Ministerie van Economische Zaken en Klimaat

Handleiding
Economische Veiligheid

Inleiding

Dit is de handleiding Economische Veiligheid van de Rijksoverheid. Deze handleiding licht toe wat economische veiligheid is, waarom dat voor jouw bedrijf relevant is en welke concrete stappen je kunt zetten om jouw bedrijf weerbaarder te maken.

Machtsverhoudingen in de wereld verschuiven, en landen zetten in toenemende mate economische (druk)middelen in om geopolitieke doelen te bereiken. Kennis en technologie zijn daarbij een strategisch wapen geworden: chipmachines, halfgeleiders, AI-modellen, biotechnologie, kwantumtechnologie. Wie deze technologie beheerst, heeft economische én militaire troeven in handen. Landen investeren daarom gericht in het verwerven ervan, via legale weg, zoals overnames en samenwerkingen, maar ook via spionage, dwang en beïnvloeding.

Die kennis en technologie beschermen kan de overheid niet alleen. Jij kent je eigen bedrijf, je 'kroonjuwelen' en je partners beter dan wie dan ook. Economische veiligheid is dan ook niet langer alleen een overheidsvraagstuk, maar een onderdeel van goed ondernemerschap. De overheid biedt het kader en de ondersteuning; jij bepaalt en voert de maatregelen uit die passen bij de risico's voor jouw bedrijf.

Bijna alles wat je als ondernemer doet, heeft daar invloed op. Of je nu nieuw personeel aanneemt, een samenwerking aangaat, of je toeleveringsketen inricht. Bij elke keuze die je maakt, zitten risico's voor je kennis en technologie. De gevolgen kunnen direct je bedrijfscontinuïteit raken: verlies van concurrentievoordeel, reputatieschade, financiële schade, of zelfs het verliezen van zeggenschap over je eigen onderneming. Het is daarom belangrijk om deze risico's niet alleen in kaart te brengen, maar er ook de nodige maatregelen tegen te treffen.

In deze handleiding zitten klikbare links naar bronnen van derden.
Raadpleeg het document daarom bij voorkeur digitaal.

Inhoudsopgave

1. Economische veiligheid

Economische veiligheid 5
Wat is economische veiligheid? 5

2. Bescherm wat je sterk maakt

De vier clusters 8

2.1 Bescherm je product

Maatregelen voor het beschermen van je product 9
Casus 10

2.2 Bescherm je omgeving

Maatregelen voor het beschermen van je omgeving 11
Casus 12

2.3 Bescherm je samenwerking

Maatregelen voor het beschermen van je samenwerking 13
Casus 14

2.4 Bescherm je groei

Maatregelen voor het beschermen van je groei 15
Casus 16

3. Wettelijke kaders en compliance

Investeringstoetsing: de Wet vifo 18
Exportcontrole van strategische goederen 19

4. Stappenplan economische veiligheid

Stap 1:
Weet wat je sterk maakt 21

Stap 2:
Ken de risico's 21

Stap 3:
Maak een actieplan 21

1 Economische veiligheid

1. Economische veiligheid

Maar waar zitten die risico's precies? Internationaal zakendoen, het aantrekken van investeringen en fuseren horen allemaal bij ondernemen in een kennisintensieve sector. Jij bent als ondernemer voortdurend op zoek naar kansen, maar moet tegelijk waakzaam zijn voor risico's. Deze handleiding behandelt de maatregelen op het gebied van economische veiligheid voor jou als ondernemer. Voordat je maatregelen neemt om je bedrijf te beschermen, is het belangrijk om in kaart te brengen waar de kwetsbaarheden zitten.

Deze handleiding biedt handvatten, zodat je de risico's zo zelfstandig mogelijk kunt aanpakken. Je leest wat de Rijksoverheid voor je kan betekenen en wat de basis is van de wettelijke kaders rond economische veiligheid. Zo weet je waar je rekening mee moet houden bij de doorontwikkeling van je onderneming.

Heb je na het lezen van deze handleiding vragen over economische veiligheid?

Kijk dan op de website www.maakjebedrijfweerbaar.nl voor meer informatie of neem contact op via het contactformulier.

