STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 35943
23 oktober 2025

Convenant samenwerking Cyclotron

Partijen:
1. De Minister van Binnenlandse Zaken en Koninkrijksrelaties, te dezen vertegenwoordigd door de directeur-generaal van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD),
2. De Minister van Defensie, te dezen vertegenwoordigd door de directeur van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD),
3. De Minister van Justitie en Veiligheid, te dezen vertegenwoordigd door de directeur van het Nationaal Cyber Security Centrum (NCSC),
4. De Minister van Justitie en Veiligheid, te dezen vertegenwoordigd door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV),
5. De politie, te dezen vertegenwoordigd door de korpschef en in ondermandaat het hoofd Operatiën van de eenheid Landelijke Opsporing en Interventies,
6. Andere publieke partijen, als zodanig opgenomen in bijlage 1,

Partijen 1 t/m 7 hierna gezamenlijk 'Publieke Partijen',

7. De private partijen, als zodanig opgenomen in bijlage 1, hierna 'Private Partijen'.

Overwegende dat:
- één van de ambities van de Nederlandse Cybersecurity Strategie 2022-2028 (NLCS) is dat publieke en private organisaties intensiever informatie met elkaar delen over cyberdreigingen en -incidenten, zodat hierop sneller gereageerd kan worden en zo mogelijk incidenten voorkomen worden;
- bovengenoemde publieke partijen in het kader van de uitvoering van de NLCS, ten aanzien waarvan de NCTV coördinerend verantwoordelijk is, hebben besloten dat er structureel zal worden samengewerkt en hiertoe functionaliteiten zullen worden ingericht, onder de naam Cyclotron, teneinde aan de samenwerking deelnemende publieke en private partijen snel gegevens met elkaar te laten uitwisselen, gezamenlijke analyses te laten maken en op basis van deze gezamenlijke analyses informatie en adviezen over cyberdreigingen en -incidenten te delen met andere belanghebbende organisaties;
- door het structureel uitwisselen van informatie of kennis en het maken van gezamenlijke analyses wordt het situationeel beeld versterkt, kunnen de deelnemende partijen hun werkzaamheden beter uitoefenen, kunnen andere belanghebbende private en publieke partijen sneller en vollediger over voor hen relevante cyberdreigingen en -incidenten worden geïnformeerd, en wordt daarmee de digitale weerbaarheid van organisaties in Nederland verhoogd;
- voor aan de samenwerking deelnemende partijen geldt dat zij gelet op hun publieke taak of private dienstverlening een rol in het cybersecuritydomein hebben, omdat zij over relevante cyberdreigings- en incidentinformatie beschikken en/of expertise op het gebied van cybersecurity hebben, zij daarnaast bereid zijn om zo veel mogelijk informatie te delen of deel te nemen aan gezamenlijke analyses van dergelijke informatie, en zij gevestigd zijn in Nederland of hun taken verrichten dan wel diensten verlenen op Nederlands grondgebied;
- deelname door partijen aan de samenwerking de uitoefening van de eigen taken, bevoegdheden en verantwoordelijkheden van die partijen onverlet laat;
- partijen in het kader van deze samenwerking, met uitzondering van de NCTV, onderling gegevens verstrekken, waaronder persoonsgegevens, en gezamenlijke analyses verrichten met betrekking tot die gegevens, met inachtneming van de voor de afzonderlijke partijen geldende wettelijke en andere juridische kaders, met dien verstande dat medewerkers van AIVD en MIVD gelet op die kaders vooralsnog niet deelnemen aan de gezamenlijke analyses;
- partijen in relatie tot gezamenlijke verwerking van persoonsgegevens in het kader van het verrichten van gezamenlijke analyses, mede gelet op artikel 26 AVG, onderlinge regels over de doeleinden en middelen van die werking en hun respectieve verantwoordelijkheden voor de nakoming van daaraan verbonden wettelijke verplichtingen in dit convenant willen vastleggen;
- partijen met dit convenant daarnaast ook andere afspraken over de samenwerking in bovengenoemde zin wensen vast te leggen.

Gelet op:
- De artikelen 8, 10, 39, 62, 66 en 68 van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017);

– De artikelen 3, 17 en 20 van de Wet beveiliging netwerk- en informatiesystemen (Wbni)[1];
– Artikel 3 van de Politiewet 2012 (Pw 2012);
– Artikel 20 van de Wet politiegegevens (Wpg)[2];
– Artikel 6, eerste lid, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 en 26 van de Algemene verordening gegevensbescherming (AVG).

Komen het volgende overeen:

1. Definities

1.1 persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, waaronder persoonsgegevens als bedoeld in artikel 4 AVG, politiegegevens, en persoonsgegevens als bedoeld in artikel 1 onder e Wiv 2017;
1.2 politiegegeven: 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; als bedoeld in artikel 1, onder a Wpg;

1.3 betrokkene: een geïdentificeerde of identificeerbare natuurlijke persoon waarop een persoonsgegeven betrekking heeft;
1.4 contactpunt: het contactpunt, bedoeld in artikel 7.1;
1.5 verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens;
1.6 verwerkingsverantwoordelijke: de verwerkingsverantwoordelijke, bedoeld in artikel 4 zevende lid, AVG, artikel 1, onder f, Wpg of artikel 17 Wiv 2017;
1.7 gezamenlijke verwerkingsverantwoordelijken: twee of meer verwerkingsverantwoordelijken die gezamenlijk de doeleinden en middelen van de verwerking bepalen;
1.8 cyberdreigingen: 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;
1.9 cyberincidenten: 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.[3]

Samenwerking algemeen

2. Doel

Dit convenant heeft tot doel om afspraken vast te leggen over de samenwerking tussen partijen, ten behoeve van het gezamenlijk versterken van het situationeel beeld met betrekking tot cyberdreigingen en -incidenten, het beter kunnen uitoefenen van werkzaamheden door deelnemende partijen, en het beter kunnen informeren van andere belanghebbende organisaties, door het op structurele wijze snel onderling delen van informatie of kennis over cyberdreigingen en -incidenten, het gezamenlijk analyseren van dergelijke informatie en het verstrekken van informatie en adviezen op basis van die analyses aan andere belanghebbende organisaties.

