STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 29185
1 november 2023

Convenant Project Melissa

Partijen

Partijen die aan samenwerkingsverband Project Melissa deelnemen zijn:
1. De Politie,
2. Het Openbaar Ministerie (OM),
3. Het Nationaal Cyber Security Center (NCSC),

Partijen 1 t/m 3 hierna gezamenlijk: "Publieke Partijen"
4. Branchevereniging Cyberveilig Nederland (CVNL),

en
5. De private cybersecurity bedrijven zoals opgenomen in Bijlage 1,

Partijen 4 en 5 hierna gezamenlijk: "Private Partijen"

hierna afzonderlijk te noemen 'partij' en gezamenlijk, te noemen 'partijen',

Inleiding

Ransomware en gerelateerde vormen van cyberaanvallen met als oogmerk het slachtoffer van de aanval af te persen, is de voornaamste cybercriminele dreiging en is uitgegroeid tot een risico voor de nationale veiligheid indien het vitale processen raakt. Zware, georganiseerde cybercriminele groeperingen zijn in staat gebleken om op uiterst effectieve en schaalbare wijze wereldwijd vele slachtoffers te maken, bedrijfsprocessen volledig stil te leggen en data te stelen om vervolgens grote losgeldbedragen te eisen.

Er is op het moment van aangaan van dit convenant nog te weinig zicht op de omvang van de dreiging van ransomware en gerelateerde vormen van cyber criminaliteit voor Nederland, onder andere door gebrek aan informatie(deling) tussen en gezamenlijke analyse door de partijen die een rol vervullen in het domein van bestrijden van dit type cybercriminaliteit. Partijen hebben 'stukjes van de puzzel', maar deze worden onvoldoende bij elkaar gelegd. Dit staat effectieve bestrijding in de weg.

Project Melissa beoogt om ransomware en gerelateerde vormen van cyberaanvallen effectiever en efficiënter te bestrijden door betere informatiedeling over dreigingen en incidenten, en beter samen te werken in het geval van incidenten. Door relevante informatie te delen, krijgen de samenwerkende partijen een vollediger overzicht van de aanvalsketen en daaraan gerelateerde operationele en tactische informatie waardoor partijen optimaal hun publieke taak kunnen uitvoeren, maatschappelijk belang dienen en schade voorkomen en beperken.

Overwegingen

de volgende overwegingen in aanmerking nemende:
- Dit convenant regelt de uitvoering van de afspraken tussen de samenwerkende partijen in het Project Melissa. Deze afspraken worden – voor zover er sprake zal zijn van de uitwisseling en dus verwerking van persoonsgegevens – juridisch geduid onder artikel 26 AVG en artikel 20 Wpg.
- De samenwerkende Partijen zijn aan te merken als samenwerkingsverband zonder rechtspersoonlijkheid, waarbij Cyberveilig Nederland en Nationaal Cyber Security Center zorgdragen voor de inrichting, onderhoud en ontwikkeling van (gemeenschappelijke) ICT-voorzieningen ten behoeve de samenwerking in Project Melissa.
- De samenwerkende partijen hebben, gelet op hun bedrijfsvoering en/of publieke taak, een rol in het domein van bestrijden van (de gevolgen van) cybercriminaliteit, onder meer in relatie tot cyber aanvallen met afpersing, hoofdzakelijk bestaande uit – maar niet beperkt tot – ransomware aanvallen, en daaraan gerelateerde aspecten binnen de aanvalsketen (hierna te noemen: "aanvalsketen").
- De samenwerkende partijen beschikken vanuit hun rol of taak over relevante operationele en

