CONVENANT

Ferm-Zeehavens

2026

Partijen:

Dit convenant wordt aangegaan door Stichting Ferm-Zeehavens met de zeehavenbeheerders Port of Moerdijk, Groningen Seaports, North Sea Port, Port of Amsterdam en Port of Rotterdam (hierna gezamenlijk aangeduid als: **"Zeehavens"**), de publieke partners, de partijen uit de cruciale ketens van de Zeehavens en overige havenfaciliteiten en -dienstverleners in de haven, **"Convenant"**.

Stichting Ferm-Zeehavens, Zeehavenbeheerders, de publieke partners en de partijen uit de cruciale ketens worden gezamenlijk aangeduid als **"Partijen"** en afzonderlijk als **"Partij"**.

Overwegingen:

A. Partijen binnen zeehavens krijgen in toenemende mate te maken met (nieuwe) dreigingen en risico's die gepaard gaan met de voortschrijdende digitalisering van de samenleving en hun interne bedrijfsvoering;

B. Partijen deel uitmaken van, en in hoge mate afhankelijk zijn van andere Partijen in, een cruciale keten die ondersteund wordt door IT-ketenomgevingen die versnipperd en complex zijn en waarin centrale regie op informatiebeveiliging vrijwel ontbreekt;

C. Partijen stellen vast dat de Zeehavenbeheerders en partijen uit de cruciale ketens aantrekkelijke doelwitten vormen voor cybercriminelen en statelijke actoren, waardoor cyberaanvallen een reëel en groeiend risico zijn voor Partijen;

D. Cyberincidenten kunnen verstrekkende en organisatie-overstijgende gevolgen hebben, zoals maatschappelijke ontwrichting en economische schade op grote schaal;

E. Een slagvaardige, snelle samenwerking en onderlinge informatiedeling, noodzakelijk om de digitale weerbaarheid van de zeehavens te verbeteren en bovenstaande risico's te beheersen;

F. Partijen op grond van de Europese NIS2-richtlijn verplicht kunnen worden om maatregelen te treffen om aan de zorgplicht te voldoen, zoals de beveiliging van de toeleveringsketens en relaties met directe dienstverleners;

G. Stichting Ferm-Zeehavens is door de Zeehavenbeheerders opgericht met als doel het verhogen van de cyber weerbaarheid en veerkracht van cruciale ketens waarin Partijen actief (kunnen) zijn binnen de Zeehavens ten aanzien van cybersecurity en andere digitale verstoringen;

H. Partijen spreken- vanwege het ontbreken van een havenbrede aanpak - af om samen te werken om digitale risico's te verminderen, de impact van incidenten te beperken en adequaat te kunnen reageren op digitale dreigingen. Partijen werken verder samen om risico's te beperken door te voldoen aan (toekomstige) regelgeving;

I. De ketenafhankelijkheid vraagt om gezamenlijke weerbaarheid, aangezien de bedrijfscontinuïteit van individuele havenorganisaties nauw verweven is met die van de totale keten. Dit betekent in eerste plaats dat de interne beveiligingsmaatregelen

noodzakelijk zijn, maar dat daarnaast door samenwerking de digitale weerbaarheid en veerkracht van het gehele ecosysteem effectief dient te worden versterkt. Hiervoor is een uniforme aanpak nodig en dienen partijen collectief verantwoordelijk te zijn voor de beveiliging;

J. Partijen verklaren zich op grond van het bovengenoemde gezamenlijk in te zetten voor het verminderen van digitale risico's, het beperken van de impact van incidenten en het adequaat reageren op digitale dreigingen;

K. In dit Convenant maken partijen afspraken over de samenwerking, informatie-uitwisseling en de uitvoering van gezamenlijke activiteiten.