3. Samenwerkingsactiviteiten

3.1 Partijen verstrekken, uitgezonderd de NCTV, ten behoeve van het doel, bedoeld in artikel 2, met inachtneming van de voor hun geldende wettelijke en andere juridische kaders, bij hen berustende informatie of kennis aangaande cyberdreigingen en -incidenten zo veel als mogelijk aan elkaar.
3.2 Partijen nemen, met uitzondering van de NCTV, de AIVD en de MIVD, ten behoeve van het doel, bedoeld in artikel 2, met inachtneming van de voor hun geldende wettelijke en andere juridische kaders, zo veel als mogelijk deel aan het gezamenlijk analyseren van informatie over cyberdreigingen en -incidenten in verschillende samenstellingen. Daarnaast stellen partijen, indien zij deelnemen aan de gezamenlijke analyses, op basis hiervan zo veel als mogelijk gezamenlijke

---

[1] De Wbni zal naar verwachting volgend jaar worden vervangen door de Cyberbeveiligingswet (Cbw), die tot strekking heeft de Europese NIS2-richtlijn (Richtlijn EU 2022/2555) in nationale wetgeving te implementeren. Sommige bepalingen uit die richtlijn hebben vanaf 17 oktober 2024 tot de datum van inwerkingtreding van de Cbw rechtstreekse werking. Dat betekent dat particuliere partijen vanaf die datum op grond daarvan bepaalde rechten hebben, zoals het van het NCSC als CSIRT ontvangen van voor hen relevante informatie over cyberdreigingen en -incidenten.
[2] Dit wordt nader vastgelegd in de artikel 20 Wpg beslissing samenwerking Cyclotron.
[3] Vgl. artikel 6 NIS2-richtlijn.

adviezen op en bepalen zij gezamenlijk voor welke derde partijen de uit die analyse voortvloeiende informatie of adviezen relevant zijn.

3.3 Partijen spreken voorts af dat het NCSC ten behoeve van het doel, bedoeld in artikel 2, belast is met het, met inachtneming van de voor het NCSC geldende wettelijke kaders, zo veel als mogelijk verstrekken van informatie en adviezen uit hoofde van de gezamenlijke analyses, bedoeld in het tweede lid, aan andere belanghebbende organisaties.

3.4 Het derde lid laat onverlet dat andere partijen dan het NCSC, indien en voor zover zij hebben deelgenomen aan gezamenlijke analyses als bedoeld in het tweede lid, de informatie en adviezen uit hoofde daarvan kunnen gebruiken ten behoeve van de uitvoering van hun eigen taken of werkzaamheden.

4. Beheer functionaliteiten

Partijen spreken af dat het NCSC ten behoeve van de activiteiten, bedoeld in artikel 3, eerste tot en met derde lid, de volgende drie functionaliteiten inricht en in stand houdt, en daartoe de wettelijke vereisten voor het nemen van passende technische en organisatorische maatregelen in acht neemt:

– technische faciliteiten waarmee partijen veilig en snel informatie kunnen uitwisselen, genaamd doordeelfunctie;
– technische faciliteiten waarmee partijen informatie ten behoeve van gezamenlijke analyses kunnen uitwisselen, gezamenlijke analyses kunnen uitvoeren, gezamenlijk adviezen op basis van die analyses kunnen opstellen, en gezamenlijk kunnen bepalen voor welke derde partijen informatie en adviezen uit hoofde van die analyses relevant is, genaamd analyse- en weerbaarheidsfunctie; en
– technische faciliteiten om informatie en adviezen uit hoofde van de gezamenlijke analyses te delen met andere belanghebbende organisaties, genaamd communicatie- en distributiefunctie.

Gezamenlijke verwerking van persoonsgegevens in het kader van de activiteiten, genoemd in artikel 3, tweede lid

5. Gezamenlijke verwerkingsverantwoordelijkheid

5.1 Partijen geven invulling aan hun gezamenlijke verwerkingsverantwoordelijkheid van persoonsgegevens, in het kader van de activiteiten, bedoeld in artikel 3, tweede lid, overeenkomstig artikel 26 AVG, met het bepaalde in de artikelen 5, tweede lid, en 6 tot en met 13.

5.2 Partijen omschrijven in bijlage 2 de soorten persoonsgegevens, de categorieën van persoonsgegevens, de betrokkenen en de ontvangers.

6. Informeren van betrokkenen

Partijen informeren betrokkenen over de gegevensverwerking, overeenkomstig de artikelen 13 en 14 AVG, middels een gezamenlijke privacyverklaring zoals beschreven in bijlage 3.

7. Rechten van betrokkenen

7.1 Partijen richten voor betrokkenen een contactpunt in. Het contactpunt is een centraal punt waar betrokkenen verzoeken kunnen indienen, overeenkomstig de artikelen 15 tot en met 20 AVG. Ook kunnen betrokkenen via het contactpunt bezwaar maken overeenkomstig artikel 21 en 22 AVG.

7.2 Het contactpunt wordt beheerd door het NCSC en zichtbaar geplaatst op de website van het NCSC.

7.3 De verzoeken en bezwaren van betrokkenen worden behandeld overeenkomstig de procedure zoals is opgenomen in bijlage 4.

