Model addendum
NIS2 en Cbw

Inleiding

Met het oog op de verplichtingen die voortvloeien uit de Richtlijn (EU) 2022/2555 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie (“NIS2-richtlijn”) en de opvolger van de Wet Beveiliging Netwerk- en Informatiesystemen: de Cyberbeveiligingswet (“Cbw”), hebben afzenders benoemd in het colofon een template addendum ontwikkeld om organisaties en bedrijven te ondersteunen om de verplichtingen die volgen uit de wet te vertalen. Dit addendum kan worden toegepast in de contractuele relatie die partijen al hebben.

Het is belangrijk om te benadrukken dat bij de vorming van deze wetgeving in Europa, het primaire doel is gesteld om de samenleving te beschermen tegen verstoringen veroorzaakt door cyberincidenten. Dit wordt bereikt door zowel essentiële als belangrijke organisaties, alsook hun directe leveranciers, te integreren binnen het kader van deze wet.

De wetgeving verplicht organisaties die vallen onder de NIS2-richtlijn en de Cbw maatregelen te nemen om de toeleveringsketen voldoende te beveiligen. In dat kader dienen toeleveranciers van organisaties die vallen onder de NIS2-richtlijn en de Cbw mogelijke veiligheidsrisico's te minimaliseren en de integriteit van de bedrijfsactiviteiten te handhaven in de leveringsketen. Deze verplichting staat beschreven in artikel 21 lid 2 sub d van de NIS2-richtlijn.

Dit template addendum is ontworpen om als hulpmiddel en aanvulling te dienen op de bestaande contractuele relatie tussen organisaties in Nederland die vallen onder de NIS2-richtlijn en de Cbw en hun leveranciers. Het biedt de mogelijkheid om specifieke verplichtingen en beveiligingsmaatregelen vast te leggen die nodig zijn om te voldoen aan de NIS2-richtlijn en de Cbw.

Ten tijde van opstellen van dit addendum is de NIS2-richtlijn nog niet geïmplementeerd in nationale wetgeving en zijn de teksten daaromtrent nog niet definitief. Derhalve is het van belang rekening te houden met het feit dat diverse onderdelen van dit addendum kunnen of moeten worden gewijzigd in het licht van de definitieve wetteksten. Daarnaast zal de uitwerking van de NIS2-richtlijn, alsmede de implementatie daarvan in nationale wetgeving, in de praktijk nog verder uitgekristalliseerd dienen te worden. Het is daarom belangrijk dat gebruikers van dit addendum aanpassingen doorvoeren waar nodig teneinde het te laten aansluiten bij de laatste stand van de wetgeving en de specifieke omstandigheden van de betrokken partijen. Voor meer informatie over het gebruik van dit addendum zie pagina 11.

Addendum NIS2-richtlijn/ Cbw

Ondergetekenden:

1. <NAAM> gevestigd te <NAAM>, te dezen rechtsgeldig vertegenwoordigd door: <NAAM>. Hierna te noemen: <Opdrachtgever>.

en

2. <NAAM> gevestigd te <NAAM>, te dezen rechtsgeldig vertegenwoordigd door: <NAAM>. Hierna te noemen: <Opdrachtnemer>

Overwegende dat:

- <Opdrachtgever> valt onder de werking van de Richtlijn (EU) 2022/2555 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie (“NIS2-richtlijn”) en de Wet beveiliging netwerk- en informatiesystemen (“Cbw”), en derhalve gehouden is aan de daarin gestelde eisen voor de beveiliging van haar netwerk- en informatiesystemen;
- op grond van artikel 21 van de NIS2-richtlijn en artikel 23 van de Cbw, <Opdrachtgever> verplicht is evenredige technische, operationele en organisatorische maatregelen te nemen om de risico’s voor de beveiliging van haar netwerk- en informatiesystemen te beheren en om incidenten te voorkomen, of, indien deze zich voordoen, de gevolgen daarvan voor de afnemers van haar diensten en voor andere diensten te beperken;
- hieronder vallen op grond van artikel 21 lid 2 sub d van de NIS2-richtlijn en artikel 23 van de Cbw, maatregelen ter beveiliging van de toeleveringsketen, met inbegrip van beveiliging gerelateerde aspecten met betrekking tot de relaties tussen <Opdrachtgever> en haar rechtstreekse leveranciers of dienstverleners;
- dat <Opdrachtgever> en <Opdrachtnemer> een <naam overeenkomst> (hierna “de Overeenkomst”) zijn aangegaan, gedateerd <datum> en derhalve <Opdrachtnemer> op grond van artikel 21 lid 2 sub d van de NIS2-richtlijn en artikel 23 van de Cbw, te kwalificeren is als leverancier van <Opdrachtgever>;
- <Opdrachtgever> en <Opdrachtnemer> het cruciale belang van cyberbeveiliging onderkennen en in dit kader afspraken wensen te maken over het te voeren cybersecuritybeleid, certificering, informatie-uitwisseling, zorgplicht en meldingsplicht, teneinde uitwerking te geven aan artikel 21 lid 2 sub d van de NIS2-richtlijn en artikel 23 van de Cbw;
- dat partijen vervolgens een of meer aanvullende en/of afwijkende voorwaarden zijn overeengekomen met betrekking tot de Overeenkomst;
- dat partijen het wenselijk achten om deze nadere afspraken schriftelijk vast te leggen in dit addendum (hierna “het Addendum”).