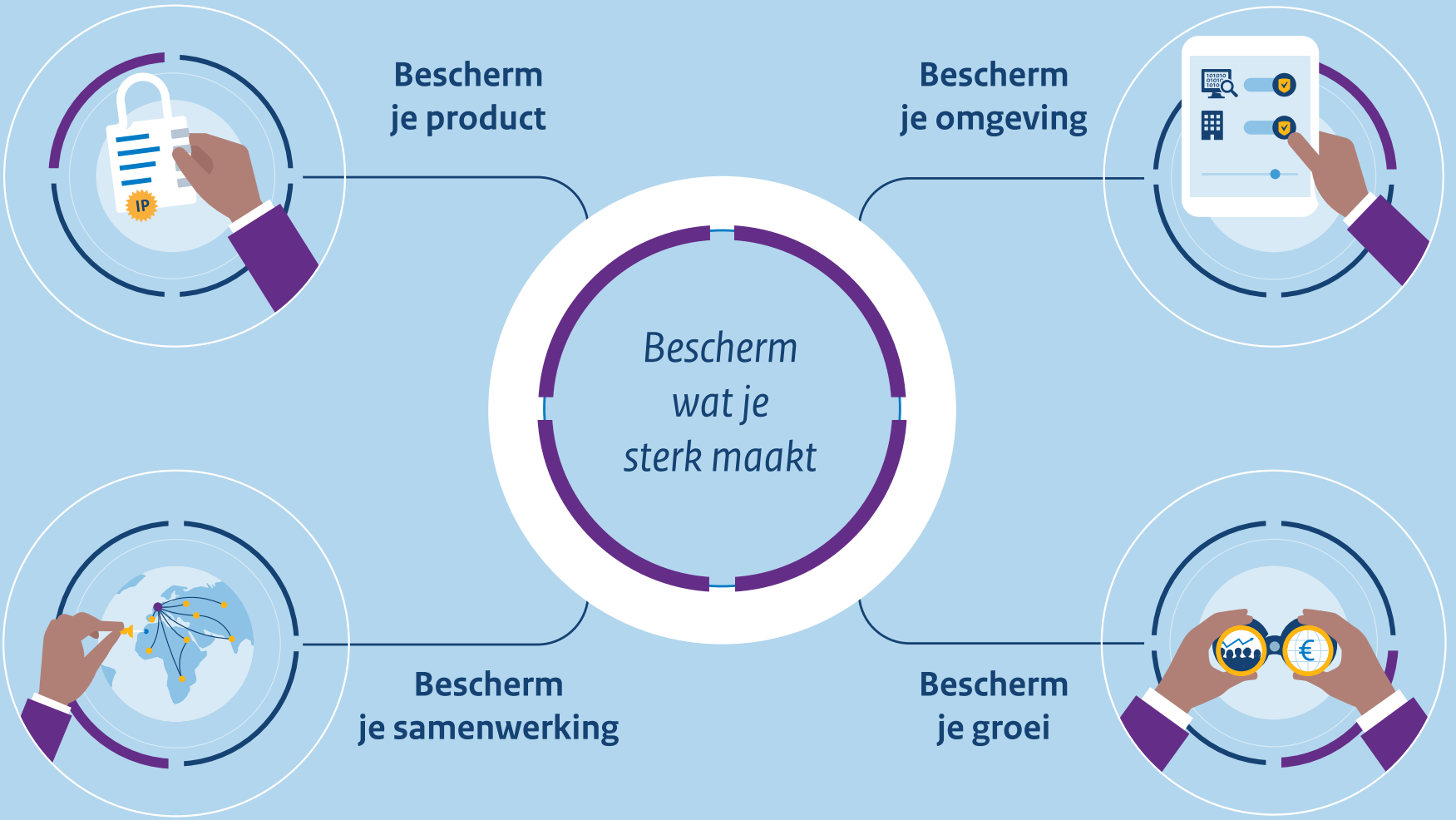
Wat is economische veiligheid?

