

Addendum bij de Algemene Inkoopvoorwaarden van UMCG

Onderwerp: Informatieveiligheid & Digitale Weerbaarheid (NIS2 / Cbw) en verduidelijking geheimhoudingsuitzondering artikel 16.1

Dit addendum ("Addendum") behoort bij en maakt, deel uit van de Algemene Inkoopvoorwaarden van UMCG, versie juni 2026 (de "Inkoopvoorwaarden" of "AIV"). Dit Addendum wijzigt en vult de Inkoopvoorwaarden aan zoals hieronder beschreven. In geval van strijdigheid tussen dit Addendum en de Inkoopvoorwaarden, prevaleert het bepaalde in dit Addendum.

1. Wijziging titel Artikel 16A

De titel van Artikel 16A wordt gewijzigd. Reden: de huidige titel "NIS2 & Cbw" dekt de lading onvoldoende en suggereert dat het artikel uitsluitend ziet op de twee genoemde wetten, terwijl het artikel bredere normen omvat (o.a. NEN7510, ISO 27001/27701/27799, AVG).

WAS

~~Artikel 16A. NIS2 & Cbw~~

WORDT

Artikel 16A. Informatie Veiligheid & Digitale Weerbaarheid (Cyberweerbaarheid)

De inhoud van Artikel 16A blijft voor het overige ongewijzigd, met uitzondering van de leden 16A.2 en 16A.4, zie artikel 2 van dit Addendum.

2. Verplaatsing van artikelleden 16A.2 en 16A.4 naar nieuwe Bijlage B

De leden 16A.2 en 16A.4 hebben specifiek betrekking op de kwalificatie van UMC als essentiële entiteit onder de NIS2-richtlijn/Cyberbeveiligingswet (Cbw) en op informatieverstrekking ten behoeve van NIS2/Cbw-onderzoeken. Deze bepalingen zijn naar hun aard niet op elke Prestatie van toepassing, maar specifiek op digitale omgevingen in de zorg (IT, OT en Medische Technologie) die onder het toepassingsbereik van de Cbw vallen.

Deze leden komen te vervallen in Artikel 16A van de Inkoopvoorwaarden en worden — inhoudelijk ongewijzigd — opgenomen in de nieuwe Bijlage B bij de Inkoopvoorwaarden (zie artikel 4 van dit Addendum). De nummering van de overige leden van Artikel 16A (16A.1, 16A.3, 16A.5 t/m 16A.14) blijft ongewijzigd; de vervallen leden worden als zodanig gemarkeerd.

WAS

~~16A.2 Leverancier erkent dat UMC kwalificeert als essentiële entiteit in de zin van de NIS2-richtlijn en de Cyberbeveiligingswet (Cbw) en zal alle verplichtingen uit hoofde daarvan faciliteren. Deze bepaling geldt onverminderd de eisen en maatregelen uit NEN7510, ISO 27001, 27701 en 27799 en de AVG. De artikelen uit artikel 16A zijn van toepassing op alle relevante softwarecomponenten, ongeacht of de Prestatie zelf bestaat uit software of dat de software onderdeel is van de te leveren Prestatie.~~

WORDT

16A.2 [VERVALLEN — verplaatst naar Bijlage B, zie Artikel B2]

WAS

~~16A.4 Leverancier levert op verzoek alle relevante informatie die UMC verzoekt voor uitvoering onderzoeken onder de NIS2, waaronder een gedetailleerd overzicht van de landen en wijzen waar dataverwerking plaatsvindt, een actuele SBOM van alle softwarecomponenten binnen de Prestatie inclusief third-party libraries, versies en bekende CVE-meldingen.~~

WORDT

16A.4 [VERVALLEN — verplaatst naar Bijlage B, zie Artikel B3]

Genummerd als 16A.2 en 16A.4 blijven deze plekken in Artikel 16A behouden onder vermelding "[vervallen, zie Bijlage B]", zodat de nummering van de overige leden niet wijzigt.