8. Inbreuk in verband met Persoonsgegevens

8.1 In het geval van een inbreuk in verband met persoonsgegevens informeert de partij die de inbreuk ontdekt de andere partijen onverwijld hierover. Beoordeling van de inbreuk geschiedt door de betrokken partijen gezamenlijk, gecoördineerd door het in artikel 7 bedoelde contactpunt, overeenkomstig de afspraken zoals vastgelegd in bijlage 6.

8.2 Indien een inbreuk in verband met persoonsgegevens zich voordoet kunnen partijen, na de beoordeling, bedoeld in het eerste lid, besluiten dit gezamenlijk te melden bij de Autoriteit Persoonsgegevens of gezamenlijk mededeling hiervan te doen aan betrokkenen, onder coördinatie van het in artikel 7 bedoelde contactpunt. Een dergelijk besluit doet niets af aan de eigen verantwoordelijkheid die partijen op grond van de voor hen geldende wettelijke kaders omtrent een inbreuk in verband met persoonsgegevens hebben.

9. Bewaartermijnen

De persoonsgegevens, die gezamenlijk worden verwerkt in het kader van de activiteiten, bedoeld in artikel 3, tweede lid, worden niet langer bewaard dan noodzakelijk is voor het doel van de samenwerking, zoals beschreven in artikel 2, en worden in ieder geval uiterlijk 2 jaar na de datum van de eerste verwerking verwijderd.

10. Beveiliging van verwerking

10.1 Partijen treffen de nodige passende technische en organisatorische maatregelen ter bescherming van de persoonsgegevens van betrokkenen in het kader van de activiteiten, bedoeld in artikel 3, tweede lid, onder gebruikmaking van de in artikel 4 daarvoor genoemde functionaliteit. Partijen leggen deze te nemen maatregelen vast in bijlage 5.

10.2 Partijen hebben in het kader van de maatregelen, bedoeld in het eerste lid, procedures om de betrouwbaarheid van medewerkers die betrokken worden bij het verrichten van de in het eerste lid bedoelde activiteiten, zowel bij aanvang van als gedurende hun deelname aan die activiteiten, vast te stellen.

11. Inschakelen van een verwerker

Partijen spreken af dat er geen verwerker wordt ingeschakeld voor de gezamenlijke verwerking van persoonsgegevens.

12. Gegevensbeschermingseffectbeoordeling (DPIA)

Partijen zullen een gezamenlijke DPIA uitvoeren met betrekking tot de gezamenlijke verwerking van persoonsgegevens, geven elkaar daarbij hun volledige medewerking, en nemen naar aanleiding daarvan zo nodig aanvullende maatregelen als bedoeld in artikel 10, eerste lid.

13. Verzoeken van de Autoriteit Persoonsgegevens

13.1 Wanneer de Autoriteit Persoonsgegevens een verzoek doet bij een partij ter zake van de gezamenlijke verwerking van persoonsgegevens, informeert de partij daarover de andere partijen.

13.2 Partijen geven elkaar zo veel als mogelijk de benodigde informatie en medewerking om aan een verzoek van de Autoriteit Persoonsgegevens als bedoeld in het eerste lid te voldoen.

Overige bepalingen in het kader van de samenwerking

14. Geheimhoudingsplicht

Partijen kunnen in voorkomende gevallen afspreken dat specifieke informatie die zij uitwisselen of gezamenlijk analyseren, vanwege het vertrouwelijke karakter van die informatie, niet met derden zal kunnen worden gedeeld.

15. Governance

15.1 Er is een governanceboard, bestaande uit vertegenwoordigers van partijen, die tot taak heeft om:
- a. toe te zien op de uitvoering van de afspraken in dit convenant;
- b. thema's te bepalen die centraal staan bij het verrichten van de gezamenlijke activiteiten, bedoeld in artikel 3, tweede lid;
- c. het vaststellen van afspraken, na afstemming met de andere partijen, over de aard en omvang van de in artikel 3 bedoelde activiteiten en de door de partijen hiervoor beschikbaar te maken personele capaciteit;
- d. het verrichten van de evaluatie van het convenant, bedoeld in artikel 18, in afstemming met de andere partijen;
- e. uitvoering geven aan de in andere artikelen van dit convenant voor de governanceboard voorziene taken, waaronder die in de artikelen 17, 19, 20 en 22.

15.2 Er is een stuurgroep, bestaande uit vertegenwoordigers van publieke partijen, die tot taak heeft om:
- a. een voorstel te maken over de verdeling van de kosten, bedoeld in artikel 16, tweede lid;
- b. een voorstel te maken voor afspraken over de aard en omvang van de in artikel 3 bedoelde activiteiten en de door de partijen hiervoor beschikbaar te maken personele capaciteit.

15.3 Partijen maken nadere afspraken over het bepalen van de partijen namens welke vertegenwoordigers in de governanceboard en de stuurgroep zitting zullen hebben.

15.4 De governanceboard voert periodiek, en ten minste drie maal per jaar, overleg.
15.5 De stuurgroep voert periodiek, en ten minste vier maal per jaar, overleg.
15.6 De governanceboard onderscheidenlijk de stuurgroep kan besluiten tot het instellen van een werkgroep, met daarin vertegenwoordigers van de partijen in de governanceboard onderscheidenlijk stuurgroep, die belast zijn met de voorbereiding van of het adviseren over het uitvoeren van de taken zoals genoemd in het eerste en tweede lid.
15.7 De governanceboard en stuurgroep kunnen nadere regels stellen omtrent de eigen werkwijze.

16. Financiën

16.1 De door deze samenwerking ontstane personele kosten worden gedragen door de partij waartoe dat personeel behoort.
16.2 Publieke partijen maken over de verdeling van de overige door deze samenwerking ontstane kosten afspraken.

