

Autorisatievoorwaarden voor conformiteitsbeoordelingsinstanties (CAB)

Versie: 02 februari 2026

Logboek documentwijzigingen

Versie	Reden voor herziening	Type herziening
2024-07-05	Creatie van het document	Nieuw document
2024-09-20	Verduidelijking	Toevoeging van: In Inleiding: 4. Vertrouwelijkheid van informatie In DEEL II en DEEL III: Opladen van informatie in het gegevensbestand van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB)
2024-09-27	Verduidelijking van de accreditatievoorwaarden	De NAB werkt volgens de EU-verordening 765/2008, werkt onder de IAF MLA en is gevestigd in een land waar de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2 directieve) van toepassing is.
2025-11-14	Verduidelijking van de vestiging van een CAB en de scope van de accreditatie	Verduidelijking van de vestiging en de reikwijdte van de accreditatie van de CAB die een autorisatie wil krijgen volgens de ISO/IEC 27001-track.
206-02-02	Aanleveren van bijkomende procedures	Aanleveren van procedures m.b.t. het toepassingsgebied en de toepasselijkheidsverklaring of elk gelijkwaardig document.

Inhoudsopgave

Inleiding	4
1. Wettelijke basis	4
2. Normatieve referenties.....	4
3. Definities en acroniemen.....	4
4. Vertrouwelijkheid van informatie.....	5
DEEL I Autorisatievoorwaarden voor volgens CyberFundamentals geaccrediteerde CABs	6
1. Algemene opmerkingen.....	6
2. Autorisatievoorwaarden	6
DEEL II Autorisatievoorwaarden voor ISO/IEC 27001 geaccrediteerde CABs	8
1. Algemene opmerkingen.....	8
2. Autorisatievoorwaarden	8
DEEL III Toelatingsvoorwaarden voor CABs die geaccrediteerd zijn volgens andere IT/OT-gerelateerde normen	11
1. Algemene opmerkingen.....	11
2. Autorisatievoorwaarden	11

Inleiding

1. Wettelijke basis

In het kader van de 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 – het omzetten in België van de Europese richtlijn (EU) 2022/2555 (bekend als de NIS2-wet) en het Koninklijk Besluit van 9 juni 2024, moeten conformiteitsbeoordelingsinstanties die de naleving van de Belgische NIS2-wetgeving willen beoordelen, een accreditatie hebben, toegekend door de Nationale Accreditatie-instantie, en een autorisatie, toegekend door het CCB. Ongeacht of de conformiteitsbeoordeling vrijwillig of verplicht is voor de betrokken entiteit.

In dit document worden de verschillende voorwaarden voor het verkrijgen van een dergelijke autorisatie uitgelegd.

2. Normatieve referenties

De volgende documenten waarnaar wordt verwezen, zijn onmisbaar voor de toepassing van dit document. Voor gedateerde referenties geldt alleen de genoemde editie. Voor ongedateerde referenties geldt de laatste editie van het document waarnaar wordt verwezen (inclusief eventuele amendementen).

ISO/IEC 17000	Conformiteitsbeoordeling - Woordenlijst en algemene principes
ISO/IEC 17021-1	Conformiteitsbeoordeling - Eisen voor instanties die audits uitvoeren en certificatie van managementsystemen - Deel 1: Eisen
ISO/IEC 17029	Conformiteitsbeoordeling - Algemene principes en eisen voor validatie- en verificatie-instellingen
ISO/IEC 27001	Informatiebeveiliging, cyberveiligheid en privacybescherming - Beheersystemen voor informatiebeveiliging - Eisen
IAF PL 3	Beleid en procedures inzake de IAF MLA-structuur en voor uitbreiding van het toepassingsgebied van de IAF MLA

3. Definities en acroniemen

In dit document zijn de termen en definities uit ISO/IEC 17000 en het volgende van toepassing.

BELAC	De Belgische Nationale Accreditatie-instantie volgens het Belgisch Koninklijk Besluit van 31 januari 2006 tot oprichting van het BELAC-accreditatiesysteem voor conformiteitsbeoordelingsinstanties. BELAC is verbonden aan de Belgische FOD Economie, KMO, Middenstand en Energie.
CAB	Conformiteitsbeoordelingsinstantie Alle conformiteitsbeoordelingsinstanties die in het kader van het schema actief zijn, worden geaccrediteerd door de Nationale Accreditatie-instantie (NAB) die werkt overeenkomstig EU-Verordening (EG) nr. 765/2008 van het Europees