3. Verduidelijking uitzondering geheimhouding — Artikel 16.1 sub d

Op verzoek van de FG wordt sub d van Artikel 16.1 (uitzonderingen op de geheimhoudingsverplichting) verduidelijkt, zodat expliciet is dat deze uitzondering alleen ziet op niet-persoonsgebonden gegevens en dus geen ruimte biedt om zelfstandig ontwikkelde informatie die persoonsgegevens betreft van de geheimhoudingsplicht uit te zonderen.

WAS

~~d) Informatie die door een Partij zelfstandig is ontwikkeld zonder dat daarbij inbreuk is gemaakt op de geheimhoudingsverplichting uit dit artikel.~~

WORDT

d) Informatie die niet-persoonsgebonden gegevens zijn die door een Partij zelfstandig is ontwikkeld zonder dat daarbij inbreuk is gemaakt op de geheimhoudingsverplichting uit dit artikel.

De overige onderdelen van Artikel 16.1 (a, b en c) en de leden 16.2 t/m 16.9 blijven ongewijzigd.

4. Nieuwe Bijlage B — Aanvullende voorwaarden Informatiebeveiliging voor Zorgomgevingen (IT, OT en Medische Technologie) onder de Cbw

Aan de Inkoopvoorwaarden wordt de volgende bijlage toegevoegd. Deze bijlage is uitsluitend van toepassing indien en voor zover dit uitdrukkelijk in de Order en/of de Overeenkomst is bepaald, namelijk voor Prestaties die zien op digitale zorgomgevingen (IT, OT en/of Medische Technologie) die vallen binnen het toepassingsbereik van de Cyberbeveiligingswet (Cbw) c.q. de NIS2-richtlijn.

Bijlage B. Toepasselijkheid en aanvullende bepalingen zorgomgevingen (Cbw)

Artikel B1. Toepasselijkheid

B1.1 Deze bijlage geldt naast het bepaalde in de artikelen 1 tot en met 23 en in het bijzonder Artikel 16A van de Inkoopvoorwaarden, indien en voor zover in de Order en/of de Overeenkomst is bepaald dat de Prestatie geheel of gedeeltelijk bestaat uit, of betrekking heeft op, digitale zorgomgevingen zoals informatietechnologie (IT), operationele technologie (OT) en/of Medische Technologie die binnen het toepassingsbereik van de Cyberbeveiligingswet (Cbw) en/of de NIS2-richtlijn vallen.

B1.2 Ingeval van strijdigheid tussen deze bijlage en Artikel 16A en/of de overige artikelen van de Inkoopvoorwaarden, prevaleert het bepaalde in deze bijlage.

Artikel B2. Erkenning essentiële entiteit (was Artikel 16A.2)

B2.1 Leverancier erkent dat UMC kwalificeert als essentiële entiteit in de zin van de NIS2-richtlijn en de Cyberbeveiligingswet (Cbw) en zal alle verplichtingen uit hoofde daarvan faciliteren. Deze bepaling geldt onverminderd de eisen en maatregelen uit NEN7510, ISO 27001, 27701 en 27799 en de AVG.

B2.2 Deze bijlage, alsmede Artikel 16A van de Inkoopvoorwaarden, is van toepassing op alle relevante softwarecomponenten binnen de Prestatie, ongeacht of de Prestatie zelf bestaat uit software of dat de software onderdeel is van de te leveren Prestatie.

Artikel B3. Informatieverstrekking ten behoeve van NIS2/Cbw-onderzoeken (was Artikel 16A.4)

B3.1 Leverancier levert op verzoek alle relevante informatie die UMC verzoekt voor de uitvoering van onderzoeken onder de NIS2/Cbw, waaronder in ieder geval:

- a) een gedetailleerd overzicht van de landen en wijzen waarop dataverwerking plaatsvindt;
- b) een actuele SBOM (Software Bill of Materials) van alle softwarecomponenten binnen de Prestatie, inclusief third-party libraries, versies en bekende CVE-meldingen.

Einde Addendum (definitief).