17. Communicatie

Partijen spreken af dat communicatie met derden over de in dit convenant bedoelde samenwerking zal plaatsvinden, na afstemming in de governanceboard, onder coördinatie van het NCSC. Indien de communicatie specifiek ziet op de uitvoering van de Nederlandse Cybersecurity Strategie vindt de in de eerste volzin bedoelde afstemming plaats onder coördinatie van de NCTV.

18. Evaluatie

Partijen verplichten zich om jaarlijks de uitvoering en werking van het convenant te evalueren.

19. Wijziging

19.1 Elke partij kan de andere partijen schriftelijk verzoeken dit convenant te wijzigen.
19.2 In geval van een verzoek, bedoeld in het eerste lid, of een andere omstandigheid die aanleiding kan geven dit convenant te wijzigen, zal de governanceboard beoordelen of en in welke zin het aangewezen is om het convenant te wijzigen en, indien aangewezen, een voorstel doen voor wijziging van het convenant.
19.3 Wijzigingen van dit convenant behoeven de schriftelijke instemming van alle partijen.

20. Toetreding

20.1 Organisaties kunnen gedurende de looptijd van het convenant als partij toetreden. Die toetreding is alleen mogelijk indien een organisatie:
  a. vanwege haar taak of dienstverlening over voor andere partijen of andere organisaties relevante cyberdreigings- en incidentinformatie of expertise op het gebied van cybersecurity beschikt; en
  b. is gevestigd in Nederland of haar taken verricht onderscheidenlijk diensten verleent op Nederlands grondgebied.
20.2 Een toetredende partij dient de verplichtingen die uit het convenant voortvloeien, zonder voorbehoud te aanvaarden.
20.3 Een organisatie die wil toetreden maakt het verzoek tot toetreding schriftelijk bekend aan de governanceboard. Zodra de governanceboard schriftelijk heeft ingestemd met het verzoek tot toetreding, na raadpleging van de andere partijen, ontvangt de toetredende partij de status van partij bij het convenant en gelden voor die partij de voor haar uit het convenant voortvloeiende rechten en verplichtingen.
20.4 Het verzoek tot toetreding en de verklaring tot instemming worden in afschrift als bijlage aan het convenant gehecht en de partij wordt toegevoegd aan de opsomming van partijen in bijlage 1.

21. Opzegging

21.1 Elke partij kan dit convenant met inachtneming van een opzegtermijn van twee maanden schriftelijk opzeggen, onder vermelding van de reden hiervoor.
21.2 Wanneer een partij dit convenant opzegt, blijft dit voor de overige partijen in stand, voor zover de inhoud en strekking ervan zich daartegen niet verzet.

22. Escalatieregeling

22.1 Een partij die meent dat een geschil bestaat in verband met dit convenant, waaronder een geschil over het al dan niet nakomen van een of meer verplichtingen in dit convenant door een andere partij of over het door een andere partij al dan niet meer voldoen aan de in artikel 20,

eerste lid, bedoelde toetredingseisen, deelt dat schriftelijk mee aan de andere partijen. De mededeling bevat een aanduiding van het geschil.

22.2 Binnen 20 werkdagen na dagtekening van de in het eerste lid bedoelde mededeling deelt iedere partij zijn zienswijze omtrent het geschil, alsmede een voorstel voor een oplossing daarvan, aan de andere partijen.

22.3 Binnen 15 werkdagen na afloop van de in het tweede lid genoemde termijn overleggen partijen over een oplossing van het geschil, waaronder de vaststelling dat een partij verplichtingen in dit convenant niet heeft nagekomen of de vaststelling dat een partij niet meer voldoet aan de in artikel 20, eerste lid, bedoelde toetredingseisen. Het overleg wordt voorgezeten door een door de governanceboard hiervoor aangewezen voorzitter.

22.4 Elke partij draagt de eigen kosten, voortvloeiend uit de procedure van het eerste tot en met het derde lid.

23. Gang naar de rechter

Alle geschillen in verband met dit convenant worden beslecht door de bevoegde rechter te Den Haag. Een partij kan zich hiervoor pas tot de rechter wenden, indien het geschil niet volgens de escalatieprocedure van artikel 22 is opgelost.

24. Niet-nakoming verplichtingen

Indien ingevolge artikel 22, derde lid, partijen hebben vastgesteld dat een partij zijn verplichtingen uit hoofde van dit convenant niet is nagekomen onderscheidenlijk niet meer voldoet aan de in artikel 20, eerste lid, bedoelde toetredingseisen, dan wel ingevolge artikel 23 de bevoegde rechter heeft vastgesteld dat een partij zijn verplichtingen uit hoofde van dit convenant niet heeft nagekomen onderscheidenlijk niet meer voldoet aan genoemde toetredingseisen, en deze partij verzuimt binnen twee maanden die verplichtingen alsnog na te komen onderscheidenlijk alsnog aan die toetredingseisen te voldoen, zijn de andere partijen ten opzichte van die partij niet meer gehouden tot het nakomen van de verplichting, bedoeld in artikel 3, eerste lid, kan die partij niet meer deelnemen aan de activiteiten, bedoeld in artikel 3, tweede lid, kan die partij geen vertegenwoordiger meer hebben in de governanceboard of de stuurgroep, kan die partij niet meer een verzoek als bedoeld in artikel 19 doen, en kan die partij niet meer een mededeling als bedoeld in artikel 22, eerste lid, doen.

25. Afdwingbaarheid

Dit convenant is in rechte afdwingbaar.

26. Toepasselijk recht

Op dit convenant is het Nederlands recht van toepassing.