Verklaren hierbij te zijn overeengekomen als volgt:

1. In aanvulling en/of afwijking op de overeenkomst komen partijen overeen navolgende <Annex> toe te voegen als <Annex> <nummer> bij de Overeenkomst:

Annex <nummer> inzake NIS2-richtlijn / Cbw

Artikel 1 Definities:

Cybersecuritybeleid:	Een cybersecuritybeleid welke voldoet aan de NIS2-richtlijn en de Cbw
NIS2-richtlijn:	Richtlijn (EU) 2022/2555 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie
Bijna-incident:	Een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan, als omschreven in artikel 6 van de NIS2-richtlijn
Incident:	Een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt, als omschreven in artikel 6 van de NIS2-richtlijn
Significant Incident:	Een ernstige operationele verstoring van de diensten of financiële verliezen voor <Opdrachtgever> kan veroorzaken, dan wel andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken, als omschreven in artikel 21 van de NIS2-richtlijn, de artikelen 28 tot en met 31 van de Cbw en eventuele implementatie wetgeving gerelateerd aan de NIS2.
Cbw:	De Wet beveiliging netwerk- en informatiesystemen

Artikel 2 toepasselijkheid NIS2-richtlijn en Cbw

2.1. Partijen stellen vast dat <Opdrachtgever> valt onder de werking van de NIS2-richtlijn en de Cbw.

2.2. Op grond van artikel 21 van de NIS2-richtlijn en artikel 23 van de Cbw is <Opdrachtgever> verplicht om evenredige technische, operationele en organisatorische maatregelen te nemen om de risico's voor de beveiliging van haar netwerk- en

informatiesystemen, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van haar diensten en voor andere diensten te beperken.

2.3. Hieronder vallen op grond van artikel 21 lid 2 sub d van de NIS2-richtlijn en artikel 23 van de Cbw, maatregelen ter beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen <Opdrachtgever> en haar rechtstreekse leveranciers of dienstverleners;

2.4. <Opdrachtgever> en <Opdrachtnemer> erkennen het cruciale belang van cybersecurity. <Opdrachtnemer> erkent dat <Opdrachtgever>, in overeenstemming met artikel 21 lid 2 sub d van de NIS2-richtlijn, een specifieke zorgplicht heeft met betrekking tot de cybersecurity binnen haar toeleveringsketen.

Artikel 3 Cybersecuritybeleid, certificering en zorgplicht

3.1. <Opdrachtgever> hanteert een cybersecuritybeleid (of cybersecurityplan) welke voldoet aan de NIS2-richtlijn en de Cbw (hierna “Cybersecuritybeleid”) en die (is opgenomen onder (…)/ beschikbaar is via: (…))

3.2. Op basis van artikel 21 lid 3 van de NIS2-richtlijn heeft <Opdrachtgever> een gecoördineerde beveiligingsrisicobeoordeling (risico-inventarisatie) uitgevoerd ten aanzien van <Opdrachtnemer>, rekening houdende met de specifieke kwetsbaarheden, de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van <Opdrachtnemer>, op basis waarvan zij passende maatregelen zoals omschreven in artikel 3.5. heeft vastgesteld.

