

Bijlage 20 Addendum Cyberbeveiliging bij de ARBIT-2022

behorend bij de Overeenkomst [titel/kenmerk] tussen de Staat der Nederlanden ([dienstonderdeel]) en [Wederpartij]

Dit Addendum kan worden gesloten bij zowel lopende als nieuwe Overeenkomsten waarop de ARBIT-2022 van toepassing zijn.

Leeswijzer: onder ieder artikellid is in grijs cursief een toelichting opgenomen met de grondslag van de bepaling. Verwijzingen: Cbw = Cyberbeveiligingswet; Cbb = Cyberbeveiligingsbesluit; Cbr = Cyberbeveiligingsregeling (ministeriële regeling(en) bij of krachtens Cbw en Cbb); NIS2 = Richtlijn (EU) 2022/2555; CRA = Verordening (EU) 2024/2847; AVG = Verordening (EU) 2016/679; Aw 2012 = Aanbestedingswet 2012. De toelichting maakt geen deel uit van de contractuele afspraken.

Overwegingen

De ondergetekenden nemen het volgende in aanmerking:

- a. op 15 augustus 2026 is de Cyberbeveiligingswet in werking getreden (implementatie van de NIS2-Richtlijn), die voor Opdrachtgever als essentiële entiteit in de zin van artikel 8, eerste lid, onderdeel g, van die wet verplichtingen meebrengt op het gebied van risicobeheersing, incidentmelding, registratie en beheersing van leveranciers- en ketenrisico's;
- b. de Cyberbeveiligingswet geeft Opdrachtgever geen publiekrechtelijke bevoegdheden jegens haar wederpartijen, zodat de daarvoor benodigde afspraken contractueel moeten worden vastgelegd;
- c. de in dit Addendum opgenomen verplichtingen strekken tot versterking van de digitale weerbaarheid van Opdrachtgever en tot het behoud van duurzame zeggenschap en effectieve controle over de voor haar taakuitoefening benodigde ICT;

Toelichting: Overweging a berust op art. 8 lid 1 onderdeel g Cbw (aanwijzing van overheidsinstanties als essentiële entiteit); de genoemde verplichtingen volgen uit art. 21 Cbw (zorgplicht), art. 25 e.v. Cbw (meldplicht), de registratieplicht van de Cbw en art. 21 lid 3 onderdeel d Cbw (beveiliging van de toeleveringsketen). Overweging b verwoordt dat de Cbw zich uitsluitend tot de entiteit zelf richt: ketenrisicobeheersing moet dus privaatrechtelijk worden geborgd.

en komen het volgende overeen:

Artikel 1 – Begrippen

De begrippen uit de ARBIT-2022 en de Overeenkomst hebben in dit Addendum dezelfde betekenis. Aanvullend gelden de volgende begrippen:

Toelichting: Koppeling aan het begrippenkader van de ARBIT-2022 (art. 1 ARBIT). De aanvullende begrippen in de leden 1.1 tot en met 1.9 volgen de terminologie van art. 1 Cbw (begripsbepalingen).

1.1 Audit: een door of namens Opdrachtgever, dan wel door of namens een toezichthouder of andere bevoegde autoriteit, uitgevoerde controle op de naleving van de Overeenkomst of van toepasselijke wet- en regelgeving, ongeacht het object van de controle, waaronder in ieder geval controles, inspecties, risicoanalyses en beveiligingsscan's op grond van de Cyberbeveiligingswet.

Toelichting: Koepelbegrip voor alle nalevingscontroles (Cbw, AVG, kwaliteit, financieel). De genoemde controlevormen sluiten aan bij de toezichtbevoegdheden van de bevoegde autoriteit op grond van de Cbw (vgl. art. 72 en 83 Cbw); de medewerkingsplicht van Wederpartij volgt uit art. 5.3 ARBIT-2022 (audits bij concrete omstandigheden) en de artikelen 8 van dit Addendum (periodieke audits).

1.2 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.

Toelichting: Definitie uit art. 1 Cbw (implementatie van art. 6, punt 5, NIS2). Het begrip is nodig voor de contractuele kanalisering van de vrijwillige meldingssystematiek van art. 33 Cbw (zie artikel 4.4).

1.3 CSIRT: Computer Security Incident Response Team als bedoeld in art. 16 Cbw.

1.4 Cyberbeveiligingswet (Cbw): de Cyberbeveiligingswet (Stb. 2026, 187);

1.5 Cyberbeveiligingsbesluit (Cbb): het Cyberbeveiligingsbesluit (Stb. 2026, 189);

1.6 Cyberbeveiligingsregeling (Cbr): de ministeriële regeling(en) bij of krachtens de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit, waaronder de regeling waarin de zorgplicht nader wordt ingevuld en de drempelcriteria voor de meldplicht worden bepaald.

Toelichting: De Cbr is een familie van sectorale ministeriële regelingen. Vermeld de toepasselijke regelingen in Bijlage 1 Cyberbeveiligingsafspraken onder 16. Toepasselijke sectorspecifieke regelgeving.

Door de formule "bij of krachtens" lopen het Cbb, de Cbr en toekomstige (sectorspecifieke) regelingen, zoals bedoeld in art. 19 Cbb, automatisch mee zonder heronderhandeling. De Cbr vult de zorgplicht van art. 21 Cbw nader in en bepaalt de drempelcriteria voor de meldplicht van art. 25 Cbw.

1.7 Cyberdreiging: elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden.

Toelichting: Definitie uit art. 1 Cbw jo. art. 6, punt 10, NIS2, dat verwijst naar art. 2, punt 8, van Verordening (EU) 2019/881 (Cyberbeveiligingsverordening). Evenals het Bijna-incident relevant voor de meldstroom van artikel 4.4 (grondslag: art. 33 Cbw).

1.8 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.

Toelichting: Definitie uit art. 1 Cbw. Door de wettelijke definitie over te nemen sluit het contractuele Incident-regime (artikel 4) naadloos aan op de wettelijke meldplicht van Opdrachtgever.

1.9 Significant incident: een Incident dat significant is als bedoeld in artikel 25 van de Cyberbeveiligingswet, met inbegrip van de bij of krachtens die wet bepaalde drempelcriteria.

Toelichting: Definitie uit art. 1 Cbw jo. art. 25 Cbw. De definitie verwijst dynamisch naar de wettelijke significantiecriteria én de bij of krachtens de Cbw bepaalde drempelcriteria (Cbb en sectorale Cyberbeveiligingsregelingen, zie lid 1.6); die lopen daardoor automatisch mee, zodat contract en wet niet uiteenlopen. De significantiebeoordeling zelf blijft aan Opdrachtgever.

De definitie van Inbreuk uit de ARBIT-2022 blijft ongewijzigd; artikel 5 van dit Addendum regelt de samenloop tussen het bestaande Inbreuk-regime en het Incident-regime van dit Addendum.

Toelichting: Afbakening van de twee regimes: Inbreuk ziet op inbreuken in verband met persoonsgegevens (art. 4, punt 12, jo. art. 33 en 34 AVG); Incident op het Cbw-domein.

Artikel 2 – Reikwijdte, doel en rangorde

2.1 Dit Addendum maakt vanaf ondertekening integraal deel uit van de Overeenkomst. De artikelen 3 tot en met 10 gelden voor zover de Prestatie betrekking heeft op netwerk- en informatiesystemen als bedoeld in de Cyberbeveiligingswet.