1. Begripsomschrijving

In dit Convenant wordt verstaan onder:

ART-Ferm	De ketentest die vanuit Ferm-zeehavens wordt georganiseerd wordt gebaseerd op het Advanced Red Teaming (ART) raamwerk wat in meerdere sectoren al succesvol wordt ingezet.
Cruciale keten	De combinatie van een Cruciaal proces en de Cruciale organisaties die bij dit proces horen.
Cruciaal proces	Een proces dat binnen één of meerdere zeehavens is geïdentificeerd wanneer de verstoring, uitval of manipulatie ervan zulke ernstige gevolgen kan hebben dat de continuïteit van (onderdelen van) de haven in gevaar komt. Dit kan bijvoorbeeld leiden tot: • significante economische schade, • niet behalen strategische doelen, • imagoschade, • langdurige milieugevolgen, • verstoring van militaire ondersteuning, • of ernstige verstoring van andere processen. Voorbeelden van cruciale processen in de haven zijn • Afwikkelen scheepvaartverkeer • Afhandelen van (container) logistiek • Overslag, verwerking en/of opslag van olieproducten • Overslag, verwerking en/of opslag van kolen • Overslag, verwerking en/of opslag van LNG • Overslag, verwerking en/of opslag van overige bulkgoederen • Overslag, verwerking en/of opslag van breakbulk goederen • Overslag, verwerking en/of opslag van chemieproducten • Opwek en/of transport van elektriciteit
Ferm-zeehavens	Stichting Ferm-zeehavens, door de Zeehavens opgerichte stichting met als doel het verhogen van de (cyber) weerbaarheid en veerkracht van cruciale ketens binnen de Zeehavens ten aanzien van cybersecurity en andere digitale verstoringen.
Overige havenfaciliteiten en -dienstverleners	Organisaties die voor de uitvoering van hun activiteiten gebonden zijn aan een van de zeehavens, maar niet noodzakelijk zijn voor de uitvoering en/of continuïteit van een cruciaal proces in de haven.
Publieke partners	Publiekrechtelijke organisaties die betrokken zijn bij dit Convenant, waaronder maar niet beperkt tot de Havenmeester, veiligheidsregio's, Omgevingsdiensten, het

	Nationaal Cybersecurity Center en de (Zeehaven) politie, waarmee Ferm-zeehavens samenwerkafspraken heeft gemaakt.
Red teaming	Met een realistisch aanvalsscenario een hacktest uitvoeren op een bepaalde scope.
Veerkracht	Het vermogen om effectief te herstellen na een Cyberincident.
Weerbaarheid	Het vermogen om dreigende Cyberincidenten te herkennen, voorkomen of af te weren.

2. Algemeen

2.1 Doel van de samenwerking

2.1.1 Het doel van deze samenwerking is het verhogen van de (cyber)weerbaarheid en veerkracht van cruciale ketens binnen de (zee)havens gelegen in Nederland ten aanzien van cyber security en andere digitale verstoringen.

2.1.2 Het is geen commerciële samenwerking en het is nadrukkelijk niet de bedoeling dat Partijen potentiële concurrentiegevoelige informatie zullen delen, in geval van twijfel over de vraag of bepaalde informatie concurrentiegevoelig is, zal eerst contact gezocht worden met juristen voor advies over of dit gedeeld mag worden.

2.2 Bestuur en taakstelling van Ferm-Zeehavens

2.2.1 Ferm-Zeehavens wordt geleid door een dagelijks bestuur. Het dagelijks bestuur neemt zelfstandig besluiten en behoeft geen instemming van Partijen.

2.2.2 Ferm-zeehavens plant op regelmatige basis overleggen in tussen Partijen om de voortgang en strategie toe te lichten. Ook kan Ferm-zeehavens werkgroepen instellen.

2.2.3 Ferm-Zeehavens doet het onderstaande om het onder artikel 2.1 genoemde doel te bereiken:

A. Regievoering: verhogen van de digitale weerbaarheid en veerkracht van Cruciale ketens binnen de Zeehavens door o.a kennis te verzamelen en te analyseren van cruciale ketens en bijbehorende dreigingen, risico's, actuele volwassenheidsniveaus en afhankelijkheden van derden; Ferm-Zeehavens bouwt een kennisbank en stelt nadere processen en dreigingsanalyses op. Verder voert Ferm-zeehavens de ART-Ferm uit;

B. Belangenbehartiging: het behartigen van de gezamenlijk belangen van Partijen op het gebied van digitale Weerbaarheid en ketenveiligheid richting overheid, andere instanties en (inter)nationale netwerken; en

C. Verbinder: Ferm-Zeehavens faciliteert dat Cruciale organisaties onderling informatie en kennis kunnen uitwisselen, onder meer door het organiseren van bijeenkomsten, het ondersteunen van initiatieven en het stimuleren van vertrouwen tussen Partijen.

