te maken van de kosteloze vervanging van zijn kentekenplaatnummer.

De bepaling beoogt daarom de Dienst voor Inschrijvingen van Voertuigen (hierna « DIV » genoemd) de mogelijkheid te geven om ambtshalve elke kentekenplaat te schrappen die als aanstootgevend wordt beschouwd, strijdig is met de openbare orde of met de goede zeden, of verwijst naar oorlogsmisdaden, gewapende conflicten, geweld, of enige inhoud die racistisch, seksistisch, negationistisch, homofoob is, of aanzet tot geweld, rassenscheiding, haat of discriminatie.

De in artikel 35/1 bedoelde procedure bepaalt vooreerst dat de DIV vooraf contact opneemt met de betrokken persoon om hem of haar te verzoeken de kentekenplaat kosteloos te wijzigen. Indien de persoon weigert of niet antwoordt binnen een termijn van dertig kalenderdagen, wordt door de DIV een beslissing tot ambtshalve schrapping van de plaat genomen, die bij aangetekende zending wordt meegedeeld.

Er dient te worden benadrukt dat de DIV slechts ambtshalve tot schrapping overgaat als uiterste maatregel, wanneer de betrokkene weigert gevolg te geven aan het verzoek om de nummerplaatcombinatie te wijzigen.

Om te beoordelen of een combinatie strijdig is met de voormelde criteria, baseren de medewerkers van de DIV zich op het gangbare gebruik en de algemeen aanvaarde betekenis van de betrokken termen, evenals op drie artificiële-intelligentiesystemen die worden ingezet om potentieel problematische combinaties op te sporen

SERVICE PUBLIC FEDERAL MOBILITE ET TRANSPORTS

[C – 2026/006560]

3 SEPTEMBRE 2026. — Arrêté royal modifiant l'arrêté royal du 20 juillet 2001 relatif à l'immatriculation de véhicules

RAPPORT AU ROI

Sire,

Le projet d'arrêté royal qui est soumis à la signature de Votre Majesté vise à modifier l'arrêté royal 20 juillet 2001 relatif à l'immatriculation de véhicules.

Examen article par article

Article 1^{er}

L'article 1^{er} vise à introduire un nouvel article 35/1 dans l'arrêté royal du 20 juillet 2001 relatif à l'immatriculation des véhicules. Cet article vise à résoudre la problématique liée à certaines plaques d'immatriculation personnalisées délivrées conformément à l'article 23 de l'arrêté royal précité. Il s'avère qu'une fois mises en circulation, certaines combinaisons de lettres et de chiffres font parfois l'objet de plaintes étant donné qu'elles sont jugées offensantes. Dans ce cadre-là, il n'est naturellement pas possible d'imaginer que le citoyen continue de circuler avec une plaque qui présente des caractères offensants. La radiation constitue dès lors une mesure ultime pour un citoyen qui a refusé un remplacement gratuit de son numéro d'immatriculation.

La disposition vise donc à permettre à la Direction de l'Immatriculation des Véhicules (ci-après dénommée « DIV ») de radier d'office toute marque d'immatriculation jugée offensante, contraire à l'ordre public ou aux bonnes mœurs, ou qui fait référence à des crimes de guerre, à des conflits armés, à la violence, ou à tout contenu raciste, sexiste, négationniste, homophobe, ou incitant à la violence, à la ségrégation raciale, à la haine ou à la discrimination.

La procédure, visée par l'article 35/1, précise dans un premier temps que la DIV contacte préalablement la personne concernée pour lui demander de changer gratuitement sa marque d'immatriculation. Si la personne refuse ou ne répond pas dans les trente jours calendriers, une décision de radiation d'office de la plaque est prise par la DIV et est notifiée par envoi recommandé.

Il convient de souligner que la DIV ne procède à une radiation d'office qu'en dernier recours, lorsque la personne concernée refuse de se conformer à la demande de changement de combinaison.

Pour juger si une combinaison est contraire aux termes susmentionnés, les agents de la DIV s'appuient sur les usages courants donnés à ces termes, ainsi que sur trois outils d'intelligence artificielle qui permettront de détecter les combinaisons problématiques.