



2026_VB_00186 Conformiteitsbeoordeling NIS2 OCMW Gent - Goedkeuring

Beslissing: Goedgekeurd in besloten vergadering van 30 april 2026

Zijn aanwezig bij de beslissing van dit punt:

Mathias De Clercq, burgemeester-voorzitter
Hafsa El-Bazioui, schepen; Astrid De Bruycker, schepen; Sofie Bracke, schepen; Bram Van Braeckevelt, schepen; Burak Nalli, schepen; Christophe Peeters, schepen
Mieke Hullebroeck, algemeen directeur; Liesbet Vertriest, adjunct-algemeendirecteur

Bevoegd: Mathias De Clercq

Betrokken: Christophe Peeters, Filip Watteeuw, Sofie Bracke, Bram Van Braeckevelt, Astrid De Bruycker, Evita Willaert, Joris Vandenbroucke, Hafsa El-Bazioui, Burak Nalli

Juridisch kader

De volgende bepalingen zijn van toepassing inzake de bevoegdheid:

Het Decreet over het lokaal bestuur van 22 december 2017, artikel 56, § 1.

De beslissing wordt genomen op grond van:

Wet van 26 april 2024: 'Wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid' - ook NIS2-wet genaamd.

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, artikel 23 § 1.

Motivering

Sinds 16 januari 2023 is de zogenaamde NIS2-richtlijn van toepassing, dewelke werd omgezet in Belgische regelgeving (de NIS2-wet). Het doel van deze regelgeving is het versterken van maatregelen op het gebied van cyberveiligheid, incidentbeheer en toezicht voor entiteiten die diensten leveren die essentieel zijn voor het in stand houden van kritieke maatschappelijke of economische activiteiten. De wet heeft ook als doel de coördinatie van overheidsbeleid op het gebied van cyberveiligheid te verbeteren.

Er is een verplicht registratiemechanisme, waarbij entiteiten die onder de regelgeving vallen, zich moesten registreren vóór 18 maart 2025.

De richtlijn maakt een onderscheid tussen verschillende niveaus van criticiteit. Deze indeling - basis, belangrijk, essentieel - wordt bepaald op basis van de impact van een mogelijke cyberaanval op de dienstverlening, het niveau van de afhankelijkheid van de organisatie door

burgers en bedrijven, specifieke sectorale risicobeoordelingen door de nationale en Europese autoriteiten. Het Centrum voor Cybersecurity bepaalt deze classificatie.

Van essentiële en belangrijke entiteiten wordt verwacht dat ze passende maatregelen nemen om de risico's te beheersen voor de beveiliging van de netwerk- en informatiesystemen die zij voor hun activiteiten of voor het verlenen van hun diensten gebruiken, en maatregelen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.

Stad en OCMW Gent zijn in april 2025 geregistreerd als een 'essentiële' entiteit. Dit betekent niet dat Stad Gent voor elk risico ook de maatregelen zal moeten implementeren op het zekerheidsniveau 'essentieel'. Uit lopende risicoanalyses blijkt dat dit waarschijnlijk op het niveau 'belangrijk' zal zijn.

De impact van onder welke classificatie (basis, belangrijk of essentieel) de entiteit valt gaat o.a. over hoe uitgebreid het risicobeheersproces moet zijn, hoe streng de technische en organisatorische maatregelen worden vereist, hoe strikt de governance moet worden bepaald, hoeveel compliance-audits nodig zijn, enz. Deze vereisten zijn gedefinieerd in het 'Cyber Fundamentals Framework'.

Een eerste stap in de conformiteitsbeoordeling is het voorleggen van een zelfevaluatie op het zekerheidsniveau 'basis', uiterlijk 18 april 2026 moest er hiervoor een overeenkomst zijn gesloten met een **geautoriseerde Conformity Assessment Body (CAB) of Conformiteitsbeoordelingsinstantie, die onze zelfevaluatie kan verifiëren**. De verificatie (audit) vindt plaats in mei 2026. Om de verificatie op niveau 'basis' te verkrijgen moeten we aan een vastgelegd maturiteitsniveau voldoen (totaalscore moet minstens 2,5 bedragen, ook voor specifieke vereisten moet Stad Gent een individuele score van minstens 2,5 halen). Volgens onze zelfevaluatie behalen we een maturiteitsscore van 3,21, deze evaluatie moet Stad Gent voorleggen aan de Conformiteitsbeoordelingsinstantie, die onze inschatting zal verifiëren.

Een volgende stap is het behalen van een verificatie op niveau 'belangrijk', uiterlijk 18 maanden na de inwerkingtreding van de NIS2-wet. Na deze verificatie wordt er blijvend toezicht gehouden door de bevoegde inspectiediensten (zoals het centrum voor cybersecurity), op basis van indicatoren zoals het zich voordoen van een incident of objectief bewijs van mogelijke tekortkomingen.

Uit communicatie die de lokale overheden recent ontvangen door de Vlaamse Overheid en het Agentschap Binnenlands Bestuur mag de deadline van 18 april 2026 worden overschreden, behoudens er vóór deze deadline een overeenkomst voor het uitvoeren van een verificatie is gesloten met een Conformiteitsbeoordelingsinstantie.

Toegepast op Stad en OCMW Gent:

Elke rechtspersoon, met een eigen KBO-nummer, moet een CyberFundamentals-verificatie verkrijgen. Voor Stad en OCMW Gent worden 2 zelfevaluaties voorgelegd aan de conformiteitsbeoordelingsinstantie, inhoudelijk is dit hetzelfde document omdat de IT-omgeving van beide organisaties niet gescheiden is en we eenzelfde maatregelen nemen.

Conclusie:

De zelfevaluatie die OCMW Gent heeft uitgevoerd op basis van het 'Cyber Fundamentals Framework' toont aan dat we het het zekerheidsniveau 'basis' halen. Deze evaluatie wordt in mei voorgelegd aan een aan Conformity Assessment Body (CAB) die een audit zal uitvoeren ter verificatie. Er is tijdig met een CAB een overeenkomst tot verificatie gesloten.

Artikel 13 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, stelt dat de entiteiten zicht moeten registreren uiterlijk op 18 maart 2025.

Bijgevoegde bijlage(n):

- Zelfevaluatie Stad en OCMW Gent NIS2_ april2026.xlsx

Beslissing

Beslist het volgende:

Artikel 1:

Keurt de zelfevaluatie op basis van het 'Cyber Fundamentals Framework' goed die OCMW Gent, conform de NIS2 richtlijn, zal voorleggen aan de Conformiteitsbeoordelingsinstantie ter verificatie van het zekerheidsniveau 'basis'.

2026_VB_00186 - Conformiteitsbeoordeling NIS2 OCMW Gent