2.2.4 Hiervoor richt Ferm-Zeehavens zich voor Cruciale organisaties en Overige havenfaciliteiten en -dienstverleners tot de volgende taken:

A. Het doorlopend verzamelen en ontvangen van voor Partijen (mogelijk) relevante informatie over incidenten;

B. Het doorlopend verzamelen en ontvangen van voor Partijen (mogelijk) relevante actuele en urgente kwetsbaarheden, dreigingen en Indicators of Compromise; het (proactief en gericht) delen van deze informatie met aangesloten Partijen en partnerorganisaties die hier (mogelijk) belang bij hebben;

C. Het actief identificeren van incidenten die bij meerdere Partijen tegelijkertijd spelen en het – indien door betrokkenen gewenst – coördineren van gezamenlijke acties in deze gevallen; en

D. Het monitoren op, en delen van, sectorspecifieke kennis op het terrein van cyber security.

2.2.5 Aanvullend hierop kan de Ferm-Zeehavens vrijblijvend de volgende taken uitvoeren:

A. Het bieden van handelingsperspectieven en/of het adviseren over de afhandeling van incidenten; en

B. Het signaleren van meer algemene (niet-urgente) gemeenschappelijke kwetsbaarheden en het aandragen van oplossingen hieromtrent.

2.2.6 Ferm-zeehavens richt zich uitsluitend op het verhogen van de Weerbaarheid en Veerkracht van de Cruciale ketens en niet op de Weerbaarheid en Veerkracht van individuele organisaties. Deze verantwoordelijkheid rust op de Partijen zelf.

2.2.7 Ferm-zeehavens verricht geen activiteiten die vallen onder incident response zoals gedefinieerd in de context van Computer Emergency Response Teams (CERT). Hieronder wordt mede verstaan:

- Het actief reageren op cyberincidenten;
- Het uitvoeren van technische analyses of forensisch onderzoek; en
- Het bieden van directe ondersteuning bij het mitigeren of oplossen van digitale dreigingen.

2.2.8 In het geval van een incident moeten Partijen dit zelfstandig melden bij de relevante toezichthouder. Partijen informeren Ferm-zeehavens over ieder incident dat relevant kan zijn voor andere Partijen.

3. Individuele verplichtingen bij samenwerking

3.1 Inspanningen individuele organisaties

3.1.1 De ondertekenende Partijen spannen zich in om op een actieve en constructieve wijze tot een vruchtbare samenwerking te komen. In het kader van deze samenwerking is iedere Partij gehouden de volgende inspanningen te leveren:

A. Iedere Partij wijst minimaal één vast aanspreekpunt aan voor cybersecurity die verantwoordelijk is voor de coördinatie van informatie-uitwisseling en incidentrespons. Deze persoon is verantwoordelijk op managementniveau. In het

geval dit redelijkerwijs niet mogelijk is, zal het vaste aanspreekpunt beslissingen intern op managementniveau afstemmen; Van dit aanspreekpunt voorziet de Partij Ferm-zeehavens van actuele contactgegevens van dit aanspreekpunt waaronder ten minste een (standaard) e-mailadres en telefoonnummer;

B. Partijen delen (onderling) vertrouwelijke informatie over dreigingen, kwetsbaarheden en incidenten, met als doel het gezamenlijk verhogen van de situational awareness en het beperken van schade;

C. Iedere Partij voert periodiek een risicoanalyse uit van haar eigen kritische processen en verbindingen met andere ketenpartners, gericht op het identificeren van kwetsbaarheden en afhankelijkheden;

D. Partijen staan toe dat Ferm-Zeehavens periodiek van buitenaf scans uitvoert op kwetsbare systemen die via het internet te benaderen zijn, met als doel vroegtijdige detectie van potentiële risico's;

E. Partijen voorzien Ferm-zeehavens hiertoe van technische gegevens over hun eigen IT-landschap, waaronder in gebruik zijnde domeinnamen, URL's, IP-adressen/ranges en eventuele AS-nummers;

F. Partijen spannen zich in om kwetsbaarheden die keteneffecten kunnen veroorzaken, zo snel mogelijk na identificatie te verhelpen; en

G. Partijen geven toestemming voor het delen van actuele dreigingsinformatie met publieke partners in het veiligheidsdomein (zoals veiligheidsregio's, havenmeesters en omgevingsdiensten), mits deze informatie geanonimiseerd en niet herleidbaar is tot individuele partijen.