27. Inwerkingtreding en duur

27.1 Dit convenant treedt in werking met ingang van de datum van uitgifte van de Staatscourant waarin het wordt gepubliceerd, werkt terug tot en met 15 oktober 2025, en wordt aangegaan voor de periode van één jaar te rekenen vanaf laatstgenoemde datum.

27.2 Na afloop van de in het eerste lid genoemde duur wordt dit convenant telkens voor dezelfde duur voortgezet, tenzij een partij uiterlijk een maand voor het einde van die duur schriftelijk kenbaar heeft gemaakt het convenant niet te willen voortzetten.

27.3 Partijen treden uiterlijk twee maanden voor afloop van de duur van het convenant in overleg over de voortzetting van dit convenant.

28. Publicatie Staatscourant

28.1 Dit convenant wordt uiterlijk binnen een maand na ondertekening door de laatste van de partijen gepubliceerd in de Staatscourant.

28.2 Bij wijziging van dit convenant vindt het eerste lid overeenkomstige toepassing.

28.3 Van toetreding of opzegging van dit convenant wordt melding gemaakt in de Staatscourant.

29. Slotbepaling

Dit convenant wordt aangehaald als: Convenant samenwerking Cyclotron.

Aldus overeengekomen en in achtentwintigvoud opgemaakt,

Den Haag, 14 oktober 2025

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
namens deze,
E.S.M. Akerboom,
de directeur-generaal van de Algemene Inlichtingen- en Veiligheidsdienst

Den Haag, 30 september 2025

De Minister van Defensie,
namens deze,
brigadegeneraal
H.J. Bos,
programmadirecteur Cybersecurity van de Militaire Inlichtingen- en Veiligheidsdienst

Den Haag, 30 september 2025

De Minister van Justitie en Veiligheid,
namens deze,
M.J. van Amelsfort,
de directeur van het Nationaal Cyber Security Centrum

Den Haag, 30 september 2025

De Minister van Justitie en Veiligheid,
namens deze,
E. van Beurden,
de directeur Cybersecurity, Weerbaarheid Statelijke Dreigingen en Analyse Nationale Veiligheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid

Den Haag, 30 september 2025

De korpschef van politie,
namens deze de politiechef van de Eenheid Landelijke Opsporing en Interventies,
namens deze,
S.J.B. Duijf,
Hoofd Operatiën

Den Haag, 14 oktober 2025

Dienst ICT Uitvoering (DICTU),
namens deze,
R.M. Wiersema,
de directeur Operatie / plv. Algemeen directeur DICTU

Den Haag, 30 september 2025

Attic B.V.,
namens deze,
E. Remmelzwaal,
CEO

Utrecht, 10 oktober 2025

Conclusion Enablement B.V.,
namens deze,
J. Jaques,
Algemeen directeur

Den Haag, 30 september 2025

Connect2Trust,
namens deze,
R. Bierens
Voorzitter

E. Slingerland,
Vice-voorzitter

Den Haag, 30 september 2025

Cyberveilig Nederland,
namens deze,
L. Holterman,
Directeur

Zoetermeer, 30 september 2025

DEFION Security Netherlands B.V.,
namens deze,
H. Ruijs,
Founder & CEO

Amsterdam, 9 oktober 2025

Deloitte Consultative Services B.V.,
namens deze,
T. Niemeijer,
Partner

Den Haag, 30 september 2025

DTACT, een merknaam van DutchSec Ventures B.V.,
namens deze,
S. Swinkels,
CEO & Co-founder

Den Haag, 30 september 2025

ESET Nederland,
namens deze,
D. Maasland,
CEO van ESET Nederland

Den Haag, 9 oktober 2025

Eye Security B.V.,
namens deze,
P.L.W. Kerkhofs,
CTO Eye Security

Den Haag, 30 september 2025

Fox-IT B.V.,
namens deze,
P. Strasmann,
Managing Director

Den Haag, 30 september 2025

Hunt & Hackett B.V.,
namens deze,
V.D. Schönfeldt,
General Counsel

Den Haag, 30 september 2025

Invictus Incident Response B.V.,
namens deze,
K. Stam,
CEO

Den Haag, 30 september 2025

Kennedy van der Laan N.V.,
namens deze,
R.C. Brand,
Partner en advocaat

Den Haag, 1 oktober 2025

KPN B.V.,
namens deze,
V. Cibic,
Executive Vice President Chief Information Security Officer

Den Haag, 30 september 2025

Mnemonic A.S.,
namens deze,
F. van der Heijden,
Senior Security Consultant

Den Haag, 30 september 2025

NFIR B.V.,
namens deze,
A. van der Sluijs,
Algemeen Directeur

Den Haag, 30 september 2025

Northwave Nederland B.V.,
namens deze,
P. Oldengarm,
President / CCO

Utrecht, 7 oktober 2025

Orange Cyber Defense Netherlands B.V.,
namens deze,
D. de Geus,
Managing Director

Utrecht, 6 oktober 2025

Sogeti Nederland B.V.,
namens deze,
R. Jonkers,
Division Manager Security & Technology Transformation

Den Haag, 30 september 2025

Tesorion Operations B.V.,
namens deze,
E. de Jong,
Chief Research Officer

Huizen, 8 oktober 2025

ThalesCyber Premium Solutions Nederland B.V.,
namens deze,
R. Wagterveld,
Director CPS NL

Helsinki, 13 oktober 2025

WithSecure Corporation,
namens deze,
P. Palumbo,
Vice President

BIJLAGE 1 OVERZICHT DEELNEMENDE PUBLIEKE EN PRIVATE PARTIJEN

Overzicht van de deelnemende publieke en private partijen.