tactische informatie ten aanzien van de aanvalsketen, gebaseerd op de Unified Kill Chain[1].
– Het Project Melissa is een samenwerkingsverband tussen de publieke sector (Politie, Openbaar Ministerie en Nationaal Cyber Security Center) en partijen uit de private sector (Cyberveilig Nederland en de Private Partijen), met het doel Nederland een onaantrekkelijk doelwit te maken voor de ransomware aanvalsketen.
– Het Project Melissa verbetert de (publiek-private) samenwerking tussen de partijen, onder meer op het gebied van onderlinge communicatie en het onderling uitwisselen van relevante informatie.
– Door relevante informatie te delen, krijgen de samenwerkende partijen een vollediger overzicht van de aanvalsketen en daaraan gerelateerde operationele en tactische informatie waardoor partijen optimaal hun publieke taak kunnen uitvoeren, maatschappelijk belang dienen en schade voorkomen en beperken.
– De relevante informatie, bestaande uit operationele en tactische informatie, bevatten in sommige gevallen ook persoonsgegevens. De, in het kader van dit samenwerkingsverband, door partijen ontvangen persoonsgegevens worden verwerkt in de eigen gegevensbestanden van de partijen, conform de op de partijen van toepassing zijnde wet- en regelgeving.
– Partijen in het samenwerkingsverband zijn ieder voor zich alleen verwerkingsverantwoordelijk voor de verwerking in de eigen gegevensbestanden en de individuele verstrekking vanuit de eigen gegevensbestanden aan elkaar, aan betrokkene(n) en derden. Partijen zijn gezamenlijk verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens binnen de MISP, MatterMost en Signal indien en voor zover die verwerking geschiedt ter uitvoering van Project Melissa overeenkomstig dit convenant.

Gelet op:

– De politietaak zoals genoemd in artikel 3 Politiewet, meer in het bijzonder de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.
– De taak van het Openbaar Miniserie zoals neergelegd in artikel 124 Wet op de Rechterlijke organisatie (Wet RO);
– De taak van het Nationaal Cyber Security Center zoals neergelegd in artikel 3 Wet beveiliging netwerk- en informatiesystemen (Wbni);
– De doelstellingen van de Private Partijen, op basis van de geldende grondslag ingevolge artikel 6 lid 1 AVG en artikel 89 AVG.

Komen navolgende overeen:

1. Definities

In dit convenant en de daarbij behorende bijlagen wordt verstaan onder:
1.1 Betrokkene: een geïdentificeerde of identificeerbare natuurlijke persoon, zoals bedoeld in art. 4 lid 1 AVG of art. 1 onder g Wpg, of art.1 onder g Wjsg;
1.2 Getroffen Partij: De organisatie die het slachtoffer is geworden van een activiteit binnen de Ransomware Aanvalsketen, over welke activiteit informatie, waaronder Persoonsgegevens, worden verwerkt in het kader van het samenwerkingsverband;
1.3 MatterMost: online open-source communicatie platform, beheerd door NCSC;
1.4 MISP: open-source threat intelligence en sharing platform, beheerd door CVNL;
1.5 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de betrokkene’) zoals bedoeld in artikel 4 eerste lid AVG;
1.6 Politiegegevens: elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet 2012, met uitzondering van:
  ○ de uitvoering van wettelijke voorschriften anders dan de Wet administratiefrechtelijke handhaving verkeersvoorschriften;
  ○ de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 1, eerste lid, onderdeel i, onder 1 en artikel 4, eerste lid, onderdeel f, van de Politiewet 2012; zoals bedoeld in artikel 1, onder a Wpg;
1.7 Ransomware aanvalsketen: de handelingen en tactieken die bij een ransomware aanval kunnen worden ingezet door een Threat Actor, zoals geïdentificeerd in de Unified Kill Chain;
1.8 Signal: mobiel communicatie kanaal, beheerd door CVNL;
1.9 Strafvorderlijke gegevens: persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het Openbaar Ministerie in een strafdossier of langs geautomatiseerde weg in een gegevensbestand verwerkt, zoals bedoeld in artikel 1, onder b Wjsg;

[1] Een van origine militair concept waarmee de structuur van een aanval wordt geïdentificeerd (‘kill chain’). Dit concept is aangepast aan de specifieke kenmerken van cyber gerelateerde aanvallen, neergelegd in de ‘unified kill chain’ (hierna te noemen: “Unified Kill Chain”).