3.2 Gezamenlijke inspanning Cruciale organisaties onderdeel van een Cruciale keten

3.2.1 Partijen die onderdeel zijn van een cruciale keten spreken af gezamenlijk initiatieven te nemen om risico's en dreigingen voor de keten als geheel beter in beeld te brengen en aan te pakken. Deze samenwerking omvat de volgende onderdelen:

A. Cruciale organisaties stellen gezamenlijk dreigingsanalyses op gericht op relevante dreigingen voor de keten en actualiseren deze;

B. Cruciale organisaties voeren gezamenlijk risicoanalyses uit gericht op onderlinge afhankelijkheden en digitale kwetsbaarheden binnen de keten;

C. Cruciale organisaties nemen actief deel aan collectieve oefeningen die gericht zijn op het verbeteren van de gezamenlijke respons op Cyberincidenten binnen de keten; en

D. Cruciale organisaties nemen deel aan of ondersteunen ketenbrede penetratietesten, red teaming en security audits om de digitale weerbaarheid van de keten te toetsen.

3.2.2 Partijen delen de bevindingen uit gezamenlijke activiteiten vertrouwelijk en geanonimiseerd. Ferm-Zeehavens zorgt voor coördinatie van rapportages en opvolging hiervan.

3.2.3 Partijen waarborgen dat informatie die wordt gedeeld uitsluitend feitelijkheden en géén persoonsgegevens bevat.

3.2.4 Om de assessments en overige onderzoeken uit te kunnen voeren en een goede opvolging aan de uitkomsten van de assessments te kunnen geven, zullen Partijen minimaal de onder 3.1.1 en 3.2.1 concreet genoemde activiteiten uitvoeren. Voor het overige geldt dat Partijen in algemene zin:

A. Actief participeren: Partijen spannen zich in om tijd, capaciteit en expertise beschikbaar te stellen voor deelname aan werkgroepen, oefeningen, kennisdeling en andere vormen van samenwerking;

B. Informatie delen: Binnen de kaders van vertrouwelijkheid en wettelijke vereisten, waaronder het mededingingsrecht, delen Partijen relevante informatie over dreigingen, kwetsbaarheden, incidenten en best practices om gezamenlijke risico's inzichtelijk te maken en de ketenweerbaarheid te versterken;

C. Deelnemen aan oefeningen: Partijen nemen deel aan gezamenlijke simulaties en oefeningen, assessments en leveren input voor dreigingsbeelden, scenario-ontwikkeling en opvolging; en

D. Doorvoeren van verbetermaatregelen: Op basis van inzichten uit samenwerking, oefeningen en incidenten spannen Cruciale organisaties en Zeehavens zich in om relevante verbetermaatregelen toe te passen binnen hun eigen processen en systemen. In het geval Cruciale organisaties de door Ferm-zeehavens vastgestelde verbetermaatregelen niet doorvoert, zal Ferm-zeehavens de Cruciale organisatie een redelijke termijn gunnen om alsnog de verbetermaatregelen door te voeren. Laat de Cruciale organisatie dit na dan zal Ferm-zeehavens op directieniveau een escalatiegesprek voeren en behoudt Ferm-zeehavens zich het recht voor om de samenwerking ingevolge artikel 4.2.3 te beëindigen.

3.2.5 Ferm-Zeehavens geeft de Zeehavens en Cruciale organisaties:

A. Toegang tot gedeelde kennis en middelen: Zeehavens en Cruciale organisaties kunnen waar mogelijk gebruik maken van gezamenlijk ontwikkelde kennisproducten, richtlijnen, scenario's en hulpmiddelen die binnen het kader van deze samenwerking beschikbaar worden gesteld. In het geval kennis en middelen, materialen samen wordt ontwikkeld verkrijgt Ferm-zeehavens de rechten van intellectueel eigendom daarop, welke zij, voorzover dit een verdere ontwikkeling betreft van de door de Zeehavens aan Ferm-zeehavens verstrekte materialen aan de Zeehavens overdraagt conform de met de Zeehavens gemaakte afspraken in de Samenwerkingsovereenkomst d.d. [*] en de Cruciale

partijen om niet een eeuwigdurend recht op het gebruik van de kennis, middelen en materialen verkrijgen voor het versterken van de Weerbaarheid en Veerkracht van hun eigen organisaties; en

B. Inspraak in samenwerking en besluitvorming: Zeehavens en Cruciale organisaties hebben de mogelijkheid actief deel te nemen aan de door Ferm-zeehavens geïnitieerde overleggen / werkgroepen, om voorstellen te doen en agendapunten in te brengen.