3.3. OPTIONEEL:<Opdrachtgever> hanteert (aantal) risicoclassificaties bij de beveiligingsrisicobeoordeling. Op basis van de risico-inventarisatie classificeert <Opdrachtgever> <Opdrachtnemer> als: (…)

3.4. <Opdrachtgever> erkent het belang van de relatie tussen <Opdrachtgever> en <Opdrachtnemer> en partijen stellen vast dat de <Opdrachtnemer> een redelijk termijn nodig zal hebben om aan de eisen die gekoppelde zijn aan voor genoemde risico-inventarisatie en uitgewerkt zijn in artikel 3.5., te voldoen. Partijen committeren zich derhalve aan een ingroeitermijn, rekening houdende met de belangen van zowel <Opdrachtnemer> als <Opdrachtgever> alsmede de eisen van de NIS2-richtlijn en de Cbw. De ingroeitermijnen zijn nader omschreven in artikel 3.5.

3.5. Teneinde <Opdrachtgever> in staat te stellen te voldoen aan de NIS2-richtlijn en de Cbw, zal <Opdrachtnemer>:

a. (OPTIONEEL: binnen …dagen/maanden/jaren) beschikken over: (opnemen gewenste certificeringen zoals NIS2-SC10 / NIS2-SC20 / NIS2-SC30 etc. Zie ANNEX I voor meer informatie).

b. (OPTIONEEL: binnen …dagen/maanden/jaren) voldoen aan de beveiligingsvereisten zoals beschreven in het Cybersecuritybeleid

c. (OPTIONEEL: binnen …dagen/maanden/jaren) voldoen aan de beveiligingsvereisten zoals overeengekomen door partijen en opgenomen in (Bijlage A)

3.6. De Partijen erkennen dat beveiligingseisen en cyberdreigingen een voortdurend veranderende aard hebben, welke een adaptieve en proactieve benadering van cyberbeveiliging vereisen. OPTIONEEL: In dit kader verplicht <Opdrachtnemer> zich ertoe een dynamisch beveiligingsmanagementproces te hanteren, gebaseerd op de Plan-Do-Check-Act (PDCA) cyclus, zoals vereist door de onder 3.5. genoemde certificering of zoals die is in het Cybersecuritybeleid/ Bijlage A

3.7. OPTIONEEL: <Opdrachtnemer> erkent dat de beveiligingseisen zoals opgenomen in het (Cybersecuritybeleid/Bijlage A) aan wijziging onderhevig kunnen zijn. <Opdrachtgever> zal eventuele wijzigingen van het (Cybersecuritybeleid/Bijlage A) tijdig aan <Opdrachtnemer> kenbaar maken. Partijen zullen vervolgens in overleg treden om de aard en omvang van de voorgestelde wijzigingen te bespreken, alsmede de gevolgen daarvan voor de verplichtingen van <Opdrachtnemer> en de tijdlijn voor implementatie. Na het bereiken van overeenstemming zal <Opdrachtnemer> de benodigde maatregelen treffen om de wijzigingen tijdig en in overeenstemming met de afgesproken voorwaarden door te voeren. Alle kosten die samenhangen met de implementatie van de wijzigingen

zullen door <Opdrachtnemer>/<Opdrachtgever> worden gedragen, tenzij anders schriftelijk overeengekomen.
<Opdrachtnemer> zal waar nodig samenwerken en overleggen met <Opdrachtgever> om de risico's voor de beveiliging van haar netwerk- en informatiesystemen van <Opdrachtgever>, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van de diensten van <Opdrachtgever> en voor andere diensten te beperken.

3.8 <Opdrachtnemer> zorgt ervoor dat alle personen die namens <Opdrachtnemer> werkzaamheden in het kader van de Overeenkomst verrichten voor <Opdrachtgever>, adequaat zijn getraind en beschikken over de noodzakelijke kennis op het gebied van (cyber)security.

Artikel 4 Controle en Naleving

4.1. <Opdrachtnemer> zal, in aanvulling artikel 3.5, uiterlijk op (datum) en daarna op eerste verzoek van <Opdrachtgever> een (kopie van een) door een erkende onafhankelijke auditor afgegeven geldig certificaat overleggen zoals omschreven artikel 3.5. sub a. Eventuele kosten die voortvloeien uit het behalen of ter beschikking stellen van het certificaat zijn voor rekening van de (<Opdrachtnemer>/<Opdrachtgever>).