1.10 Strafrechtelijke gegevens: persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen, zoals bedoeld in art. 10 AVG en artikel 1 UAVG;
1.11 Threat Actor: een persoon, groep of organisatie die verantwoordelijk is voor, of betrokken is bij, een ransomware aanval en/of handeling(en) binnen de ransomware aanvalsketen;
1.12 Verwerkingsverantwoordelijke: de verwerkingsverantwoordelijke zoals bedoeld in art. 4 zevende lid AVG, of art.1 onder f Wpg; of art. 1 onder k Wjsg;
1.13 Gezamenlijke verwerkingsverantwoordelijke: de verwerkingsverantwoordelijken, zoals bedoeld in art. 26 AVG;
1.14 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens zoals bedoeld in art. 4 tweede lid AVG.

2. Doeleinden

De doeleinden van het samenwerkingsverband zijn:
2.1 Nederland een onaantrekkelijk doelwit te maken voor de ransomware aanvalsketen, door verbetering van de efficiëntie en effectiviteit van:
- de 'pakkans' en mogelijkheden voor verstoring van criminele activiteiten
- het bieden van handelingsperspectief voor de samenleving
- de ondersteuning van (potentiële) slachtoffers van activiteiten binnen de ransomware aanvalsketen

2.2 Door relevante informatie te delen:
- verkrijgen Partijen een beter inzicht in de ransomware aanvalsketen aan de hand van de Unified Kill Chain, waardoor Partijen optimaal hun (publieke) taak kunnen uitvoeren, maatschappelijk belang dienen en schade voorkomen en beperken;
- kan door middel van (statistisch) onderzoek beter inzicht worden verkregen in de ransomware aanvalsketen, waarmee een betere bijdrage kan worden geleverd aan de uitvoering van de (publieke) taak, het dienen van maatschappelijk belang, schade voorkomen en beperken, alsmede het bieden van handelingsperspectief voor de samenleving;
- wordt op gestructureerde en met waarborgen omklede wijze relevante informatie uitgewisseld, wat bijdraagt aan de bescherming van persoonsgegevens en het tegengaan van oneigenlijke toegang daartoe.

2.3 Het verbeteren van de (publiek-private) samenwerking door gestructureerde kennisdeling, onder meer door gestandaardiseerde overleggen en aangewezen communicatiekanalen, waaronder:
- Gegevensdeling via MISP;
- Technische sessies onder TLP:Red[2] met daartoe aangewezen personen;
- Gezamenlijke kennisdelingssessies met alle samenwerkende Partijen;
- Communicatie via Signal en MatterMost;
- Publiceren van *white papers* en andersoortige kennisdocumentatie.

3. Grondslagen gegevensverwerking

3.1 De politie verwerkt politiegegevens voor zover die verwerking noodzakelijk is voor de vervulling van de politietaak, zoals neergelegd in artikel 3 Politiewet. De grondslag voor de structurele verstrekking van artikel 8, artikel 9 en artikel 13, Wet Politiegegevens, aan alle partijen in het samenwerkingsverband is gelegen in artikel 20 Wpg. Dit is nader vastgelegd in de Artikel 20 Beslissing Project Melissa.
3.2 Ten behoeve van de uitvoering van wetenschappelijke analyses dienen de daartoe wettelijke procedures te doorlopen worden zoals neergelegd in artikel 22 Wpg en artikel 15 Wjsg.
3.3 Het Openbaar Ministerie verwerkt strafvorderlijke gegevens, voor zover die verwerking noodzakelijk is voor de vervulling van artikel 124 Wet op de Rechterlijke organisatie (Wet RO). De wettelijke grondslagen voor gegevensverwerking zijn voor het Openbaar Ministerie gelegen in de Wet justitiële en strafvorderlijke gegevens (Wjsg). De grondslag voor de verstrekking van strafvorderlijke gegevens door het Openbaar Ministerie aan alle partijen in het Samenwerkingsverband is gelegen in artikel 39 f Wjsg, respectievelijk artikel 39f lid 1 sub a en e Wjsg.
3.4 Ten behoeve van de uitvoering van wetenschappelijke analyses dienen de daartoe wettelijke procedures te doorlopen worden zoals neergelegd in artikel 22 Wpg en artikel 15 Wjsg.
3.5 Het Nationaal Cyber Security Center (NCSC) verwerkt persoonsgegevens, voor zover die verwerking noodzakelijk is voor de vervulling van de taak zoals neergelegd in 3 Wet beveiliging netwerk- en informatiesystemen (Wbni). De wettelijke grondslag voor de verwerking van persoonsgegevens is voor het NCSC gelegen in artikel 17 lid 1 Wbni en voor de verstrekking van vertrouwelijke gegevens in artikel 20 Wbni.