Publieke partijen:
- Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
- Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
- Nationaal Cyber Security Centrum (NCSC)
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
- De politie
- Dienst ICT Uitvoering (DICTU)

Private partijen:
- Attic B.V.
- Conclusion Enablement B.V.
- Connect2Trust
- Cyberveilig Nederland (CVNL)
- DEFION Security Netherlands B.V.
- Deloitte Consultative Services B.V.
- DTACT, een merknaam van DutchSec Ventures B.V.
- ESET Nederland
- Eye Security B.V.
- Fox-IT B.V.
- Hunt & Hackett B.V.
- Invictus Incident Response B.V.
- Kennedy van der Laan N.V.
- KPN B.V.
- Mnemonic A.S.
- NFIR B.V.
- Northwave Nederland B.V.
- Orange Cyberdefense Netherlands B.V.
- Sogeti Nederland B.V.
- Tesorion Operations B.V.
- Thales Cyber Premium Solutions Nederland B.V.
- WithSecure Corporation

BIJLAGE 2 GEZAMENLIJKE VERWERKING VAN PERSOONSGEGEVENS

Partijen spreken af dat zij in het kader van de activiteiten, bedoeld in artikel 3, tweede lid, van het convenant, ieder met inachtneming van de voor hen geldende wettelijke kaders, de volgende soorten en categorieën persoonsgegevens ten aanzien van de volgende betrokkenen gezamenlijk verwerken:

Categorieën betrokkenen, categorieën en soorten persoonsgegevens

Categorie betrokkenen	Soorten persoonsgegevens	Categorieën persoonsgegevens
Werknemer van partijen die deelnemen aan de samenwerking	– Naam, Voornaam, en voorletters – Zakelijke telefoonnummer en e-mailadres – Organisatie en functie	Gewoon
Natuurlijk persoon die doelwit of slachtoffer is van een cyberdreiging of incident	– IP-adres – Accountnaam – E-mailadres – Domeinnaam – MAC-adres	Gewoon
Natuurlijk persoon die verantwoordelijk is voor cyberdreigingen of incidenten of daaraan heeft bijgedragen	– IP-adres – Accountnaam – E-mailadres – Domeinnaam – MAC-adres	Gewoon

Ontvangers van de persoonsgegevens en gezamenlijke verantwoordelijkheid

Partijen spreken af dat de informatie en adviezen die voortkomen uit de gezamenlijke analyses, indien het NCSC niet heeft deelgenomen aan de betreffende analyse, worden gedeeld met het NCSC ten behoeve van het verrichten van de activiteiten, bedoeld in artikel 3, derde lid, van het convenant. Gelet op voorgaande kan het NCSC in voorkomende gevallen ook ontvanger zijn. Daarnaast zijn derde belanghebbende partijen, die bovenbedoelde informatie en adviezen ontvangen van het NCSC of door een andere partij verstrekt krijgen, ontvanger.

BIJLAGE 3 GEZAMENLIJKE PRIVACYVERKLARING

Partijen spreken af dat de gezamenlijke privacyverklaring, bedoeld in artikel 6 van het convenant, als volgt luidt:

Gezamenlijke Privacyverklaring

De deelnemende partijen hechten veel belang aan de privacy. Partijen gaan daarom ook bij het maken van gezamenlijke analyses van cyberdreigings- en incidentinformatie en het op basis daarvan opstellen van adviezen, zorgvuldig om met persoonsgegevens en zorgen ervoor dat de verwerkingen daarvan voldoen aan geldende wet- en regelgeving.

Toepassingsgebied van deze Gezamenlijke Privacyverklaring

Deze gezamenlijke privacyverklaring is van toepassing op de gezamenlijke verwerkingen van persoonsgegevens door de partijen bij het convenant samenwerking Cyclotron in het kader van bovenbedoelde gezamenlijke activiteiten.

Deze Gezamenlijke Privacyverklaring is niet van toepassing op alle overige verwerkingen van persoonsgegevens in het kader van de uitvoering van het convenant door de daaraan deelnemende partijen.

Contactpunt

Partijen hebben een contactpunt ingericht voor de verzoeken en bezwaren van betrokkenen. Het contactpunt wordt beheerd door het NCSC. De contactgegevens van het NCSC zijn als volgt:

Nationaal Cyber Security Centrum
t.a.v. de privacy officer
Postbus 117
2501 CC Den Haag
Ook kunt u direct contact opnemen via dit mailadres.

Welke persoonsgegevens verwerken wij?

In het kader van de bovenbedoelde gezamenlijke activiteiten worden de volgende (soorten) persoonsgegevens verwerkt:
- Contactgegevens van medewerkers van deelnemende partijen aan de samenwerking: naam, voornaam, voorletters, zakelijk mailadres, zakelijk telefoonnummer, organisatie en functie;
- Gegevens van een natuurlijk persoon die doelwit of slachtoffer is van een cyberdreiging of incident: IP-adres, accountnaam, e-mailadres, domeinnaam en MAC-adres;
- Gegevens van een natuurlijk persoon die verantwoordelijk is voor cyberdreigingen of incidenten of daar aan heeft bijgedragen: IP-adres, accountnaam, e-mailadres, domeinnaam en MAC-adres;

Op basis van welke grondslagen

Partijen nemen deel aan de bovenbedoelde gezamenlijke activiteiten indien en voor zover dat mogelijk is op basis van de eigen wettelijke en andere juridische kaders.

Het doel van de verwerking

De samenwerking Cyclotron, waarbinnen bovenbedoelde gezamenlijke activiteiten worden verricht, heeft als doel om gezamenlijk een beter beeld te krijgen van cyberdreigingen en incidenten. Hierdoor kunnen partijen hun werkzaamheden beter uitoefenen en belanghebbende organisaties beter worden geïnformeerd. De digitale weerbaarheid van organisaties in Nederland wordt hiermee verhoogd.