Toelichting: *Scopingclause: de vergaande Cbw-verplichtingen gelden alleen voor Prestaties met een NIS-component (begrip "netwerk- en informatiesysteem": art. 1 Cbw). Bewust geen uitbreiding naar alle IT: informatieveiligheid is het doel, niet informatiebeveiliging als doel op zich. Artikel 11 kent een eigen, ruimere reikwijdte (zie artikel 11.2).*

2.2 De verplichtingen in dit Addendum strekken tot versterking van de digitale weerbaarheid van Opdrachtgever. Naleving van toepasselijke wettelijke verplichtingen geldt daarbij als minimumniveau; voor zover dit Addendum of de Overeenkomst verdergaande eisen stelt, prevaleren die verdergaande eisen.

Toelichting: *Doelbepaling en uitlegfactor. Wettelijke compliance is de basis, geen plafond: de Cbw en NIS2 (art. 5 NIS2, minimumharmonisatie) verzetten zich niet tegen verdergaande contractuele eisen. Het lid kleurt de uitleg van open normen in de sleutel van digitale weerbaarheid.*

2.3 Bij strijd tussen dit Addendum en de Overeenkomst of de ARBIT-2022 prevaleert dit Addendum, met uitzondering van een tussen partijen gesloten verwerkersovereenkomst, die onverkort van kracht blijft.

Toelichting: *Rangorderegeling. De uitzondering voor de verwerkersovereenkomst waarborgt dat het dwingendrechtelijke kader van art. 28 AVG (verplichte inhoud verwerkersovereenkomst) niet door dit Addendum wordt doorkruist.*

Artikel 3 – Beveiligingsniveau

3.1 In aanvulling op artikel 19.6 ARBIT-2022 omvat de Informatiebeveiliging ten minste de maatregelen als bedoeld in artikel 21, derde lid, van de Cyberbeveiligingswet, nader uitgewerkt bij of krachtens het Cyberbeveiligingsbesluit, waaronder hoofdstuk 4 van dat besluit en de Cyberbeveiligingsregeling, voor zover die betrekking hebben op de Prestatie. De maatregelen zijn evenredig aan de risico's, rekening houdend met de in artikel 21, tweede lid, van de Cyberbeveiligingswet genoemde factoren.

Toelichting: *Kern van het materiële regime. Grondslag: de zorgplicht van art. 21 Cbw — lid 3 somt de verplichte maatregelen categorieën op (o.a. risicoanalyse, incidentenbehandeling, bedrijfscontinuïteit, ketenbeveiliging, cryptografie, personeelsbeveiliging, multifactorauthenticatie), hoofdstuk 4 Cbb en de Cbr werken deze nader uit. De evenredigheidstoets berust op art. 21 lid 2 Cbw. De contractuele doorvertaling is nodig omdat de wet zich tot Opdrachtgever richt en niet tot Wederpartij (overweging b).*

3.2 De maatregelen zijn voorts in overeenstemming met de stand van de techniek en het actuele dreigingsbeeld. Wederpartij beoordeelt periodiek, alsmede na een Incident of bij een gewijzigd dreigingsbeeld, of de maatregelen nog passend zijn, past deze zo nodig aan en informeert Opdrachtgever over materiële aanpassingen.

Toelichting: *Dynamische actualiseringsplicht. Grondslag: het vereiste "rekening houdend met de stand van de techniek" in art. 21 lid 1 Cbw (vgl. art. 21 lid 1 NIS2 en art. 32 AVG) en de plicht de effectiviteit van maatregelen te toetsen (art. 21 lid 3 onderdeel f Cbw; art. 13 Cbb). Wat vandaag passend is, kan morgen ontoereikend zijn; de herbeoordelings- en informatieplicht maakt de norm dynamisch zonder de evenredigheidstoets los te laten.*

Artikel 4 – Melding van Incidenten, dreigingen en kwetsbaarheden

4.1 Wederpartij treft onverwijld alle maatregelen die binnen haar macht liggen om Incidenten te beëindigen en de gevolgen te beperken. Wederpartij informeert Opdrachtgever uiterlijk binnen twaalf (12) uur nadat zij kennis heeft genomen van een Incident, onder vermelding van ten minste: (a) een beschrijving van het Incident en het tijdstip waarop het is vastgesteld; (b) of het Incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt; (c) of het Incident grensoverschrijdende gevolgen kan hebben; (d) de contactgegevens van de functionaris die verantwoordelijk is voor de afhandeling.

Toelichting: Grondslag: art. 25 Cbw verplicht Opdrachtgever tot een vroegtijdige waarschuwing aan het CSIRT en de bevoegde autoriteit binnen 24 uur na kennisname van een Significant incident. De contractuele termijn van 12 uur is daarvan een afgeleide: Opdrachtgever heeft in de keten een voorsprong nodig om zijn eigen wettelijke termijn te halen. De elementen (a) t/m (d) volgen de wettelijk voorgeschreven inhoud van de vroegtijdige waarschuwing (art. 25 Cbw; art. 23 lid 4 NIS2). De termijn loopt vanaf kennisname en vergt geen afgeronde analyse.

4.2 Na de melding als bedoeld in artikel 4.1 verstrekt Wederpartij aan Opdrachtgever: (a) uiterlijk binnen achtenveertig (48) uur: een update van de bedoelde informatie, een initiële beoordeling van het Incident en de ernst en gevolgen ervan, alsmede — indien beschikbaar — de indicatoren voor aantasting; (b) op verzoek van Opdrachtgever: een tussentijds verslag over relevante ontwikkelingen; (c) uiterlijk binnen één maand: een eindverslag met een gedetailleerde beschrijving van het Incident, de ernst en de gevolgen ervan, het type dreiging of de grondoorzaak, de toegepaste en lopende mitigatiemaatregelen en de eventuele grensoverschrijdende gevolgen.

Toelichting: Getrapte vervolgrapportage conform de wettelijke meldsystematiek van art. 27 tot en met 29 Cbw: incidentmelding met beoordeling binnen 72 uur, tussentijdse verslagen op verzoek en een eindverslag binnen één maand. De contractuele 48-uurstermijn geeft Opdrachtgever de ruimte om zijn eigen 72-uursmelding tijdig en volledig te doen; de inhoudselementen van het eindverslag volgen de wettekst. Het begrip "aantasting" in art. 27, lid 1 onderdeel c Cbw verwijst naar het gecompromitteerd of gehackt zijn van de netwerk- en informatiesystemen van de entiteit; het feit dat een aanvaller is binnengedrongen of de systemen heeft weten te compromitteren (Indicators of Compromise uit NIS2).

4.3 Wederpartij laat het doen van meldingen aan het CSIRT en de bevoegde autoriteit als bedoeld in de Cyberbeveiligingswet over aan Opdrachtgever en verleent alle medewerking die redelijkerwijs nodig is om Opdrachtgever in staat te stellen aan haar wettelijke meldplichten te voldoen, waaronder het tijdig verstrekken van alle benodigde informatie en het beschikbaar stellen van technisch personeel.

Toelichting: De meldplicht van art. 25 e.v. Cbw rust op Opdrachtgever als meldplichtige entiteit; kanalisering via Opdrachtgever voorkomt dubbele of tegenstrijdige meldingen. Omdat de Cbw Wederpartij niet bindt, wordt de benodigde medewerking (informatie, technisch personeel) contractueel geborgd.