3.3 Normeringen

3.3.1 Partijen spannen zich in om te voldoen aan een passend beveiligingsniveau voor de eigen organisatie. Hiervoor kunnen standaarden zoals NIST, ISO27001 of 62443, CyFun, BIO, of CYRA kunnen worden gebruikt.

4. Toetreding en uittreding

4.1 Aansluiting als Cruciale organisatie

4.1.1 De samenwerking vangt aan op 1 januari 2026. De Cruciale organisaties worden Partij bij dit Convenant na ondertekening van het hiervoor bestemde intekenformulier (appendix 1).

4.2 Uittreding

4.2.1 Een Cruciale organisatie kan met inachtneming van een opzegtermijn van zes maanden de samenwerking onder dit Convenant voor zover het haar betreft opzeggen door de directie van Ferm-zeehavens schriftelijk per aangetekende brief van dit besluit in kennis te stellen. De verplichtingen tussen partijen blijven gedurende de opzegtermijn van kracht.

4.2.2 Ferm-zeehavens behoudt zich het recht voor om de samenwerking met een Partij eenzijdig te beëindigen indien:

A. de betreffende Partij structureel tekortschiet in de naleving van de afspraken zoals vastgelegd in dit Convenant; en/of

B. sprake is van gedrag, handelingen of uitlatingen die het vertrouwen in de samenwerking of de reputatie van het samenwerkende Partijen kunnen schaden.

4.2.3 Voordat Ferm-Zeehavens overgaat tot beëindiging van de samenwerking, stelt zij de betreffende Partij schriftelijk in gebreke met betrekking tot de geconstateerde tekortkoming(en) en biedt zij, indien mogelijk, een redelijke termijn om alsnog na te komen. Indien nakoming uitblijft of blijvend onmogelijk is, kan de samenwerking worden beëindigd middels een schriftelijke opzegging.

5. Overige bepalingen

5.1 Evaluatie

5.1.1 Uiterlijk één (1) jaar na ondertekening van het Convenant, vindt een evaluatie samenwerking plaats. Partijen zullen indien gewenst de opzet en werking van de eerste versie van dit Convenant aanpassen. Evaluaties vinden vervolgens minimaal elke twee (2) jaar plaats.

5.2 Geheimhouding

5.2.1 Partijen verplichten zich tot geheimhouding van alle vertrouwelijke informatie die zij in het kader van dit Convenant van elkaar verkrijgen. Onder vertrouwelijke informatie wordt verstaan: alle schriftelijke, mondelinge of anderszins verstrekte gegevens waarvan Partijen weten of redelijkerwijs kunnen vermoeden dat deze een vertrouwelijk karakter hebben. De ontvangende Partijen betrachten hierbij ten minste dezelfde mate van zorg en nemen ten minste dezelfde maatregelen in acht als dat ze voor de bescherming van hun eigen vertrouwelijke informatie betrachten en in acht te nemen.

De verplichting tot geheimhouding geldt niet voor:

- het delen van vertrouwelijk informatie binnen de eigen organisatie van een Partij aan personen die een geheimhoudingsverplichting hebben, voor zover noodzakelijk voor de uitvoering van dit Convenant;
- indien openbaarmaking wordt vereist door enige wet- of regelgeving, of een bevel of instructie tot openbaarmaking wordt gegeven door een bevoegde autoriteit;
- indien de vertrouwelijke informatie op of na de datum van dit Convenant openbaar is geworden, anders dan door een toerekenbare tekortkoming van een Partij, dan wel enig ander onrechtmatig handelen waarvan de betrokken Partij op het moment van openbaarmaking wist of redelijkerwijs had kunnen weten dat deze onrechtmatig was;
- voor zover openbaarmaking geschiedt in het kader van het doel van dit Convenant aan professionele adviseurs of opdrachtnemers van de openbaar makende Partij, onder oplegging van een gelijkwaardige geheimhoudingsverplichting; of
- voor zover openbaarmaking geschiedt van informatie noodzakelijk voor de verantwoording aan de aandeelhouders van Partijen.