Hoelang bewaren wij uw persoonsgegevens?

De gezamenlijke verwerkingsverantwoordelijken bewaren uw persoonsgegevens niet langer dan nodig is voor het bereiken van de in deze gezamenlijke privacyverklaring genoemde doeleinden. Uw persoonsgegevens worden maximaal twee jaar bewaard.

Welke rechten heeft u als betrokkene?

De persoon over wie de persoonsgegevens gaan, noemen we de betrokkene. De betrokkene heeft op grond van de wetgeving hierover een aantal rechten, zoals:

- het recht om te verzoeken of wij persoonsgegevens van u verwerken en indien dit het geval is, het recht op inzage in uw persoonsgegevens en bepaalde informatie over de verwerking van uw persoonsgegevens;
- het recht op rectificatie van uw persoonsgegevens indien deze onjuist of onvolledig zijn;
- het recht om uw persoonsgegevens te laten wissen (‘recht op vergetelheid’);
- het recht om bezwaar te maken tegen de verwerking van uw persoonsgegevens;
- het recht op beperking van de verwerking van uw persoonsgegevens;
- het recht op ontvangst of afgifte van je persoonsgegevens aan een door u aangewezen derde in een gestructureerde, gangbare en machineleesbare vorm (‘recht op dataportabiliteit’).

Om uw rechten uit te oefenen is door de gezamenlijke verwerkingsverantwoordelijken het bovenbedoelde contactpunt ingericht. U kunt contact opnemen met het contactpunt per post of mail onder gebruikmaking van de contactgegevens die aan het begin van deze Gezamenlijke Privacyverklaring zijn vermeld.

Beveiliging

De persoonsgegevens die in het kader van de bovenbedoelde gezamenlijke activiteiten, gezamenlijk worden verwerkt, worden door passende technische en organisatorische maatregelen beschermd.

Wijzigingen

De partijen bij het convenant samenwerking Cyclotron behouden zich het recht voor deze privacyverklaring aan te passen. De meest recente versie is te vinden op deze pagina.

U wordt geadviseerd met enige regelmaat deze pagina te checken.

Vragen en klachten

Heeft u een klacht of vraag over de manier waarop in het kader van bedoelde gezamenlijke activiteiten wordt omgegaan met uw persoonsgegevens? Dan kunt u via e-mail of post contact opnemen met de privacyofficer van het NCSC. De gegevens staan vermeld onder ‘Contactpunt’.

Wanneer u het niet eens bent met de manier waarop de samenwerking Cyclotron uw klacht behandelt, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens.

BIJLAGE 4 BEHANDELING VERZOEKEN EN BEZWAREN BETROKKENEN

De procedure voor de behandeling van verzoeken en bezwaren van betrokkenen, bedoeld in artikel 7 van het convenant, met betrekking tot de gezamenlijke verwerking van persoonsgegevens in het kader van het verrichten van de activiteiten, bedoeld in artikel 3, tweede lid, van het convenant, luidt als volgt:

Procedure voor behandelen verzoeken en bezwaar van betrokkenen:

Ontvangst:

- Het verzoek wordt ingediend bij het contactpunt, ofwel direct of via een deelnemende partij. Het contactpunt verifieert de identiteit van de betrokkene. Indien de betrokkene een bovenbedoeld verzoek of bezwaar heeft ingediend bij een van de partijen bij het convenant en dat verzoek of bezwaar betrekking heeft op een gezamenlijke verwerking van persoonsgegevens in bovenbedoelde zin, zendt die partij dat verzoek of bezwaar door naar het contactpunt. Indien het verzoek of bezwaar is ingediend bij het contactpunt en ziet op de individuele verwerkingsverantwoordelijkheid van een partij, stuurt het contactpunt het verzoek of bezwaar ter verdere behandeling door naar die partij.
- Het contactpunt ontvangt het verzoek via de post of via de mail.
- In een verzoek of bezwaar van de betrokkene dienen de volgende gegevens te worden opgenomen:
  - De naam van de betrokkene
  - De contactgegevens van de betrokkene
  - Een omschrijving van het verzoek of bezwaar
  - [optioneel] bewijs van bevoegde vertegenwoordiging van de betrokkene
- Indien het ontvangen verzoek of bezwaar niet reeds alle gegevens bevat, zal het contactpunt de betrokkene verzoeken om de ontbrekende gegevens aan te vullen.

Registratie en ontvangstbevestiging

- Het contactpunt registreert het verzoek van betrokkene per omgaande, onder vermelding van datum van ontvangst van het verzoek of bezwaar.
- Het contactpunt inventariseert welke partijen betrokken zijn bij de gezamenlijke verwerking waarop het verzoek of bezwaar van betrokkene ziet en informeert die partijen over de ontvangst van het verzoek.
- Op basis van de ontvangen gegevens stelt het contactpunt de identiteit van de betrokkene vast en stuurt het de betrokkene een ontvangstbevestiging.

Controle

- Het contactpunt beoordeelt het verzoek of bezwaar op:
  - de identiteit van de indiener van het verzoek of bezwaar en diens eventuele vertegenwoordigers;
  - de machtiging van eventuele vertegenwoordigers;
  - aard en omvang van het verzoek of bezwaar.
- Bij constatering van een gebrek in het verzoek of bezwaar, informeert het contactpunt de betrokkene daar schriftelijk over.