4.4 Zodra zij daarvan kennis neemt, meldt Wederpartij aan Opdrachtgever tevens Bijna-incidenten en Cyberdreigingen die betrekking hebben op de Prestatie of de netwerk- en informatiesystemen die worden gebruikt bij de uitvoering van de Overeenkomst. De Bijlage Cyberbeveiligingsafspraken of de Service Level Agreement kan de drempel, vorm en frequentie van deze meldingen nader bepalen.

Toelichting: Contractuele regeling van de vrijwillige meldingssystematiek van art. 33 Cbw (vrijwillige melding van bijna-incidenten, cyberdreigingen en niet-significante incidenten). De slotzin bevat de uitdrukkelijke grondslag om drempel, vorm en frequentie in de Bijlage (art. 4) of de SLA nader te bepalen. Zo is realtime melding voorstelbaar bij kritieke systemen terwijl een periodiek dreigingsoverzicht mogelijk volstaat bij standaarddiensten. Zonder die delegatie zou de onvoorwaardelijke meldplicht ("zodra") via de rangorderegel van artikel 2.3 boven een SLA-drempel gaan; nu is de differentiatie die overrapportage en alarmmoetheid voorkomt ook juridisch sluitend. Let op: Waar niets is afgesproken, blijft onverwijld melding het uitgangspunt.

4.5 Wederpartij informeert Opdrachtgever onverwijld over kwetsbaarheden in door haar geleverde of beheerde producten, programmatuur of diensten die betrekking hebben op de Prestatie, en werkt mee aan gecoördineerde bekendmaking van die kwetsbaarheden.

Toelichting: Grondslag: de zorgplichtcategorie kwetsbaarhedenbeheer (art. 21 lid 3 onderdeel e Cbw) en het wettelijke kader voor gecoördineerde openbaarmaking van kwetsbaarheden

(coordinated vulnerability disclosure, art. 17 en art. 34 Cbw, met het CSIRT als coördinator). De procesmatige uitwerking (patchtermijnen) staat in art. 5 van de Bijlage.

Artikel 5 — Samenloop met het Inbreuk-regime

5.1 Indien een gebeurtenis zowel kwalificeert als een Inbreuk in de zin van de ARBIT-2022 als een Incident in de zin van dit Addendum, zijn de artikelen 19.7 tot en met 19.9 ARBIT-2022 en artikel 4 van dit Addendum cumulatief van toepassing. Wederpartij kan in dat geval volstaan met één gecombineerde melding aan Opdrachtgever, mits die melding voldoet aan de eisen en termijnen van beide regimes. Bij strijdigheid van termijnen geldt de kortste termijn.

Toelichting: *Samenloopregeling voor gebeurtenissen die zowel het AVG- als het Cbw-regime raken (bijvoorbeeld ransomware waarbij persoonsgegevens zijn betrokken): de meldplicht bij een Inbreuk berust op art. 33 en 34 AVG, die bij een Incident op art. 25 e.v. Cbw. Een gecombineerde melding met de kortste termijn voorkomt dubbele meldroutes bij één feitelijke gebeurtenis.*

Artikel 6 — Continuïteit en crisisbeheer

6.1 Wederpartij test en evalueert regelmatig haar procedures voor incidentenbehandeling, bedrijfscontinuïteit en crisisbeheer ten behoeve van de uitvoering van de Overeenkomst, en werkt op verzoek van Opdrachtgever mee aan door Opdrachtgever georganiseerde cybercrisisbeheers oefeningen.

Toelichting: *Bewust smal geformuleerd: de plicht om over procedures voor incidentenbehandeling, bedrijfscontinuïteit en crisisbeheer te beschikken volgt reeds uit artikel 3 (via art. 21 lid 3 onderdelen b en c Cbw) en wordt hier niet herhaald. Dit lid regelt uitsluitend wat daaruit niet volgt: de test- en evaluatieplicht (art. 21 lid 3 onderdeel f Cbw; art. 13 Cbb) en de medewerking aan cybercrisisbeheers oefeningen (vgl. art. 20 Cbw). De materiële uitwerking staat in art. 6 van de Bijlage; voor kritieke trajecten kan het facultatieve art. 6b (keten-oefeningen en stresstests) van toepassing worden verklaard.*

Artikel 7 — Aantoonbare naleving

7.1 Wederpartij toont ten minste eenmaal per jaar, alsmede op eerste verzoek van Opdrachtgever, aan dat zij voldoet aan de in artikel 3 bedoelde maatregelen. Daartoe volstaat een geldig, voor de Prestatie relevant certificaat of een gelijkwaardige verklaring van een onafhankelijke, ter zake kundige auditor. De Bijlage Cyberbeveiligingsafspraken kan bepalen dat (a) gelet op het risicoprofiel van de Prestatie een eigen verklaring van Wederpartij volstaat, dan wel (b) een op de Prestatie toegesneden verklaring van een onafhankelijke, ter zake kundige auditor is vereist.

Toelichting: *Opdrachtgever moet de passendheid van de maatregelen, ook in de keten, tegenover de toezichthouder aantoonbaar kunnen maken (art. 21 Cbw jo. de toezichtbevoegdheden van art. 72 e.v. Cbw). Basisniveau is hergebruik van bestaand materiaal (bijv. ISO/IEC 27001, SOC 2), dus minimale extra last; per contract kan in de Bijlage naar beneden (eigen verklaring) of naar boven (toegesneden assurance) worden afgeweken, zodat wordt voldaan aan de evenredigheidstoets van art. 21 lid 2 Cbw en de Gids Proportionaliteit.*

Artikel 8 — Audits

8.1 In aanvulling op artikel 5.3 ARBIT-2022 is Opdrachtgever bevoegd periodiek Audits te (laten) uitvoeren op de naleving van de in artikel 3 bedoelde maatregelen, ook zonder dat sprake is van concrete omstandigheden die daartoe aanleiding geven. De frequentie, de norm en de vorm van deze Audits worden vastgelegd in de Bijlage Cyberbeveiligingsafspraken.

Toelichting: *Onvoorwaardelijk periodiek auditrecht als verificatie-instrument voor de wettelijke ketenrisicobeheersing van Opdrachtgever (art. 21 lid 3 onderdeel d Cbw: beveiliging van de toeleveringsketen). Art. 5.3 ARBIT-2022 vereist "concrete omstandigheden"; dit lid heft*

die drempel voor periodieke cyberbeveiligingsaudits op. De lastenbeperking zit in de Bijlage: frequentie, norm en vorm worden per contract risicogebaseerd bepaald.

8.2 Wederpartij verleent alle medewerking aan Audits door of namens de op grond van de Cyberbeveiligingswet bevoegde autoriteit of het CSIRT, voor zover die betrekking hebben op de Prestatie of op de netwerk- en informatiesystemen die worden gebruikt bij de uitvoering van de Overeenkomst.

Toelichting: Verzekert dat toezichthandelingen van de bevoegde autoriteit of het CSIRT (vgl. art. 72 en 83 Cbw: toezichts- en handhavingsbevoegdheden, waaronder inspecties en beveiligingsscan's) niet stuklopen op de uitbestedingsrelatie. Zonder deze bepaling zou de toezichthouder Opdrachtgever kunnen aanspreken op systemen die feitelijk bij Wederpartij draaien, zonder dat Opdrachtgever medewerking kan afdwingen.