Economische veiligheid gaat in de kern over het beschermen van je kennis en je technologie. Als kennisintensieve ondernemer bouw je aan iets waardevols. Technologie, kennis en producten waarin je hebt geïnvesteerd en die je onderscheiden in de markt. Economische veiligheid gaat erom dat jij dat kunt beschermen: tegen diefstal, cyberaanvallen, dwang en ongewenste beïnvloeding door statelijke actoren. Wat voor jou telt als concurrentievoordeel, telt namelijk net zo goed als nationaal belang. Als kennisintensieve bedrijven zoals dat van jouw kwetsbaar zijn, raakt dat ook de Nederlandse economie, de toeleveringsketens en de vitale infrastructuur waar we met z'n allen van afhankelijk zijn. Preciezer gezegd: economische veiligheid betekent het beschermen van de economie, toeleveringsketens, technologie en vitale infrastructuur tegen externe risico's en afhankelijkheden.

Met externe risico's bedoelen we dreigingen vanuit het buitenland die jouw bedrijf, de economie of de nationale veiligheid kunnen schaden. Denk aan economische afhankelijkheid, verstoring van toeleveringsketens, economische dwang, cyberaanvallen en het weglekken van unieke technologie, zoals halfgeleider- of kwantumtechnologie.

Maar hoe bescherm jij als ondernemer wat je hebt opgebouwd? Juist kennisintensieve producten en diensten, zoals onderzoek naar of ontwikkeling van cruciale (dual-use) technologie, zijn een aantrekkelijk doelwit. Jouw bedrijf beschermen is dan ook niet alleen in je eigen belang, maar ook van gemeenschappelijk belang.

2 Bescherm wat je sterk maakt


Bescherm je product
Bescherm je omgeving
Bescherm wat je sterk maakt
Bescherm je samenwerking
Bescherm je groei

2. Bescherm wat je sterk maakt

Economische veiligheid gaat over het beschermen van je kennis en je technologie. Bijna alles wat je als ondernemer doet, heeft daar invloed op. Of je nu nieuw personeel aanneemt, een samenwerking aangaat, of je toeleveringsketen inricht. Bij elke stap neemt het risico toe dat je de controle over je kennis en technologie ongewenst gedeeltelijk of geheel verliest. Het is daarom belangrijk om deze risico's in kaart te brengen en de nodige maatregelen te treffen.

De vier clusters

Maar waar begin je? Economische veiligheid raakt in de praktijk bijna elk onderdeel van je onderneming, van je bedrijfsvoering en onderzoeksafdeling tot je reisbeleid en je samenwerkingen. Om dat behapbaar te maken, is economische veiligheid onderverdeeld in clusters. Elk cluster kijkt naar een ander onderdeel van je bedrijfsvoering en de risico's die zich daarbinnen kunnen voordoen. Alle clusters hangen met elkaar samen: een zwakke plek in je samenwerkingen kan bijvoorbeeld net zo goed je product raken als een lek in je digitale omgeving dat kan doen.

De vier clusters bieden houvast om systematisch te bepalen waar je kwetsbaar bent en waar je dus als eerst maatregelen zou moeten nemen:

- **Bescherm je product**: je uitvindingen, kennis en technologie die uniek zijn voor je bedrijf.
- **Bescherm je omgeving**: je digitale en fysieke werkplek, je reizen naar het buitenland en de veiligheid van je informatie.
- **Bescherm je samenwerking**: de bedrijven waar je spullen van koopt en de partners waarmee je samenwerkt.
- **Bescherm je groei**: je medewerkers, je vestigingen in het buitenland en je investeringen.

Door in kaart te brengen hoe veiligheid samenhangt met jouw product, omgeving, samenwerkingen en groei, bescherm je niet alleen je huidige positie, maar verstevig je deze ook. Het nemen van maatregelen vraagt aandacht en focus én het is een belangrijke investering in je continuïteit en groei. Ze helpen je voorop te blijven lopen.

Op de website 'Maak je bedrijf weerbaar' vind je maatregelen per cluster.

2.1 Bescherm je product

Jouw kennis, product of dienst is jouw ‘kroonjuweel’, de basis waarop je bedrijf gebouwd is. Logischerwijs wil je dat beschermen. Het beschermen van je waardevolle kennis en producten vraagt een strategische aanpak die verder gaat dan alleen bewustzijn. Er zijn verschillende instrumenten beschikbaar om je intellectueel eigendom, bedrijfsgeheimen en technische knowhow effectief te beveiligen. Of het nu gaat om het registreren van octrooien, het classificeren van vertrouwelijke informatie of het maken van waterdichte samenwerkingsafspraken, elke situatie vraagt om specifieke maatregelen.