4.2. OPTIONEEL:<Opdrachtgever> heeft het recht toe te (laten) zien op de naleving van de vereisten zoals omschreven in artikel 3.5. <Opdrachtnemer> zal op eerste verzoek <Opdrachtgever>, of een door partijen gezamenlijk aan te wijzen derde partij, toegang verlenen tot alle relevante gegevens, systemen en documenten die vereist zijn voor <Opdrachtgever> om vast te kunnen stellen dat zij voldoet aan de in artikel 3.5. genoemde vereisten, teneinde <Opdrachtgever> in staat te stellen aan haar verplichting op grond van artikel 21 lid 2 sub d NIS2-richtlijn en artikel 23 van de Cbw te voldoen. Eventuele kosten verbonden aan voorgenoemde controle zijn voor rekening van de <Opdrachtgever>.In het geval dat <Opdrachtgever> en <Opdrachtnemer> geen overeenstemming bereiken over de aan te wijzen derde partij, zal de onafhankelijke deskundige op verzoek van een van de partijen worden benoemd door de [bevoegde instantie].

4.3. OPTIONEEL: Indien en voor zover de onder 4.2. genoemde beoordeling van relevante gegevens, systemen en documenten daar aanleiding toe zou geven, zal <Opdrachtnemer>, al dan niet op verzoek van <Opdrachtgever> maatregelen treffen binnen een redelijke termijn.

4.4. Onafhankelijk van bovenstaande zal <Opdrachtnemer> periodiek, haar beveiligingsmaatregelen evalueren en, waar nodig, de maatregelen verbeteren om te blijven voldoen aan de verplichtingen op grond van artikel 3.5.

Artikel 5 Meldingsplicht en samenwerking

5.1. <Opdrachtnemer> erkent dat <Opdrachtgever> op grond van artikel 23 van de NIS2-richtlijn en artikel 27 tot en met 31 van de Cbw en eventuele implementatie wetgeving gerelateerd aan de NIS2, verplicht is Significante Incidenten te melden bij de daarvoor bevoegde autoriteit. <Opdrachtnemer> zal zijn medewerking verlenen en zal de instructies van <Opdrachtgever> opvolgen voor zover vereist voor <Opdrachtgever> om te voldoen aan bovengenoemde verplichtingen.

<u>Melding Significante Incidenten</u>

5.2. <Opdrachtnemer> zal actief zijn beveiliging van netwerk- en informatiesystemen monitoren om Bijna-incidenten, Incidenten of Significante Incidenten te voorkomen.

5.3. <Opdrachtnemer> zal elk Significante Incident onverwijld en in elk geval binnen (24 uur) nadat zij kennis heeft gekregen van het Significante Incident aan <Opdrachtgever> melden. <Opdrachtnemer> zal daarbij aangeven of het Significante Incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt, dan wel grensoverschrijdende gevolgen zou kunnen hebben.
5.4. <Opdrachtnemer> zal in elk geval binnen (72 uur) nadat zij kennis heeft gekregen van een Significante Incident bij <Opdrachtgever> een incidentmelding indienen met, indien van toepassing, een update van de in onder lid 6.3 bedoelde informatie, een initiële beoordeling van het Significante Incident, met inbegrip van de ernst en de gevolgen ervan en, indien beschikbaar, de indicatoren voor aantasting. Ook zal <Opdrachtnemer> op verzoek van <Opdrachtgever> een tussentijds verslag indienen over relevante updates van de situatie.
5.5. <Opdrachtnemer> zal in elk geval binnen (3 weken) nadat zij kennis heeft gekregen van het Significante Incident bij <Opdrachtgever> een eindverslag indienen, inhoudende:

i) een gedetailleerde beschrijving van het Significante Incident, met inbegrip van de ernst en de gevolgen ervan;
ii) het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid;
iii) toegepaste en lopende risicobeperkende maatregelen;
iv) in voorkomend geval, de grensoverschrijdende gevolgen van het incident;

5.6. In afwijking van artikel 6.5. komen partijen overeen dat indien het Significante Incident nog aan de gang is op het moment dat het in artikel 6.5. bedoelde eindverslag wordt ingediend, zal <Opdrachtnemer> op dat moment een voortgangsverslag indienen en binnen één maand nadat zij het Significante Incident hebben afgehandeld, een eindverslag indienen.

<u>Risico beperkende maatregelen</u>

5.7. <Opdrachtnemer> zal bij een Bijna-incident, Incident of Significant Incident risicobeperkende maatregelen nemen die redelijkerwijs van <Opdrachtnemer> kunnen worden verwacht.

Dit Addendum zal aan de geldende Overeenkomst worden gehecht en maakt - na ondertekening - onlosmakelijk onderdeel uit van de Overeenkomst. De overige bepalingen, zoals opgenomen in de Overeenkomst, blijven onverkort van toepassing.

Aldus overeengekomen en ondertekend in tweevoud op (…) te (…).