Artikel 9 — Toeleveringsketen

9.1 Bij een verzoek om toestemming voor inschakeling van een derde als bedoeld in artikel 23.1 ARBIT-2022 verstrekt Wederpartij aan Opdrachtgever informatie over de cyberbeveiligingspraktijken van de beoogde derde, waaronder diens beveiligingsmaatregelen, certificeringen en eventuele eerdere Incidenten.

Toelichting: Grondslag: art. 21 lid 3 onderdeel d Cbw verplicht Opdrachtgever tot beheersing van de beveiliging van de toeleveringsketen, met inbegrip van de beoordeling van de algehele kwaliteit en cyberbeveiligingspraktijken van leveranciers en verwerkers. Dit lid maakt die beoordeling mogelijk op het natuurlijke moment: het toestemmingsverzoek bij onderaanneming (art. 23.1 ARBIT-2022).

9.2 Wederpartij legt de cyberbeveiligingsverplichtingen uit dit Addendum, waaronder in ieder geval de artikelen 3, 4, 6 en 7, schriftelijk op aan de door haar ingeschakelde derden en ziet toe op de naleving daarvan.

Toelichting: Back-to-back-doorlegging in de keten. De zorgplicht van art. 21 lid 3 onderdeel d Cbw strekt zich uit tot de gehele toeleveringsketen; omdat de wet geen rechtstreekse verplichtingen op onderaannemers legt, moet de doorwerking contractueel worden geborgd. De genoemde kernartikelen (beveiligingsniveau, melding, continuïteit, aantoonbaarheid) zijn het minimum dat de meldketen en het beveiligingsniveau in de keten sluitend houdt.

9.3 Het auditrecht van Opdrachtgever strekt zich mede uit tot deze derden, voor zover dat noodzakelijk is voor de beoordeling van de naleving van de cyberbeveiligingsverplichtingen.

Toelichting: Sluistuk van de ketenrisicobeheersing (art. 21 lid 3 onderdeel d Cbw): zonder doorwerkend auditrecht is de naleving in de keten niet verifieerbaar. De noodzakelijkheidsclausule begrenst het recht conform het evenredigheidsbeginsel (art. 21 lid 2 Cbw).

Artikel 10 — Leveranciersbeperking (artikel 21a Cbw)

10.1 Indien Opdrachtgever op grond van artikel 21a van de Cyberbeveiligingswet wordt verplicht in aangewezen onderdelen van haar netwerk- en informatiesystemen geen gebruik meer te maken van producten of diensten van een door de minister aangewezen leverancier, en deze verplichting betrekking heeft op de Prestatie, is Opdrachtgever gerechtigd de Overeenkomst bij schriftelijke kennisgeving eenzijdig te wijzigen of geheel of gedeeltelijk te beëindigen voor zover noodzakelijk om aan die verplichting te voldoen. De rechtsgevolgen worden in overleg tussen partijen vastgesteld, met dien verstande dat Wederpartij in ieder geval recht heeft op vergoeding van de redelijke kosten die rechtstreeks voortvloeien uit de wijziging of beëindiging.

Toelichting: Ordening van het wettelijke risico van art. 21a Cbw (bevoegdheid van de minister om het gebruik van producten of diensten van een aangewezen leverancier in aangewezen onderdelen van netwerk- en informatiesystemen te verbieden). Het wijzigings- en gedeeltelijk beëindigingsrecht is begrensd tot het noodzakelijke; de kostenvergoeding houdt de bepaling evenwichtig en aanbestedingsrechtelijk houdbaar.

Artikel 11 — Producten met digitale elementen (Cyber Resilience Act)

11.1 Indien de Prestatie producten met digitale elementen omvat als bedoeld in Verordening (EU) 2024/2847 (Cyber Resilience Act), geleidt Wederpartij onverwijld aan Opdrachtgever door: (a) informatie die de fabrikant op grond van artikel 14 van die verordening beschikbaar stelt over actief uitgebuite kwetsbaarheden van en ernstige incidenten met gevolgen voor de beveiliging van die producten, alsmede (b) door de fabrikant beschikbaar gestelde beveiligingsupdates en andere corrigerende of risicobeperkende maatregelen.

***Toelichting:** Grondslag: art. 14 CRA legt de fabrikant per 11 september 2026 een meldplicht op voor actief uitgebuite kwetsbaarheden en ernstige incidenten; via de overgangsbepaling van art. 69 CRA geldt die ook voor producten die dan al in de handel zijn. De fabrikant meldt echter aan het CSIRT en ENISA — niet aan de afnemer — en Wederpartij is vaak wederverkoper of dienstverlener, geen fabrikant. Dit lid slaat die brug: fabrikantinformatie die Wederpartij bereikt moet onverwijld worden doorgeleid, zodat Opdrachtgever tijdig kan patchen en zijn eigen zorg- en meldplichten (art. 21 en 25 e.v. Cbw; artikel 3 en 4 van dit Addendum) kan nakomen. De verdergaande producteisen van de CRA per 11 december 2027 zijn bewust nog niet verwerkt.*

11.2 In afwijking van artikel 2.1 geldt dit artikel ongeacht of de Prestatie betrekking heeft op netwerk- en informatiesystemen als bedoeld in de Cyberbeveiligingswet.

***Toelichting:** De CRA hanteert een productbegrip ("product met digitale elementen", art. 3 CRA) dat losstaat van het begrip netwerk- en informatiesysteem uit de Cbw. Artikel 11 valt daarom buiten de NIS-scoping van artikel 2.1 en geldt voor alle producten met digitale elementen, ook buiten NIS-bereik.*

11.3 Voor zover Wederpartij de systemen beheert of exploiteert waarin de in artikel 11.1 bedoelde producten worden gebruikt, past zij de door de fabrikant beschikbaar gestelde beveiligingsupdates toe binnen de termijnen van artikel 5 van de Bijlage Cyberbeveiligingsafspraken; dat artikel is daartoe van overeenkomstige toepassing ongeacht of de Prestatie betrekking heeft op netwerk- en informatiesystemen als bedoeld in de Cyberbeveiligingswet. Indien toepassing binnen die termijn aantoonbaar tot een onaanvaardbaar risico voor de continuïteit van de dienstverlening leidt, treft Wederpartij onverwijld compenserende maatregelen en meldt zij dit gemotiveerd aan Opdrachtgever, onder vermelding van de termijn waarbinnen toepassing alsnog plaatsvindt. Voor producten in systemen die Opdrachtgever zelf beheert, ondersteunt Wederpartij Opdrachtgever op diens verzoek en tegen redelijke voorwaarden bij de toepassing van die updates.