Autorisatievoorwaarden voor conformiteitsbeoordelingsinstanties

	Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93, tenzij in de nationale wetgeving anders is bepaald.
CAS	Conformiteitsbeoordelingschema
CCB	Centrum voor Cybersecurity België, federale administratie opgericht bij Koninklijk Besluit van 10 oktober 2014. Aangewezen als Nationale autoriteit voor cyberbeveiliging door de BE NIS2 wet en BE NIS2 KB.
CyFun	CyberFundamentals Framework - CyFun is een wettelijk geregistreerd en beschermd handelsmerk dat eigendom is van de CCB.
IAF	Internationaal accreditatieforum
IEC	Internationale Elektrotechnische Commissie
ISO	Internationale Organisatie voor Standaardisatie
MLA	Multilaterale Erkenningsregeling
NAB	Nationale Accreditatie-instantie (in België: BELAC)
NIS2 wet	Belgische Wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerken en informatiesystemen die van belang zijn voor de openbare veiligheid.
NIS2 KB	Belgisch Koninklijk besluit van 09 juni 2024 tot uitvoering van de Belgische wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerken en informatiesystemen van openbaar belang.
TLP	Verkeerslichten Protocol

4. Vertrouwelijkheid van informatie

Alle informatie die is verkregen of gecreëerd tijdens het uitvoeren van de supervisieactiviteiten van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB) in het kader van de Belgische NIS2-wet, wordt als vertrouwelijk behandeld, behalve wanneer hier door wettelijke bepalingen van moet worden afgeweken.



DEEL I **Autorisatievoorwaarden voor volgens CyberFundamentals geaccrediteerde CABs**

1. Algemene opmerkingen

Het CyberFundamentals Raamwerk is een raamwerk dat eigendom is van het Centrum voor Cybersecurity België (CCB).

De beoordeling van het CyberFundamentals Framework, of de conformiteitsbeoordeling nu vrijwillig of verplicht is voor de betrokken entiteit, wordt uitgevoerd zoals beschreven in het CyberFundamentals Conformiteitsbeoordelingschema voor CABs die geaccrediteerd zijn voor de beoordeling van dit schema door een NAB (bv. BELAC).

Het CyberFundamentals Raamwerk is beschikbaar op www.cyfun.eu.

Het CyberFundamentals Conformiteitsbeoordelingschema is beschikbaar op www.cyfun.eu.

Het acroniem "CyFun®" staat voor "The CyberFundamentals Framework" en is een geregistreerd handelsmerk van het CCB.

Het gebruik van het acroniem CyFun® en/of delen van dit document is toegestaan, mits de bron duidelijk wordt vermeld.

2. Autorisatievoorwaarden

Volgens de artikelen 14 en 15 van het BE NIS2 KB van 9 juni 2024 moet aan de volgende voorwaarden worden voldaan om een autorisatie te verkrijgen:

- De CAB moet geaccrediteerd zijn in overeenstemming met het CyberFundamentals Conformiteitsbeoordelingschema door een NAB (bv. BELAC) en moet een geldig accreditatiecertificaat voorleggen. Het CCB kan de NAB om details vragen over deze accreditatie ter ondersteuning van haar autorisatiebeslissing.
- De conformiteitsbeoordelingsinstantie moet een vestiging hebben in een land waar de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2 directieve) van toepassing is.
- De activiteiten van die vestiging in een land waar de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2 directieve) van toepassing is, moeten in het accreditatiebereik zijn opgenomen.
- Tussen de CAB en het CCB moet een juridisch bindende overeenkomst bestaan, zoals in het NIS2 Autorisatieverzoek op www.cyfun.eu :
 - Deze overeenkomst vereist het gebruik van het schema zonder beperkingen of toevoegingen en vereist samenwerking met de eigenaar van het systeem.
 - De overeenkomst bevat de verplichting voor de CAB om jaarlijks een verslag in te dienen bij het CCB met de volgende gegevens:

Autorisatievoorwaarden voor conformiteitsbeoordelingsinstanties

Voor CABs die werken voor zekerheidsniveaus 'Basic' en 'Important'.

- Lijst van verificatieverklaringen + contact
- Lijst van geweigerde claims
- Klachten (ontvangen, behandeld)
- Beroepen (ontvangen, behandeld)
- Herziene verificatieverklaringen

Voor CABs die werken voor zekerheidsniveau 'Essential'.