[2] Traffic Light Protocol. Dit protocol voorziet in gestandaardiseerde aanduiding voor het toegestane gebruik van verstrekte gevoelige informatie. 'Red' houdt in dat de informatie niet mag worden gedeeld en bepekt is tot de deelnemers.

3.6 De Private Partijen verstrekken persoonsgegevens voor zo ver dit noodzakelijk is op grond van artikel 6 lid 1 onder f AVG en artikel 89 AVG.

4. Categorieën betrokkenen en categorieën persoonsgegevens

4.1 In het kader van de samenwerking kunnen door partijen over de volgende categorieën betrokkenen de volgende categorieën persoonsgegevens worden verstrekt:
Categorie betrokkenen 1: Eigen werknemers van de verwerkingsverantwoordelijken
Categorie betrokkenen 2: Natuurlijke personen gelieerd aan de Getroffen Partij
Categorie betrokkenen 3: Natuurlijke personen gelieerd aan een derde partij die bij een incident betrokken zijn (zoals IT provider of klant van Getroffen Partij)
Categorie betrokkenen 4: Natuurlijke personen (zoals verdachten of andere personen) gelieerd aan de Threat Actor.

4.2 **Categorie betrokkene 1**:
a. Naam en initialen;
b. Zakelijk telefoonnummer en e-mailgegevens;
c. Organisatie en functie (optioneel);
d. Foto (optioneel);
e. Inhoud communicatie via Signal en MatterMost;

4.3 **Categorie betrokkene 2**:
a. IP-adres
b. Accountnaam
c. E-mail adres

4.4 **Categorie betrokkene 3**:
a. IP-adres
b. Accountnaam
c. E-mailadres

4.5 **Categorie betrokkene 4**:
a. IP-adres
b. Cryptocoin adres
c. Contactinformatie, inclusief social media informatie
d. Omschrijving van gedraging
e. Onderhandelingsinformatie
f. Andere (strafrechtelijke) persoonsgegevens

In aanvulling daarop kunnen door de politie de volgende Politiegegevens worden verstrekt:
- artikel 8 Politiegegevens;
- artikel 9 Politiegegevens;
- artikel 13 Politiegegevens;

In aanvulling daarop kunnen door het Openbaar Ministerie Strafvorderlijke gegevens worden verstrekt.

5. Inspanningen, inrichting samenwerking en verwerkingsverantwoordelijkheid

5.1 Om de doeleinden te bereiken, verplichten partijen zich tot bepaalde handelingen, bijdragen en/of inspanningen. Deze worden per Partij nader vermeld in de bij dit convenant behorende bijlagen.

5.2 Er zijn gezamenlijke werkprocessen opgesteld waarin wordt beschreven hoe de informatie-uitwisseling tussen Partijen plaatsvindt en welke verwerkingsactiviteiten plaatsvinden waarbij ook de verwerkingsverantwoordelijkheden worden beschreven. Deze worden vermeld in de bij dit convenant behorende bijlagen.

5.3 Er is sprake van een aantal structurele gezamenlijke overleggen tussen Partijen. De doeleinden, frequentie en samenstelling van deze overleggen worden nader uitgewerkt in de bij dit convenant horende bijlagen.

5.4 Artikel 5.1 van dit convenant is niet afdwingbaar, Partijen kunnen op tekortkomingen in de nakoming van artikel 5.1 van dit convenant of van afspraken die daarmee samenhangen, bij de burgerlijke rechter geen beroep doen.

6. Wijze van verstrekking

6.1 Persoonsgegevens worden alleen verstrekt door en aan die medewerkers van partijen die door die partijen zijn aangewezen en geautoriseerd voor het verwerken van deze gegevens voor zover dit noodzakelijk is voor hun taak bij het behalen van de doelstellingen van het convenant.

6.2 Politiegegevens kunnen mondeling en/of schriftelijk door de politie worden verstrekt middels MISP en overleggen zoals nader vermeld in de bij dit convenant behorende bijlagen.