***Toelichting:** Sluit de kloof tussen informatieplicht en actieplicht: zonder dit lid gold voor producten buiten NIS-bereik wél de doorgeleidingsplicht van artikel 11.1, maar geen contractuele plicht de doorgeleide update toe te passen (Bijlage art. 5 geldt via artikel 2.1 immers alleen binnen NIS-scope). De toepassingsplicht is gedifferentieerd naar rol: alleen waar Wederpartij beheert of exploiteert (scenario A) kan zij patchen; bij producten in systemen van Opdrachtgever zelf (scenario B) geldt een ondersteuningsplicht. Het continuïteitsventiel voorkomt dat een overhaaste noodpatch zelf een verstoring veroorzaakt; de compenserende maatregelen en de gemotiveerde melding houden het risico beheerst en controleerbaar. Grondslag: art. 14 CRA (informatiestroom fabrikant), art. 21 lid 3 onderdeel e Cbw en art. 12 Cbb (kwetsbaarhedenbeheer binnen NIS-scope); daarbuiten een zuiver contractueel verlengstuk daarvan.*

Artikel 12 — Boetevrijwaring en aansprakelijkheid

12.1 Wederpartij vrijwaart Opdrachtgever tegen bestuurlijke boetes die de op grond van de Cyberbeveiligingswet bevoegde autoriteit aan Opdrachtgever oplegt wegens niet-naleving van de bij of krachtens die wet gestelde verplichtingen, voor zover die niet-naleving het gevolg is van een toerekenbare tekortkoming van Wederpartij in de nakoming van de Overeenkomst.

***Toelichting:** De bevoegde autoriteit kan Opdrachtgever — ook als overheidsinstantie — bestuurlijke boetes opleggen (art. 80 Cbw: voor essentiële entiteiten tot € 10 miljoen of 2% van de wereldwijde jaaromzet; Nederland heeft de lidstaatoptie van art. 34 lid 7 NIS2 benut*

om ook overheidsinstanties beboetbaar te maken). Een opgelegde boete is vermogensschade (art. 6:95 BW); de vrijwaring legt dat risico bij de veroorzaker, maar uitsluitend voor zover de niet-naleving het gevolg is van een toerekenbare tekortkoming van Wederpartij (art. 6:74 BW).

12.2 Voor Overeenkomsten waarbij dit Addendum deel uitmaakte van de uitvraag geldt dat aan artikel 26 lid 4 ARBIT-2022 een onderdeel e wordt toegevoegd, luidende:

e. in geval van aanspraken op schadevergoeding ten gevolge van het toerekenbaar tekortschieten in de nakoming van verplichtingen uit het Addendum Cyberbeveiliging. Onder schade wordt mede begrepen een door de toezichthoudende autoriteit opgelegde boete.

Toelichting: De onder e opgenomen uitzondering heeft betrekking op schade als gevolg van het toerekenbaar tekortschieten in de nakoming van de cyberbeveiligingsverplichtingen uit dit Addendum. De digitale weerbaarheid van de overheid beschermt de continuïteit van de publieke dienstverlening en daarmee het maatschappelijk verkeer dat daarvan afhankelijk is; falende cyberbeveiliging kan tot ernstige en zich kettingsgewijs uitbreidende schade leiden, ook bij derden. Door de toegenomen digitalisering, uitbesteding en dreiging heeft de Europese en nationale wetgever met de NIS2-richtlijn en de Cyberbeveiligingswet in 2026 een krachtiger beschermingsregime geïntroduceerd. Dat heeft de financiële risico's van tekortschietende cyberbeveiliging substantieel vergroot: niet alleen omdat de bevoegde autoriteit hoge boetes kan opleggen (art. 80 Cbw), maar ook vanwege de kosten die zijn gemoeid met het herstellen, voorkomen en beperken van schade. Voor de verdeling van deze risico's is aansluiting gezocht bij het adagium "de vervuiler betaalt": de wet legt de verantwoordelijkheid bij Opdrachtgever, maar bij uitbesteding ligt de feitelijke naleving in handen van Wederpartij; wie toerekenbaar tekortschiet, draagt de gevolgen. Maximeren van deze aansprakelijkheid zou afbreuk doen aan de door de wetgever beoogde doeltreffende, evenredige en afschrikkende handhaving. Ter verduidelijking is bepaald dat het begrip schade mede door de toezichthoudende autoriteit opgelegde boetes omvat. De uitzondering geldt uitsluitend voor Overeenkomsten waarbij het Addendum deel uitmaakte van de uitvraag: inschrijvers kennen het risico dan vooraf en kunnen het in hun prijs verdisconteren. Bij lopende Overeenkomsten blijft het reguliere regime van art. 26 ARBIT-2022 gelden, naast de vrijwaring van artikel 12.1; de uitbreiding van de uitzonderingen zou daar het economisch evenwicht ten nadele van Wederpartij wijzigen en daarmee al snel een wezenlijke wijziging opleveren (art. 2.163g Aw 2012).

Artikel 13 — Bijlage Cyberbeveiligingsafspraken

13.1 De als Bijlage 1 aangehechte Bijlage Cyberbeveiligingsafspraken maakt integraal deel uit van dit Addendum. Voor zover invulvelden bij ondertekening nog niet zijn ingevuld, vullen partijen deze gezamenlijk in binnen [drie] maanden na ondertekening; tot dat moment gelden de in de Bijlage genoemde standaardregels, waaronder BIO2 als normenkader.

Toelichting: Uitwerking van de taakverdeling "het 'wat' in de Voorwaarden, het 'hoe' in de Bijlage": het Addendum bevat de uniforme verplichtingen, de Bijlage de contractspecifieke invulling conform de evenredigheidstoets van art. 21 lid 2 Cbw. De invulregeling met standaardregels voorkomt dat een niet-ingevulde bijlage tot een normvacuüm leidt; BIO2 is het uitgangspunt omdat zij voor overheidsorganisaties het verplichte basisnormenkader vormt.

Artikel 14 — Meerkosten

14.1 Voor Overeenkomsten die vóór ondertekening van dit Addendum zijn gesloten geldt: aantoonbare, redelijke meerkosten die rechtstreeks en uitsluitend voortvloeien uit de verplichtingen van dit Addendum, komen op basis van een vooraf door Wederpartij in te dienen en door Opdrachtgever goed te keuren specificatie voor vergoeding in aanmerking, volgens de wijzigingsprocedure van de Overeenkomst. Kosten van maatregelen waartoe Wederpartij reeds op grond van de Overeenkomst, de wet of haar eigen zorgplicht gehouden was, komen niet voor vergoeding in aanmerking.

Toelichting: De "contractuele smeerolie" voor lopende overeenkomsten: het Addendum vergt instemming van Wederpartij en de meerkostenregeling maakt die instemming redelijkerwijs verkrijgbaar.

Let op: Als wijziging van de Overeenkomst een aanbestedingsrechtelijke grondslag vereist, leg die dan vast in het inkoopdossier.

14.2 Voor Overeenkomsten waarbij dit Addendum deel uitmaakte van de offerteaanvraag geldt dat de kosten van naleving geacht worden in de prijzen te zijn verdisconteerd.

Toelichting: Bij nieuwe overeenkomsten wordt het Addendum als bijlage bij de offerteaanvraag gevoegd en in de overeenkomst van toepassing verklaard; het kostenrisico ligt dan bij de inschrijver, die er bij prijsstelling rekening mee kon houden. Dit sluit aan bij het transparantie- en gelijkheidsbeginsel van het aanbestedingsrecht (art. 1.9 Aw 2012).

Artikel 15 — Duur en overgang

15.1 Dit Addendum treedt in werking op de datum van ondertekening door beide partijen, doch niet eerder dan 15 augustus 2026, en geldt voor de resterende duur van de Overeenkomst, verlengingen daaronder begrepen.

Toelichting: De ondergrens van 15 augustus 2026 is gekoppeld aan de inwerkingtreding van de Cbw: eerdere gelding zou verplichtingen activeren waarvan de wettelijke referentiekaders (Cbb, Cbr) nog niet in werking zijn.