- Lijst van actieve certificaten + naam van entiteiten + registratienummer bedrijf (indien beschikbaar) + contactpersoon
 - Lijst van geweigerde of ingetrokken certificeringen
 - Lijst van certificaten die momenteel zijn geschorst
 - Klachten (ontvangen, behandeld)
 - Beroepen (ontvangen, behandeld)
 - De autorisatieaanvraag **zal worden vergezeld van een procedure** die uitlegt hoe de certificatie-instelling (CAB) ervoor zorgt dat het toepassingsgebied van de audit of certificatie volledig duidelijk is vóór de start van de verificatie of certificatie. Deze procedure moet nazien dat de conformiteitsbeoordeling betrekking heeft op de hele organisatie, behalve wanneer IT- en OT-omgevingen fysiek of technisch van elkaar gescheiden zijn. Als er zo'n scheiding bestaat, moet dat:
 - Duidelijk gedocumenteerd zijn;
 - Aantonen dat de uitgesloten omgevingen geen invloed hebben op de risico's van de omgeving die wél in scope zit.In alle gevallen moet deze afbakening helder worden vermeld in het toepassingsgebied van de conformiteitsbeoordeling.
- De overeenkomst omvat de verplichting voor de CAB om CCB de toestemming te geven om details op te vragen bij de NAB over de accreditatie van de CAB ter ondersteuning van de autorisatiebeslissing van het CCB.
 - De overeenkomst omvat de verplichting voor de CAB om mee te werken aan elk verzoek van het CCB met betrekking tot de verificatie- of certificeringsactiviteiten.
 - Bij het niet reageren op een verzoek van het CCB, volgt een waarschuwing.
 - Herhaaldelijk onvoldoende antwoord op een verzoek kan leiden tot een waarschuwing
 - Wanneer de inspectiedienst van de nationale autoriteit voor cyberbeveiliging een schending van de in dit hoofdstuk bedoelde autorisatievoorwaarden vaststelt, kan de inspectiedienst volgens de procedure van titel 4, hoofdstuk 2, afdeling 1, van de BE NIS2 Wet de conformiteitsbeoordelingsinstantie aanmanen een einde te maken aan de schending. Zo niet, dan kan de nationale autoriteit voor cyberbeveiliging de autorisatie schorsen of intrekken.

DEEL II Autorisatievoorwaarden voor ISO/IEC 27001 geaccrediteerde CABs

1. Algemene opmerkingen

Dit hoofdstuk heeft betrekking op CABs die geaccrediteerd zijn om managementsystemen te certificeren conform ISO/IEC 27001 volgens ISO/IEC 17021-1.

De accreditatie van de CAB wordt verleend door een NAB die :

- Werkt volgens de EU-verordening 765/2008 waarin de vereisten voor accreditatie en markttoezicht zijn vastgelegd.

En

- Werkt onder de IAF Multilaterale Erkenningsregeling (MLA) beschreven in IAF PL 3.

En

- Gevestigd is in een land waar de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2 directieve) van toepassing is.

2. Autorisatievoorwaarden

Volgens de artikelen 14 en 15 van het BE NIS2 KB moet aan de volgende voorwaarden worden voldaan om een autorisatie te verkrijgen:

- De CAB moet geaccrediteerd zijn om managementsystemen te certificeren conform ISO/IEC 27001 volgens ISO/IEC 17021-1 en moet een geldig accreditatiecertificaat voorleggen.
Het CCB kan de NAB om details vragen over deze accreditatie ter ondersteuning van zijn autorisatiebeslissing.
- De conformiteitsbeoordelingsinstantie moet een vestiging hebben in een land waar de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2 directieve) van toepassing is.
- De activiteiten van die vestiging in een land waar de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2 directieve) van toepassing is, moeten in het accreditatiebereik zijn opgenomen.
- Tussen de CAB en het CCB moet een juridisch bindende overeenkomst van kracht zijn, zoals opgenomen in het NIS2 autorisatieverzoek op www.cyfun.eu , die het volgende omvat