6.3 Strafvorderlijke en/of justitiële gegevens kunnen mondeling en/of schriftelijke door het Open-

baar Ministerie worden verstrekt door middel van MISP en overleggen zoals nader vermeld in de bij dit convenant behorende bijlagen.

6.4 Persoonsgegevens kunnen mondeling en/ of schriftelijke door de Private Partijen worden verstrekt door middel van MISP, Signal, MatterMost en overleggen zoals nader vermeld in de bij dit convenant behorende bijlagen.

6.5 Iedere partij die na verstrekking constateert dat de verstrekte persoonsgegevens onjuist of onvolledig zijn, stelt de andere partijen op de hoogte van correcties van en/ of aanvullingen op de persoonsgegevens, op de wijze zoals opgenomen in de bij dit convenant behorende bijlagen.

7. Geheimhoudingsplicht

7.1 De partijen dragen er zorg voor dat diegenen die persoonsgegevens verwerken, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, verklaren tot geheimhouding over persoonsgegevens en over andere gegevens waarvan zij het vertrouwelijke karakter kennen of redelijkerwijs moeten vermoeden, behoudens voor zover enig wettelijk voorschrift hen tot bekendmaking verplicht of uit hun taak daartoe voortvloeit. Daar waar het gaat om activiteiten vallend onder de wetenschappelijk verwerkingsgrondslag worden de condities van de goedkeuringsbeslissing gevolgd.

7.2 Doorverstrekking van persoonsgegevens aan derden vindt alleen plaats onder de voorwaarden zoals neergelegd in de bij dit convenant behorende bijlagen.

7.3 Partijen komen overeen dat het is toegestaan om de in het samenwerkingsverband ontvangen gegevens intern verder te verwerken voor andere doeleinden dan de doeleinden in het samenwerkingsverband. Partijen houden daarbij rekening met de vereisten van artikel 6 vierde lid AVG danwel met de voor hen van toepassing zijnde wetgeving.

8. Bewaartermijnen en vernietiging

8.1 De persoonsgegevens die worden verwerkt in het samenwerkingsverband worden bewaard voor de periode zoals neergelegd in de bij dit convenant behorende bijlagen.

8.2 Van belang is om op te merken dat deze termijnen de persoonsgegevens betreffen die worden verwerkt onder de gezamenlijke verwerkingsverantwoordelijkheid. Informatie die relevant wordt bevonden door de partijen en welke verder worden verwerkt voor eigen doeleinden vallen onder de individuele verwerkingsverantwoordelijkheid.

8.3 Na verloop van de bewaartermijn worden de persoonsgegevens vernietigd overeenkomstig het proces zoals opgenomen in de bij dit convenant behorende bijlagen.

9. Beveiliging

9.1 Partijen beveiligen de persoonsgegevens van de betrokkenen tegen verlies of enige vorm van onrechtmatige verwerking en treffen daartoe de nodige passende technische en organisatorische maatregelen zoals neergelegd in dit de bij dit convenant behorende bijlagen.

9.2 Partijen hebben procedures om de betrouwbaarheid, zowel bij aanname als gedurende het dienstverband, van medewerkers die betrokken zijn bij Project Melissa vast te stellen op de wijze zoals neergelegd in dit de bij dit convenant behorende bijlagen.

9.3 Partijen zijn zich bewust dat alle afspraken ten spijt veiligheidsincidenten kunnen optreden. Indien een Partij kennis krijgt van een incident aangaande een (mogelijk) inbreuk op de beveiliging van gegevens wordt de procedure gevolgd zoals neergelegd in dit de bij dit convenant behorende bijlagen.

10. Informatieplicht

10.1 Ten einde ervoor te zorgen dat personen en organisaties bekend worden met de gegevensuitwisseling in het kader van dit samenwerkingsverband wordt dit convenant door de deelnemende partijen gepubliceerd op hun website en/of op andere wijze openbaar gemaakt.

11. Rechten van betrokkene

11.1 De rechten van betrokkenen worden door de partijen afgehandeld overeenkomstig het protocol verzoeken betrokkenen zoals neergelegd in de bij dit convenant behorende bijlagen.