15.2 Voor het overige blijft de Overeenkomst ongewijzigd van kracht.

Toelichting: Standaard slotbepaling: het Addendum wijzigt de Overeenkomst uitsluitend op de in dit Addendum geregelde onderwerpen.

Aldus overeengekomen en in tweevoud ondertekend:

De Staat der Nederlanden (Opdrachtgever)	[Naam Wederpartij]
Naam:	Naam:
Functie:	Functie:
Datum:	Datum:
Handtekening:	Handtekening:

Bijlage 1 — Bijlage Cyberbeveiligingsafspraken

Involvelden zijn geel gemarkeerd en moeten per Overeenkomst worden ingevuld.

1. Toepassingsbereik

Deze bijlage is van toepassing op de onderdelen van de Prestatie die betrekking hebben op netwerk- en informatiesystemen als bedoeld in de Cyberbeveiligingswet. De Prestatie betreft (aankruisen wat van toepassing is):

☐ Scenario A: Wederpartij levert, beheert of exploiteert een netwerk- en informatiesysteem ten behoeve van Opdrachtgever.

☐ Scenario B: Wederpartij levert producten of diensten die worden gebruikt in een netwerk- en informatiesysteem van Opdrachtgever.

Beschrijving van de betrokken systemen en diensten: [per contract in te vullen]

Toelichting: De scenario-indeling volgt de twee rollen die een leverancier ten opzichte van een Cbw-plichtige opdrachtgever kan hebben binnen de ketenrisicobeheersing van art. 21 lid 3 onderdeel d Cbw: exploitant of beheerder van een netwerk- en informatiesysteem (scenario A) dan wel toeleverancier van producten of diensten die in zo'n systeem worden gebruikt

(scenario B). De systeembeschrijving bakent de reikwijdte van alle volgende artikelen af (vgl. artikel 2.1 van het Addendum).

2. Cyberbeveiligingsmaatregelen

Wederpartij treft ten aanzien van de in artikel 1 bedoelde systemen en diensten de maatregelen als bedoeld in artikel 3 van het Addendum. De concrete invulling wordt per contract bepaald aan de hand van de hiernavolgende artikelen en het bij de Overeenkomst behorende beveiligingsplan.

Toelichting: Scharnierbepaling: zij koppelt de Bijlage aan de materiële norm van artikel 3 van het Addendum (art. 21 lid 3 Cbw, hoofdstuk 4 Cbb, Cbr). Zo blijft er één normatieve bron met één uitwerkingsslaag.

3. Normenkader

Wederpartij richt de Informatiebeveiliging in overeenkomstig de volgende normen en kaders: Baseline Informatiebeveiliging Overheid 2 (BIO2), aangevuld met: [per contract in te vullen, bijvoorbeeld: NEN-EN-ISO/IEC 27001, NEN-EN-ISO/IEC 27002, NEN 7510 of andere sectorspecifieke normen]

Toelichting: Legt vast tegen welk normenkader wordt ingericht én getoetst (vgl. artikel 7 van het Addendum). BIO2 is het uitgangspunt omdat zij voor overheidsorganisaties het verplichte basishandboek vormt dat de zorgplicht van art. 21 Cbw operationaliseert. Let wel: toepasselijkheid van BIO2 of ABRO vervangt de contractspecifieke invulling van de overige artikelen niet — die kaders richten zich tot de overheidsorganisatie en laten concrete waarden (RTO/RPO, patch- en meldtermijnen, auditfrequentie) bewust open (zie het kritiekdocument BIO2/ABRO). Bij samenloop met de ABRO gaan de ABRO-eisen bij strijdigheid voor, voor zover zij strekken tot bescherming van de nationale veiligheid.

4. Incidentmeldprocedure

Voor de melding van Incidenten, Bijna-incidenten en Cyberdreigingen gelden de artikelen 4 en 5 van het Addendum. De operationele classificatie en termijnen zijn vastgelegd in de Service Level Agreement. Contactgegevens voor incidentmeldingen: [per contract in te vullen: contactpersoon, e-mailadres, telefoonnummer, beschikbaarheid]

Toelichting: Operationalisering van de meldplichten van artikel 4 en 5 van het Addendum (art. 25 t/m 29 en 33 Cbw): de juridische termijnen staan in het Addendum, de praktische afhandeling (classificatie, contactgegevens, bereikbaarheid) hier en in de SLA. De incidentclassificatie in de SLA bepaalt onder meer de drempel voor de melding van Bijna-incidenten en Cyberdreigingen.

5. Kwetsbaarhedenbeheer

Ter nadere uitwerking van artikel 4.5 van het Addendum hanteert Wederpartij een gedocumenteerd proces voor het identificeren, beoordelen en verhelpen van kwetsbaarheden in de bij de Prestatie gebruikte systemen en programmatuur. Wederpartij past beveiligingsupdates toe binnen de volgende termijnen: [per contract in te vullen, bijvoorbeeld: kritieke kwetsbaarheden binnen 48 uur, hoge kwetsbaarheden binnen 7 dagen, overige binnen 30 dagen]. Voor systemen die Wederpartij beheert of exploiteert omvat dit proces de feitelijke toepassing van beveiligingsupdates binnen de genoemde termijnen, met inbegrip van de op grond van artikel 11.1 van het Addendum doorgeleide updates; artikel 11.3 van het Addendum verklaart dit artikel van overeenkomstige toepassing op producten met digitale elementen buiten NIS-bereik.

Toelichting: Uitwerking van artikel 4.5 van het Addendum (art. 21 lid 3 onderdeel e Cbw: kwetsbaarhedenbeheer en -bekendmaking; art. 17 en 34 Cbw: gecoördineerde openbaarmaking). De voorbeeldtermijnen volgen gangbare praktijk; bij kritieke systemen kunnen zij worden aangescherpt. De slotzin verbindt dit artikel met de CRA-doorgeleiding van artikel 11 van het Addendum: informatie- en actieplicht vormen zo één keten, ook buiten NIS-bereik (zie artikel 11.3, inclusief het continuïteitsventiel aldaar).

6. Bedrijfscontinuïteit

Ter nadere uitwerking van de artikelen 3 en 6 van het Addendum beschikt Wederpartij over de volgende plannen en procedures: [per contract in te vullen, bijvoorbeeld: bedrijfscontinuïteitsplan, disaster recovery plan, maximale hersteltijd (RTO), maximaal gegevensverlies (RPO), testfrequentie]

Toelichting: Uitwerking van de continuïteitsmaatregelen van art. 21 lid 3 onderdelen b en c Cbw (incidentenbehandeling; bedrijfscontinuïteit, back-upbeheer en crisisbeheer) en de test- en evaluatieplicht van artikel 6 van het Addendum: welke plannen bestaan, welke hersteldoelen gelden (RTO/RPO) en hoe vaak wordt getest.

6a. Zeggenschap en controle

Wederpartij richt de Prestatie zodanig in dat Opdrachtgever duurzame zeggenschap en effectieve controle behoudt over het gebruik, de wijziging, de beveiliging, de voortzetting, de migratie en de beëindiging van de bij de Prestatie geleverde of gebruikte systemen en gegevens. Daartoe waarborgt Wederpartij ten minste dat: (a) gegevens en configuraties op verzoek van Opdrachtgever in een open, gedocumenteerd en machineleesbaar formaat kunnen worden geëxporteerd; (b) geen technische of contractuele voorzieningen worden toegepast die migratie naar een andere leverancier of omgeving belemmeren; (c) Opdrachtgever inzicht heeft in de jurisdicties van waaruit de Prestatie wordt geleverd en van waaruit toegang tot gegevens mogelijk is, en wijzigingen daarin vooraf worden gemeld; (d) [per contract in te vullen, bijvoorbeeld: broncode-escrow, terugvalvoorziening, datalocatie-eisen, exit-ondersteuning].