Inhoudelijke behandeling

- Een verzoek of bezwaar wordt door betrokken partijen gezamenlijk en in onderling overleg inhoudelijke behandeld, onder coördinatie van het contactpunt, met inachtneming van de voor hun geldende wettelijke kaders.
- Het contactpunt stelt vast welk recht de betrokkene wenst uit te oefenen. Partijen onderzoeken, onder coördinatie van het contactpunt, vervolgens:
  - of aan de criteria voor het uitoefenen van dat recht is voldaan; en
  - of een uitzonderingsgrond ten aanzien van het verzoek of bezwaar van toepassing is.
- Betrokkene wordt, binnen een maand, door het contactpunt geïnformeerd over de voortgang van het verzoek of bezwaar.
- Afhankelijk van de complexiteit van het verzoek of het bezwaar, kan deze termijn met twee maanden worden verlengd.

Schriftelijke beslissing en verdere afronding

- Partijen stellen, onder coördinatie van het contactpunt, op basis van de inhoudelijke behandeling,

een schriftelijke concept beslissing op het verzoek of bezwaar van de betrokkene op.
– De gezamenlijke verwerkingsverantwoordelijke partijen nemen, ieder voor zich, een schriftelijke beslissing op het verzoek of bezwaar van de betrokkene.

BIJLAGE 5 PASSENDE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

Hieronder volgt een overzicht van de maatregelen die partijen ten minste ter bescherming van persoonsgegevens die gezamenlijk worden verwerkt in het kader van het verrichten van de activiteiten, bedoeld in artikel 3, tweede lid, van het convenant, nemen.

Partijen spreken met betrekking tot de (bouw en de) instandhouding van de functionaliteit voor de activiteiten, bedoeld in artikel 3, tweede lid, af dat de maatregelen overeenkomstig de Baseline Informatiebeveiliging Overheid (BIO) in acht worden genomen. Aanvullend hierop (voor zover de BIO hier reeds niet in voorziet) gelden minimaal de volgende maatregelen:

Technische beveiligingsmaatregelen:
- Logische en fysieke (toegangs)beveiliging en beveiliging van apparatuur.
- Autorisatiebeheer (least privilage).
- Logging en monitoring.
- Beheer van technische kwetsbaarheden (‘patch management’).
- Software up-to-date houden, zoals browsers, virusscanners en besturingssystemen.
- Back-ups maken waarmee de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig kan worden hersteld.
- Verouderde gegevens automatisch verwijderen.
- Gegevens versleutelen (encryptie).
- Hashing gebruiken als methode om persoonsgegevens te pseudonimiseren.
- Compartimentering van netwerken/databases.
- Dataminimalisatie.

Organisatorische beveiligingsmaatregelen:
- Mensen verantwoordelijkheden toewijzen voor informatiebeveiliging.
- Beveiligingsbewustzijn vergroten bij bestaande en nieuwe medewerkers.
- Procedures opstellen om op gezette tijdstippen de beveiligingsmaatregelen te testen, te beoordelen, te evalueren en eventueel aan te scherpen.
- Regelmatig de logbestanden controleren.
- Een protocol opstellen voor de afhandeling van datalekken en beveiligingsincidenten.
- Per verwerking het besluitvormingsproces en de achterliggende overwegingen vastleggen.

Evaluatie

Partijen spreken af om jaarlijks de te nemen maatregelen te evalueren en te updaten indien nodig.

BIJLAGE 6 AFSPRAKEN BETREFFENDE INBREUK IN VERBAND MET PERSOONSGEGEVENS (DATALEKPROCEDURE)

Procedure voor beoordeling

In het geval van een datalek dat betrekking heeft op de gezamenlijke verwerking van persoonsgegevens in het kader van het verrichten van de activiteiten, bedoeld in artikel 3, tweede lid, van het convenant, zal de Partij die de inbreuk ontdekt de andere Partijen en het contactpunt ter stond voorzien van alle relevante informatie met betrekking tot het datalek. Partijen spreken af dat in geval van een datalek in bovenbedoelde zin de gezamenlijke beoordeling hiervan wordt gecoördineerd door het contactpunt.

Daarbij wordt de volgende procedure in acht genomen:

- De partij die het datalek ontdekt voorziet de andere partijen, voor zover mogelijk, van een beschrijving van de situatie, waarin zo mogelijk is opgenomen:
  a. *de oorzaak van het datalek;*
  b. *de datum waarop het ontstaan is;*
  c. *de datum en het tijdstip waarop is kennisgenomen van het datalek;*
  d. *wat voor soort persoonsgegevens gelekt zijn;*
  e. *hoeveel persoonsgegevens gelekt zijn? Om hoeveel personen het gaat en om hoeveel gegevens per persoon;*
  f. *een inschatting van het aantal en type (mogelijk) getroffen Betrokkenen (gaat het om kwetsbare groepen, klanten, werknemers);*
  g. *hoeveel onbevoegden bij benadering (mogelijk) toegang tot de gelekte persoonsgegevens hadden of hebben;*
  h. *zicht op de onbevoegden, kwaadwillende of betrouwbare partner;*
  i. *of er vooraf maatregelen getroffen waren waardoor de gelekte persoonsgegevens (deels) ontoegankelijk zijn voor onbevoegden? Zoals door versleuteling;*
  j. *duurt het datalek nog voort of zijn maatregelen getroffen om verder misbruik te voorkomen (welke maatregelen en wanneer ingevoerd).*
- Partijen beoordelen gezamenlijk, onder coördinatie van het contactpunt, het datalek, doen zo nodig nader onderzoek en bepalen welke mitigerende maatregelen er nodig zijn om de schadelijke gevolgen te beperken of te stoppen.
- Partijen beoordelen daarnaast gezamenlijk, onder coördinatie van het contactpunt, of het datalek bij de Autoriteit Persoonsgegevens moet worden gemeld en of mededeling hierover gedaan moet worden bij de betrokkenen.
- Partijen evalueren, onder coördinatie van het contactpunt, het datalek en nemen waar nodig aanvullende maatregelen om herhaling in de toekomst te voorkomen.