De maatregelen die je kunt treffen voor het (juridisch) beschermen van jouw kenniskapitaal zijn uiteenlopend. Dit kan bijvoorbeeld via het vastleggen van intellectueel eigendom en octrooien. Maar ook door het veilig omgaan met bedrijfsgeheimen, het structureren van samenwerkingen en het operationeel beveiligen van je kenniskapitaal.

Maatregelen voor het beschermen van je product

- Breng in kaart welke technologie, kennis, werkwijzen en data jouw bedrijf uniek maken en je concurrentievoordeel opleveren (dit zijn je kroonjuwelen).
- Combineer octrooien en bedrijfsgeheimen slim: vraag octrooi aan voor de zichtbare delen en houd de kennis erachter geheim.
- Breng per informatiebron en medewerker in kaart welke toegang vereist is en scherm de informatie voor alle anderen af (het ‘need-to-know’-principe).
- Leg vóór de start van een samenwerking vast welke kennis en technologie (intellectueel eigendom) je zelf al bezit en inbrengt.
- Maak afspraken over nieuwe kennis die tijdens een samenwerking ontstaat en leg vast wie eigenaar wordt van nieuwe resultaten en welke gebruiksrechten de andere partij krijgt.
- Zet duidelijke afspraken op papier over eigendom, gebruiksrechten en licenties van kennis en uitvindingen.
- Zorg dat je toegangsrechten kunt intrekken, gegevens kunt terugvorderen of laten vernietigen en dat geheimhoudingsverplichtingen ook na afloop van de samenwerking blijven gelden.

Wat kun je doen om je intellectueel eigendom (IE) te beschermen?
IE-recht verschilt van land tot land, ook binnen de EU en een geregistreerd recht is geen garantie: je zult zelf actief moeten monitoren of het wordt geschonden. Ga daarnaast goed na hoe je medewerkers, leveranciers en samenwerkingspartners omgaan met je vertrouwelijke kennis en leg bij elke samenwerking vooraf vast wie welke kennis inbrengt, wie eigenaar wordt van nieuwe resultaten en wat er gebeurt met gedeelde kennis als de samenwerking stopt.

Voor advies op maat over de keuze tussen octrooi en bedrijfsgeheim, over samenwerkingsafspraken, of over IE-bescherming in het buitenland, kun je terecht bij het Octrooicentrum Nederland. Je kunt ook hulp zoeken bij een advocatenkantoor dat gespecialiseerd is in het land van samenwerking en contact leggen met de Nederlandse ambassade daar. De plaatselijke ambassade heeft vaak een goed kennisnetwerk in het land waar je wilt zakendoen.

Casus

Eindelijk was het moment daar! De CEO van tech-start-up A kon haar geluk niet op toen zij bericht ontving dat hun beoogde partner bedrijf B, gevestigd in land C, akkoord wilde gaan met een formele samenwerking in land C. In deze samenwerking zou de R&D plaatsvinden in Nederland, maar het productieproces in land C. Of de CEO van tech-start-up A volgende week naar land C wilde komen om daar formeel de samenwerking te ondertekenen?

De CEO van tech-start-up A lichtte alvast haar investeerders in. Deze waren blij te horen dat hun investeringen zich nou eens zouden gaan uitbetalen, na al die jaren van geduld, tijd en moeite. Het moment van ondertekening was dan nu eindelijk daar. Op de bovenste verdieping van een imposante wolkenkrabber in het zakendistrict van de hoofdstad van land C kwamen de ingewijden van tech-start-up A en bedrijf B samen. Het banket stond al klaar en op de centrale tafel lag een stapel documenten. De CEO van tech-start-up A nam plaats en bekeek de documenten – sommigen kwamen haar bekend voor, maar er lagen ook nieuwe documenten bij welke gingen over de uitwisseling van technologische kennis en het delen van de rechten rondom deze technologie. Ze keek met een vragende blik richting de vertegenwoordigers van bedrijf B. “Waar komt dit vandaan?”