Toelichting: Operationele uitwerking van de doelstelling van duurzame zeggenschap en effectieve controle. De onderdelen a en b sluiten aan op de cloud-overstap- en exitverplichtingen van de Data Act (Verordening (EU) 2023/2854, hoofdstuk VI); onderdeel c regelt jurisdictie-transparantie (relevant voor extraterritoriale wetgeving); onderdeel d is een invulveld voor zwaardere waarborgen bij verhoogd risico.

6b. Keten-oefeningen en stresstests [OPTIONEEL – van toepassing indien aangekruist: ()]

Wederpartij neemt periodiek deel aan door of namens Opdrachtgever georganiseerde ketenbrede tabletop-simulaties en stresstests, waarin onder meer de meldketen — van detectie van een Incident door een ingeschakelde derde tot de melding aan Opdrachtgever en de bevoegde autoriteit — en de herstelprocedures feitelijk worden beproefd. Wederpartij draagt er zorg voor dat de door haar ingeschakelde derden aan deze oefeningen deelnemen voor zover hun rol in de keten dat vereist. Frequentie, scope, testomgeving en spelregels: [per contract in te vullen]. Kostenverdeling: [per contract in te vullen]. Indien Wederpartij een dienst aan meerdere afnemers levert en deelname aan klantspecifieke oefeningen redelijkerwijs niet van haar kan worden gevergd, kan zij volstaan met deelname aan een eigen, gelijkwaardig oefenprogramma en met rapportage aan Opdrachtgever over de voor de Prestatie relevante uitkomsten. Bevindingen uit oefeningen en stresstests gelden op zichzelf niet als tekortkoming in de nakoming van de Overeenkomst, maar verplichten Wederpartij tot het opstellen en uitvoeren van een verbeterplan binnen een door partijen overeen te komen redelijke termijn.

Toelichting: Facultatief artikel voor kritieke inkooptrajecten, gebaseerd op artikel 6 van het Addendum en art. 20 Cbw (cybercrisisbeheersoefeningen), met doorlegging naar derden via artikel 9. Certificeringen toetsen opzet en werking van maatregelen, maar niet de ketencoördinatie onder tijdsdruk; alleen een feitelijke simulatie legt bloot of de meldtermijn van artikel 4.1 door de gehele keten haalbaar is. De safe harbour (bevindingen zijn geen tekortkoming, wel verbeterplicht) voorkomt defensief oefengedrag; de rapportagevariant voorkomt onuitvoerbaarheid bij multi-tenant diensten.

7. Toeleveringsketen

Ter nadere uitwerking van artikel 9 van het Addendum verstrekt Wederpartij bij aanvang van de Overeenkomst en vervolgens bij iedere wijziging een overzicht van de derden die betrokken zijn bij de uitvoering van de Prestatie, met vermelding van: (a) de naam en vestigingsplaats van de derde; (b) de aard van de door de derde geleverde diensten of producten; (c) de

cyberbeveiligingsmaatregelen die op de derde van toepassing zijn; (d) of de derde kritiek is voor de beveiliging of continuïteit van de Prestatie.

Wederpartij overlegt op eerste verzoek van Opdrachtgever de bepalingen uit haar overeenkomsten met deze derden waaruit blijkt dat de cyberbeveiligingsverplichtingen overeenkomstig artikel 9.2 van het Addendum schriftelijk zijn opgelegd. Commercieel vertrouwelijke onderdelen mogen onleesbaar worden gemaakt.

Toelichting: *Uitwerking van artikel 9 van het Addendum: een actueel ketenoverzicht stelt Opdrachtgever in staat zijn wettelijke ketenrisicobeheersing (art. 21 lid 3 onderdeel d Cbw) aantoonbaar in te vullen, ook tegenover de toezichthouder.*

Met de inzageplicht kan Opdrachtgever de doorlegging vaststellen zonder een audit. Zo'n audit vormt voor Wederpartij namelijk een veel grotere last.

8. Audits en rapportage

Ter nadere uitwerking van artikel 8 van het Addendum worden Audits op de naleving van de cyberbeveiligingsverplichtingen uitgevoerd met de volgende periodiciteit: **[per contract in te vullen, bijvoorbeeld: jaarlijks een externe audit, halfjaarlijks een penetratietest]**. Wederpartij rapporteert ten minste **[halfjaarlijks/jaarlijks]** aan Opdrachtgever over: (a) de naleving van de in artikel 3 van het Addendum bedoelde maatregelen; (b) de resultaten van uitgevoerde beveiligingsaudits en penetratietesten; (c) geconstateerde kwetsbaarheden en de naar aanleiding daarvan getroffen maatregelen; (d) wijzigingen in het risicoprofiel van de Prestatie. (e) **[OPTIONEEL – bij verhoogd risicoprofiel:]** geldige certificaten of gelijkwaardige verklaringen van de in het overzicht van artikel 7 als kritiek aangemerkte derden. De rapportage geschiedt in een door Opdrachtgever voorgeschreven format.

Toelichting: *Uitwerking van het periodieke auditrecht (artikel 8 Addendum; art. 5.3 ARBIT-2022) en de aantoonplicht (artikel 7 Addendum): hier wordt per contract bepaald welke auditvorm, frequentie en welk rapportageformat gelden — en daarmee op welke trede van de getrapte aantoonplicht het contract zit. De zwaarte volgt het risicoprofiel, conform art. 21 lid 2 Cbw.*

9. Medewerking bevoegde autoriteit

Wederpartij informeert Opdrachtgever onverwijld indien een bevoegde autoriteit of het CSIRT zich in het kader van de Cyberbeveiligingswet rechtstreeks tot haar wendt met een verzoek of toezichthandeling die de Prestatie raakt, tenzij een wettelijk voorschrift dat verbiedt, en stemt haar reactie waar mogelijk vooraf met Opdrachtgever af. Contactpunt en doorlooptijden: **[per contract in te vullen]**

Toelichting: *De medewerkingsplicht zelf staat in artikel 8.2 van het Addendum (vgl. art. 72 en 83 Cbw) en wordt hier niet herhaald; dit artikel regelt uitsluitend het "hoe": onverwijld notificatie en afstemming wanneer de toezichthouder of het CSIRT zich rechtstreeks tot Wederpartij wendt. Zonder deze plicht zou Opdrachtgever — die tegenover de toezichthouder verantwoording aflegt — van dat contact niet weten. Het voorbehoud ("tenzij een wettelijk voorschrift dat verbiedt") ziet op wettelijke geheimhoudingsplichten, bijvoorbeeld bij strafrechtelijk onderzoek.*

10. Cryptografiebeleid

Wederpartij past bij de uitvoering van de Prestatie cryptografische maatregelen toe die voldoen aan de volgende eisen: **[per contract in te vullen, bijvoorbeeld: toe te passen encryptiestandaarden, eisen aan sleutelbeheer, beleid ten aanzien van algoritme-migratie — waaronder de migratie naar post-quantumcryptografie conform de actuele adviezen van NCSC en AIVD —, eisen aan crypto-agility en de noodzakelijke beschermingstermijn van de gegevens]**

Toelichting: *Uitwerking van de maatregelen categorie cryptografie en encryptie (art. 21 lid 3 onderdeel h Cbw; art. 15 Cbb). De PQC-elementen (crypto-agility, migratiepad, beschermingstermijn) staan in de Bijlage (het 'hoe') zodat de ARBIT-2022 inclusief Addendum*

technologieneutraal blijven. Vast aandachtspunt in de Bijlage bij lange vertrouwelijkheidsduur en contracten voorbij 2030.