11.2 Partijen die vallen onder het regime van de AVG hebben het recht om een verzoek geheel of gedeeltelijk af te wijzen op grond van de criteria zoals genoemd in artikel 41 UAVG.

11.3 De politie heeft het recht om een verzoek geheel of gedeeltelijk af te wijzen op grond van de criteria zoals genoemd in artikel 27 Wpg. Deze weigeringsgrond kan worden ingeroepen indien gegevens vanuit MISP verder worden verwerkt voor de eigen taak.

11.4 Het Openbaar Ministerie heeft het recht om een verzoek geheel of gedeeltelijk af te wijzen op grond van de criteria zoals genoemd in artikel 39i Wjsg. Deze weigeringsgrond kan worden

ingeroepen indien gegevens vanuit MISP verder worden verwerkt voor de eigen taak.

11.5 De partij(en) stemmen eerst onderling af, in overeenstemming met het protocol zoals neergelegd in de bij dit convenant behorende bijlagen, alvorens betrokkene wordt beantwoord conform de op de partijen van toepassing zijnde wet- en regelgeving en de daarin geldende termijnen.

12. Schade en kosten

12.1 Een ieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op de voor de partijen van toepassing zijnde wet- en regelgeving, heeft het recht van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade.

12.2 Partijen zijn in geval van toerekenbare tekortkoming ieder voor zich aansprakelijk voor schade als gevolg van hun eigen interne gegevensverwerking danwel hun verstrekking aan partijen in het samenwerkingsverband of derden.

12.3 De partijen berekenen onderling kosten voor werkzaamheden en middelen voortvloeiende uit dit convenant, overeenkomstig het bepaalde in de bij dit convenant behorende bijlagen.

13. Evaluatie en wijzigingen

13.1 Partijen verplichten zich tenminste jaarlijks de samenwerking te evalueren. Indien partijen dit willen laten plaatsvinden middels een onafhankelijke audit dan maken zij hierover afspraken in de bij dit convenant opgesteld bijlagen.

13.2 Indien de evaluatie uitwijst dat het convenant aanpassing behoeft, zal dientengevolge het convenant worden gewijzigd.

13.3 Wijzigingen en aanvullingen van dit convenant vereisen de goedkeuring, ondertekening en dagtekening van alle partijen, op de wijze zoals uitgewerkt in de bij dit convenant opgestelde bijlagen.

14. Toetreding en uittreding

14.1 Partijen worden vooraf op de hoogte gebracht van de voorgenomen toetreding van een nieuwe partij tot het samenwerkingsverband overeenkomstig de procedure in de bij dit convenant opgestelde bijlagen.

14.2 Toetreding vindt plaats door middel een ondertekening van dit convenant door de toetredende partij en opname van die partij in de bijlage bij dit convenant.

14.3 Uitreding vindt plaats door middel van verwijdering van die partij van de bijlage bij dit convenant, na het volgen van de procedure voor uittreding zoals opgenomen in de bij dit convenant opgestelde bijlagen.

15. In werking treding en looptijd

15.1 Dit convenant treedt in werking na publicatie in de Staatscourant en heeft een looptijd van drie (3) jaar. De looptijd wordt steeds verlengd met een periode van één (1) jaar, tenzij partijen schriftelijk besluiten het convenant niet te verlengen.

16. Ondertekening

Aldus overeengekomen en ondertekend te Den Haag op 3 oktober 2023

Den Haag, 3 oktober 2023

De korpschef van politie
namens deze,
R. van Bree
Plv. politiechef Landelijke Eenheid

Het Openbaar Ministerie, het College van procureurs-generaal, te dezen vertegenwoordigd door de hoofdofficier van justitie,
J. de Smet - Dierckx
Plv. Hoofdofficier van Justitie

Het Nationaal Cyber Security Center, hierbij rechtsgeldig vertegenwoordigd door:
H. de Vries
Directeur NCSC

Cyberveilig Nederland, hierbij rechtsgeldig vertegenwoordigd door:
P. Oldengarm
Directeur

Private Partijen, overeenkomstig het proces voor toetreding zoals opgenomen in de bijlage bij dit convenant.