Autorisatievoorwaarden voor conformiteitsbeoordelingsinstanties

- De verplichting voor de CAB om jaarlijks een verslag in te dienen bij het CCB met de volgende gegevens:
 - Lijst van actieve ISO 27001-certificaten in een NIS2-context + naam van entiteiten + bedrijfsregistratienummer (indien beschikbaar) + contactpersoon
 - Lijst van geweigerde of ingetrokken certificaten
 - Lijst van certificaten die momenteel zijn geschorst
 - Klachten (ontvangen, behandeld)
 - Beroepen (ontvangen, behandeld)
 - Opladen van informatie in het gegevensbestand van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB) in het kader van ISO/IEC 27001 certificatie
 - De geautoriseerde conformiteitsbeoordelingsinstantie (CAB) zal elk ISO/IEC 27001 certificaat en de daaraan verbonden toepasselijkheidsverklaring ('Statement Of Applicability') dat werd verleend in een NIS2 context opladen in het gegevensbestand van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB). Hiervoor zal de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB) de nodige instructies verstrekken.
 - Entiteiten die opteren voor het gebruik van een ISO/IEC 27001 certificatie om een vermoeden van conformiteit t.o.v. NIS2 ('presumption of conformity') te verkrijgen zijn zoals bepaald in het BE NIS2 KB van 09 juni 2024 (Koninklijk besluit 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) Art 22 §1 2° verplicht het toepassingsgebied en de toepasselijkheidsverklaring aan het CCB te bezorgen.
 - De autorisatieaanvraag **zal worden vergezeld van een procedure** die uitlegt hoe de certificatie-instelling (CAB) ervoor zorgt dat het toepassingsgebied van de audit of certificatie volledig duidelijk is vóór de start van de verificatie of certificatie. Deze procedure moet nazien dat de conformiteitsbeoordeling betrekking heeft op de hele organisatie, behalve wanneer IT- en OT-omgevingen fysiek of technisch van elkaar gescheiden zijn. Als er zo'n scheiding bestaat, moet dat:
 - Duidelijk gedocumenteerd zijn;
 - Aantonen dat de uitgesloten omgevingen geen invloed hebben op de risico's van de omgeving die wél in scope zit.In alle gevallen moet deze afbakening helder worden vermeld in het toepassingsgebied van de conformiteitsbeoordeling.
 - De autorisatieaanvraag **zal worden vergezeld van een procedure** die garandeert dat de verklaring van toepasselijkheid (Statement of Applicability – SoA) aantoont dat de organisatie cyberbeveiligingsmaatregelen implementeert die aantoonbaar gelijkwaardig zijn aan de maatregelen uit de CyFun® zekerheidsniveaus Basis, Belangrijk of Essentieel. Welk zekerheidsniveau van toepassing is, wordt bepaald op basis van de risicoanalyse van de entiteit. Hiervoor wordt bij voorkeur de 'CyFun® Selection Tool' gebruikt.
- De overeenkomst omvat de verplichting voor de CAB om CCB de toestemming te geven om details op te vragen bij de NAB over de accreditatie van de CAB ter ondersteuning van de autorisatiebeslissing van het CCB.

Autorisatievoorwaarden voor conformiteitsbeoordelingsinstanties

- De overeenkomst omvat de verplichting voor de CAB om mee te werken aan elk verzoek van het CCB met betrekking tot de bovengenoemde certificeringsactiviteiten.
 - Bij het niet reageren op een verzoek van het CCB, volgt een waarschuwing.
 - Herhaaldelijk onvoldoende beantwoorden van een verzoek kan leiden tot een waarschuwing.
 - Wanneer de inspectiedienst van de nationale autoriteit voor cyberbeveiliging een overtreding van de in dit document bedoelde autorisatievoorwaarden vaststelt, kan de inspectiedienst volgens de procedure van titel 4, hoofdstuk 2, afdeling 1, van de BE NIS2 Wet de conformiteitsbeoordelingsinstantie aanmanen om een einde te maken aan de overtreding. Anders kan de nationale autoriteit voor cyberbeveiliging de autorisatie schorsen of intrekken.



DEEL III Toelatingsvoorwaarden voor CABs die geaccrediteerd zijn volgens andere IT/OT-gerelateerde normen

1. Algemene opmerkingen

Dit hoofdstuk heeft betrekking op CABs die zijn geaccrediteerd volgens ISO/IEC 17029 of ISO/IEC 17021-1 en die entiteiten verifiëren of certificeren tegen andere IT/OT-gerelateerde normen dan ISO/IEC 27001.

De accreditatie van het CAB wordt verleend door een NAB die:

- Werkt volgens de EU-verordening 765/2008 waarin de vereisten voor accreditatie en markttoezicht zijn vastgelegd.

En

- Werkt onder de IAF Multilaterale Erkenningsregeling (MLA) beschreven in IAF PL 3.

En

- Gevestigd is in een land waar de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2 directieve) van toepassing is.