11. Authenticatie en beveiligde communicatie

Wederpartij past bij de uitvoering van de Prestatie de volgende authenticatie- en communicatiebeveiligingsmaatregelen toe: [per contract in te vullen, bijvoorbeeld: multifactorauthenticatie, beveiligde communicatiekanalen, continue authenticatieoplossingen]

Toelichting: Uitwerking van de maatregelencategorie multifactorauthenticatie en beveiligde communicatie (art. 21 lid 3 onderdeel j Cbw; art. 17 Cbb).

12. Personeelsbeveiliging en toegangsbeheer

Wederpartij treft ten aanzien van het personeel dat betrokken is bij de uitvoering van de Prestatie de volgende maatregelen: [per contract in te vullen, bijvoorbeeld: screening, need-to-know, least-privilege, assetmanagement, toegangsbeleid]

Toelichting: Uitwerking van de maatregelencategorie personeelsbeveiliging, toegangsbeleid en assetmanagement (art. 21 lid 3 onderdeel i Cbw; art. 16 Cbb). Aanvullend gelden de personele voorschriften van art. 19.2 t/m 19.5 ARBIT-2022 (VOG, veiligheidsonderzoek).

13. Opleiding en bewustwording

Wederpartij draagt er zorg voor dat het personeel dat betrokken is bij de uitvoering van de Prestatie aantoonbaar en periodiek wordt opgeleid en getraind op het gebied van cyberbeveiligingsrisico's en -maatregelen, overeenkomstig de eisen van artikel 24 van de Cyberbeveiligingswet.

Toelichting: Grondslag: art. 24 Cbw (opleidingsplicht — bestuurders en medewerkers moeten aantoonbaar over relevante kennis en vaardigheden beschikken) en de maatregelencategorie cyberhygiëne en training (art. 21 lid 3 onderdeel g Cbw). Doorvertaling naar het leveranciersdomein: ook ingehuurd of uitbesteed personeel in de keten moet getraind zijn.

14. Secure development en SBOM

Indien de Prestatie mede omvat het ontwikkelen of onderhouden van programmatuur, hanteert Wederpartij de volgende veilige ontwikkelprocedures: [per contract in te vullen, bijvoorbeeld: secure development lifecycle, beveiligingstesten, configuratiemanagement]. Voor programmatuur die Wederpartij zelf ontwikkelt of onderhoudt levert Wederpartij periodiek — en ten minste bij iedere release — een actuele Software Bill of Materials (SBOM) in een machineleesbaar formaat [per contract in te vullen, bijvoorbeeld: SPDX of CycloneDX]. Voor overige producten met digitale elementen verstrekt Wederpartij de SBOM van de fabrikant voor zover deze redelijkerwijs verkrijgbaar is.

Toelichting: Uitwerking van de maatregelencategorie beveiliging bij verwerving, ontwikkeling en onderhoud van netwerk- en informatiesystemen, inclusief kwetsbaarhedenbeheer (art. 21 lid 3 onderdeel e Cbw; art. 12 Cbb). De SBOM-eis is aangescherpt: voor eigen ontwikkel- en onderhoudswerk een leverplicht (periodiek, machineleesbaar), voor standaardproducten van derden een inspanningsplicht — een fabrikant is onder de CRA wel verplicht een SBOM op te stellen (bijlage I CRA), maar niet om die aan afnemers te verstrekken, zodat Wederpartij daarvoor niet onvoorwaardelijk kan instaan. Een machineleesbare SBOM maakt het kwetsbaarhedenbeheer van art. 5 automatiseerbaar en versnelt de beoordeling bij doorgeleide fabrikantmeldingen (artikel 11 Addendum).

15. Effectiviteitsbeoordeling

Wederpartij beoordeelt periodiek de effectiviteit van de getroffen cyberbeveiligingsmaatregelen. De frequentie en methode van beoordeling zijn: [per contract in te vullen]

Toelichting: Grondslag: art. 21 lid 3 onderdeel f Cbw (beleid en procedures om de effectiviteit van maatregelen te beoordelen; art. 13 Cbb). Sluit de plan-do-check-act-cyclus: niet de toezegging maar de geverifieerde feitelijke werking staat centraal (vgl. artikel 7 van het Addendum).

16. Toepasselijke sectorspecifieke regelgeving

Op de Overeenkomst zijn de volgende ministeriële regelingen bij of krachtens de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit van toepassing (waaronder de Cyberbeveiligingsregeling en sectorspecifieke regelingen als bedoeld in artikel 19 van dat besluit): **[per contract in te vullen]**. Indien gedurende de looptijd op grond van artikel 19 van het Cyberbeveiligingsbesluit nadere eisen worden gesteld, kan Opdrachtgever deze bij schriftelijke kennisgeving van toepassing verklaren; Wederpartij voldoet daaraan binnen een door Opdrachtgever te bepalen redelijke implementatietermijn.

Toelichting: Grondslag: art. 19 Cbb (grondslag voor sectorspecifieke ministeriële regelingen met nadere eisen). De bepaling combineert de opsomming van reeds toepasselijke regelingen met een kapstok voor toekomstige regelgeving, inclusief redelijke implementatietermijn — de contractuele pendant van de dynamische verwijzing “bij of krachtens” (lid 1.6) en de actualiseringsplicht (artikel 3.2).

Toelichting voor gebruik (geen onderdeel van het Addendum)

Lopende overeenkomsten. Het Addendum vergt instemming van de Wederpartij; de meerkostenregeling van artikel 14.1 is daarvoor de contractuele smeerolie. Als wijziging van de Overeenkomst een aanbestedingsrechtelijke grondslag vereist, leg die dan vast in het inkoopdossier.

Nieuwe overeenkomsten. Voeg het Addendum als bijlage bij de uitvraag en verklaar het in de overeenkomst van toepassing; artikel 14.2 legt het kostenrisico dan bij de inschrijver. In een volgende versie van de ARBIT zijn de bepalingen verwerkt en is geen Addendum meer nodig is.

Cyber Resilience Act. Artikel 11 regelt de doorgeleiding én — voor door Wederpartij beheerde systemen — de toepassing van fabrikantmeldingen en beveiligingsupdates onder de Cyber Resilience Act (artikel 11.3 jo. Bijlage art. 5). De meldplicht van de fabrikant (art. 14 CRA) geldt per 11 september 2026, ook voor producten die dan al in de handel zijn (art. 69 CRA); de fabrikant meldt echter aan het CSIRT en ENISA, niet aan de afnemer. Omdat de CRA een productbegrip hanteert dat losstaat van het begrip netwerk- en informatiesysteem, valt artikel 11 buiten de reikwijdtebeperking van artikel 2.1 en geldt het voor alle producten met digitale elementen — ook buiten NIS-bereik.