<Naam>	<Naam >
< Naam vertegenwoordiger >	< Naam>
<Functie>	<Functie>

Plaats: _____ Plaats: _____

Datum: _____ Datum: _____

ANNEX I: Informatie normen A

- Voor bedrijven die leveren aan organisaties die onder de reikwijdte vallen van de NIS2-richtlijn of de Cyberbeveiligingswet (Cbw), biedt NIS2 Supply Chain-certificering in drie niveaus een specifieke invulling voor alle verplichte NIS2-onderdelen.
- Er bestaan meerdere normen, zoals ISO 27001 en NEN 7510. Wij stellen vast dat deze qua scope en leverancierscontrole niet volledig aansluiten op de intentie van de NIS2-richtlijn. Het zijn uitstekende normen. De mogelijkheid bestaat echter dat door het toepassen van “scoping” niet de gehele organisatie aan een audit is onderworpen. Wij adviseren om daar rekening mee te houden. Aanvullend zijn leveranciersbeoordelingen binnen deze normen vaak gericht op IT-leveranciers, terwijl de (aankomende) NIS2 Cyberbeveiligingswet spreekt over “alle gevaren”. Dit wijst ook op leveranciers die op een andere manier een verstoring van digitale systemen kunnen veroorzaken.

Er bestaan ruim 40 verschillende normen. Wij adviseren om de keten niet te zwaar of disproportioneel te belasten en zijn daarom voorstander van NIS2 Supply Chain-certificering. De genoemde standaarden op deze pagina zijn niet volledig en dienen uitsluitend als voorbeeld.

Co-creatie en aanpassingen

Wij geloven in co-creatie. Organisaties of personen die menen dat dit document fouten bevat of die aanvullingen hebben, suggesties, verbeterpunten of andere aanpassingen kunnen die insturen via de Supportdesk van Samen Digitaal Veilig. Het panel van juristen zal dit document regelmatig beoordelen en waar nodig dit document aanpassen.

Dynamiek en nieuwe versies

De NIS2 is volop in beweging. Ten tijde van productie van dit document is de Nederlandse wetgever volop bezig om de NIS2 Richtlijn te implementeren in de Nederlandse wetgeving. Het daarom van belang om regelmatig te checken of er nieuwe versies bestaan van dit document. Die nieuwe versies zullen te vinden zijn op de website samendigitaalveilig.nl. Verder zullen nieuwe versies ook worden verspreid via de samenstellers genoemd in het colofon.

Disclaimer

Dit document wordt uitsluitend als hulpmiddel aangeboden en is bedoeld om algemene informatie te verstrekken over de inkoopvoorwaarden. Hoewel wij ernaar streven om betrouwbare en actuele informatie te verstrekken, garanderen wij niet de volledigheid, nauwkeurigheid, of toepasbaarheid van de inhoud voor specifieke situaties. Gebruikers van dit document kunnen er geen rechten aan ontlenen. Wij accepteren geen aansprakelijkheid voor schade, direct of indirect, die voortvloeit uit of in verband staat met het gebruik van dit document of de daarin verstrekte informatie. Wij adviseren gebruikers nadrukkelijk om, alvorens te handelen op basis van de informatie uit dit document, altijd professioneel juridisch advies in te winnen en de relevantie van de informatie te toetsen aan de lokale wet- en regelgeving. Het gebruik van dit document is op eigen risico van de gebruiker.

Colofon

Deze inkoopvoorden zijn samengesteld door gespecialiseerde juristen in opdracht van en in samenwerking met:

NEVI

Nevi is hét kennisnetwerk voor inkoop, contract- en supply management. We zetten ons in om het inkoopvak naar een hoger niveau te brengen voor het individu, organisaties én de maatschappij. Nevi is er voor iedereen die zich bezighoudt met het inkoopvak. We bundelen inzichten uit het bedrijfsleven, de publieke sector, onderwijs en wetenschap en delen deze kennis in onze krachtige vereniging van 6.500 inkoopprofessionals die elkaar inspireren en stimuleren.

www.nevi.nl

Samen Digitaal Veilig Het platform voor cybersecurity en NIS2.

Samen Digitaal Veilig is een initiatief van MKB-Nederland en VNO-NCW, gericht op het verbeteren van cybersecurity voor bedrijven. De website biedt informatie over cyberveiligheid voor alle bedrijven in Nederland en heeft aanvullend veel aandacht voor de NIS2 richtlijn, die van groot belang is voor bedrijven binnen de EU met betrekking tot cybersecurity.

www.samendigitaalveilig.nl