5.2.2 Partijen zullen onderling nadere schriftelijk afspraken maken voor het delen van data in het kader van de assessments en de opvolging hiervan.

5.2.3 Informatie die tussen Partijen wordt gedeeld wordt geclassificeerd op basis van het zogeheten Traffic Light Protocol (TLP). Deze classificatie geeft de vereiste mate van vertrouwelijkheid van de informatie aan. Het TLP onderscheidt vier categorieën:

- TLP:RED
  Deze informatie mag alleen worden gedeeld door de informatie-eigenaar zelf,

mag nooit verder worden verspreid door de ontvanger, ook niet binnen de Partij, en mag niet worden genoteerd op papier of in digitale vorm.

- TLP:AMBER
  Deze informatie is beperkt tot de Partijen aan wie de informatie wordt verstrekt en degenen binnen hun organisatie die weet moeten hebben van deze informatie om actie te kunnen ondernemen (hetzij directe medewerkers, consultants, aannemers of ingeleend personeel). Informatie mag, mits goed beveiligd/beschermd worden gedeeld per e-mail. Het minimale niveau van beveiliging om de informatie per e-mail te versturen is middels een met een wachtwoord beschermde zipfile.
- TLP:GREEN
  Deze informatie mag uitsluitend onder gelijksoortige organisaties binnen de brede gemeenschap of sector worden gedeeld, en mag bijvoorbeeld wel worden gepubliceerd op een gesloten internetforum, maar niet op een openbaar toegankelijke website. Er geldt geen beperking voor het delen met ICT-toeleveranciers.
- TLP:WHITE
  Er is geen beperking op het delen.

5.2.4 Indien een Partij haar ICT-diensten heeft uitbesteed, is het toegestaan om aan de betreffende ICT-dienstverlener instructies te verstrekken die voortvloeien uit informatie geclassificeerd als TLP:RED of TLP:AMBER, mits te allen tijde volledig wordt geborgd dat de inhoud van de betreffende informatie zelf niet aan deze dienstverlener wordt verstrekt. De Partij blijft verantwoordelijk voor het naleven van de vertrouwelijkheidsclassificatie en draagt zorg voor passende technische en organisatorische maatregelen ter waarborging.

5.2.5 Als de betreffende Partij geen classificatieniveau conform artikel 5.2.3 toekent aan de informatie, wordt deze informatie geacht te zijn gekenmerkt als TLP: AMBER en de bron van informatie TLP:RED.

5.3 Inspanningsplicht

5.3.1 De afspraken in dit Convenant zijn gebaseerd op wederzijds vertrouwen en vrijwillige samenwerking tussen de betrokken partijen. Dit is niet vrijblijvend, van Partijen wordt verwacht dat zij zich inspannen om de overeengekomen doelstellingen te bereiken.

5.4 Duur en beëindiging

5.4.1 Dit Convenant is gesloten voor (de) bepaalde duur van drie (3) jaar. Het Convenant treedt in werking met ingang van 1 januari 2026 en eindigt van rechtswege op 31 december 2028, tenzij (een deel van de) Partijen schriftelijk overeenkomen dit Convenant te verlengen in welk geval de verlenging zal gelden tussen de Partijen die dat zijn overeengekomen.

5.4.2 Artikel 5.2 Vertrouwelijkheid en 5.5 Toepasselijk recht en geschillen en alle andere bepalingen uit dit Convenant die naar hun aard en bedoeling, bedoeld zijn om ook

na de beëindiging van dit Convenant van Kracht hun werking tussen Partijen te behouden, blijven onverminderd van kracht na de beëindiging van dit Convenant.

5.5 Toepasselijk recht en geschillen

5.5.1 Dit Convenant en de overeenkomsten die ter uitvoering van of in samenhang met dit Convenant worden gesloten en alle niet-contractuele verplichtingen die voortvloeien uit of verband houden met dit Convenant, inclusief geschillen over de geldigheid van dit Convenant worden beheerst door en zullen worden uitgelegd overeenkomstig Nederlands recht.

5.5.2 Partijen zullen trachten elk geschil in goed overleg en te goeder trouw op te lossen. Indien Partijen het relevante verschil niet naar hun tevredenheid minnelijk hebben kunnen regelen, zal dit bij uitsluiting worden voorgelegd aan de bevoegde rechter te Rotterdam.