2. Autorisatievoorwaarden

Volgens de artikelen 14 en 15 van het KB NIS2 moet aan de volgende voorwaarden worden voldaan om een autorisatie te verkrijgen:

- De CAB moet geaccrediteerd zijn volgens ISO/IEC 17029 of ISO/IEC 17021-1 en moet een geldig accreditatiecertificaat voorleggen.
Het CCB kan de NAB om details vragen over deze accreditatie om zijn autorisatiebeslissing te ondersteunen.
- De conformiteitsbeoordelingsinstantie moet een vestiging hebben in een land waar de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2 directieve) van toepassing is.
- De activiteiten van die vestiging in een land waar de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS2 directieve) van toepassing is, moeten in het accreditatiebereik zijn opgenomen.
- Tussen de CAB en het CCB moet een juridisch bindende overeenkomst bestaan, zoals opgenomen in het NIS2 autorisatieverzoek op www.cyfun.eu :
 - De overeenkomst bevat de verplichting voor de CAB om jaarlijks een verslag in te dienen bij het CCB met de volgende gegevens:

Autorisatievoorwaarden voor conformiteitsbeoordelingsinstanties

Voor CABS geaccrediteerd volgens ISO/IEC 17029

- Lijst van verificatieverklaringen in een NIS2-context + contactpersoon
- Lijst van geweigerde claims
- Klachten (ontvangen, behandeld)
- Beroepen (ontvangen, behandeld)
- Herziene verificatieverklaringen

Voor CABs geaccrediteerd volgens ISO/IEC 17021-1

- Lijst van actieve certificaten in een NIS2-context + naam van entiteiten + bedrijfsregistratienummer (indien beschikbaar) + contactpersoon
- Lijst van geweigerde of ingetrokken certificaties
- Lijst van certificaten die momenteel zijn geschorst
- Klachten (ontvangen, behandeld)
- Beroepen (ontvangen, behandeld)
- Opladen van informatie in het gegevensbestand van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB)
 - De geautoriseerde conformiteitsbeoordelingsinstantie (CAB) zal elk certificaat en de daaraan verbonden informatie dat werd verleend in een NIS2 context opladen in het gegevensbestand van de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB). Hiervoor zal de certificatieautoriteit van het Centrum voor Cybersecurity België (CCB) de nodige instructies verstrekken.
- De autorisatieaanvraag **zal worden vergezeld van een procedure** die uitlegt hoe de certificatie-instelling (CAB) ervoor zorgt dat het toepassingsgebied van de audit of certificatie volledig duidelijk is vóór de start van de verificatie of certificatie. Deze procedure moet nazien dat de conformiteitsbeoordeling betrekking heeft op de hele organisatie, behalve wanneer IT- en OT-omgevingen fysiek of technisch van elkaar gescheiden zijn.

Als er zo'n scheiding bestaat, moet dat:

 - Duidelijk gedocumenteerd zijn;
 - Aantonen dat de uitgesloten omgevingen geen invloed hebben op de risico's van de omgeving die wél in scope zit.

In alle gevallen moet deze afbakening helder worden vermeld in het toepassingsgebied van de conformiteitsbeoordeling.
- De autorisatieaanvraag **zal worden vergezeld van een procedure** die garandeert dat de verklaring van toepasselijkheid (Statement of Applicability – SoA) of elk gelijkwaardig document aantoont dat de organisatie cyberbeveiligingsmaatregelen implementeert die aantoonbaar gelijkwaardig zijn aan de maatregelen uit de CyFun® zekerheidsniveaus Basis, Belangrijk of Essentieel.

Welk zekerheidsniveau van toepassing is, wordt bepaald op basis van de risicoanalyse van de entiteit. Hiervoor wordt bij voorkeur de 'CyFun® Selection Tool' gebruikt.
- De overeenkomst omvat de verplichting voor de CAB om CCB de toestemming te geven om details op te vragen bij de NAB over de accreditatie van de CAB ter ondersteuning van de autorisatiebeslissing van het CCB.

Autorisatievoorwaarden voor conformiteitsbeoordelingsinstanties

- De overeenkomst omvat de verplichting voor het CAB om mee te werken aan elk verzoek van het CCB met betrekking tot de verificatie- of certificeringsactiviteiten.
 - Bij het niet reageren op een verzoek van het CCB, volgt een waarschuwing.
 - Herhaaldelijk onvoldoende beantwoorden van een verzoek kan leiden tot een waarschuwing.
 - Wanneer de inspectiedienst van de nationale autoriteit voor cyberbeveiliging een schending van de in dit hoofdstuk bedoelde autorisatievoorwaarden vaststelt, kan de inspectiedienst volgens de procedure van titel 4, hoofdstuk 2, afdeling 1, van de BE NIS2 Wet de conformiteitsbeoordelingsinstantie aanmanen een einde te maken aan de schending. Zo niet, dan kan de nationale autoriteit voor cyberbeveiliging de autorisatie schorsen of intrekken.