Het antwoord van bedrijf B was weinig geruststellend: “Onze excuses mevrouw, maar wij hebben ook net pas gehoord dat buitenlandse partijen verplicht zijn om in hun rechten omtrent hun technologische kennis met ons te delen als we in land C een zakelijke samenwerking aangaan.” Het zweet brak uit bij de CEO van tech-start-up A: “Wat nu? Ons IE is het bestaansrecht van onze onderneming, als we deze afstaan hebben we niks meer dat ons uniek maakt. Kan ik nog weglopen? En wat zullen onze investeerders hiervan vinden?

Op de website ‘Maak je bedrijf weerbaar’ vind je meer informatie over de maatregelen om je product te beschermen.

2.2 Bescherm je omgeving

Je kunt je fysieke en digitale omgeving door het nemen van verschillende maatregelen beschermen. Maatregelen zijn er ook voor internationale reizen en informatieveiligheidsbeleid.

Je organisatie draait op een veilige digitale en fysieke basis. Cyberaanvallen, een slecht beveiligd kantoor, onveilige personeelsidentificatie of risicovolle dienstreizen kunnen een ingang vormen tot jouw waardevolle kennis en technologie.

Bij bezoeken aan jouw bedrijf loop je het risico dat gasten op plekken in jouw pand komen waarvoor ze niet geautoriseerd zijn. Ook online kan een ongewenste gast zomaar binnenkomen: open daarom niet zomaar e-mails en klik niet zonder nadenken op links. Bij het reizen naar het buitenland lopen jij en je collega's eveneens risico's. Je kunt bespioneerd worden door kwaadwillende statelijke actoren of concurrenten en apparaten of datadragers met gevoelige informatie kunnen worden gestolen. Mogelijke gevolgen hiervan zijn: je raakt je IE kwijt, je wordt gechanteerd, er ontstaat een datalek, je bedrijf loopt imagoschade op of je verliest een stuk van je onderhandelingspositie.

Maatregelen voor het beschermen van je omgeving

Digitale omgeving

- Maak regelmatig back-ups van je belangrijkste bestanden.
- Stel tweefactorauthenticatie in voor inloggen in meerdere stappen.
- Zet automatische updates aan voor alle systemen en software.
- Gebruik actuele antivirussoftware op alle apparaten.
- Controleer de beveiligingsstandaarden van je e-mailsysteem.
- Leer phishing herkennen en train je team hierin.
- Print een bellijst voor noodsituaties en houd deze bij de hand.

Fysieke omgeving

- Creëer bouwkundige scheiding tussen werkruimtes met gevoelige informatie en algemene ruimtes.
- Maak handelingen herleidbaar tot individuele personen.
- Beperk toegang tot logbestanden tot alleen geautoriseerde personen.
- Stel een alarmeringsprocedure op voor beveiligingsincidenten.
- Richt voorzieningen in voor veilige opslag van gevoelige informatie op gegevensdragers en in hardcopy.
- Registreer uitgaande kennis en technologie voor traceerbaarheid.
- Inventariseer informatieveiligheidsrisico's bij transport van gevoelige informatie en prototypes en maak hier overwogen keuzes in.
- Pas je verzendmethode aan bij de gevoeligheid van de informatie.

Internationale reizen

- Wees je bewust van de risico's van het reizen naar bepaalde landen.
- Bespreek vooraf de specifieke risico's van je reisbestemming en evalueer achteraf je ervaringen.
- Zorg dat je weet hoe je omgaat met informatiebeveiliging op externe locaties, beurzen en conferenties.
- Overweeg tijdelijke apparatuur, neem een tijdelijke laptop en telefoon mee in plaats van je standaard werkapparatuur.
- Zorg dat je eigen apparaten geen gevoelige gegevens bevatten als je deze meeneemt.
- Bewaar belangrijke bestanden in de cloud in plaats van lokaal op je apparaten.
- Schakel automatisch zoeken naar netwerken uit om ongewenste verbindingen te voorkomen.
- Zet bluetooth en GPS uit waar mogelijk om lokalisatie te beperken.
- Installeer de nieuwste software op al je apparaten voordat je vertrekt.
- Maak thuis een back-up van belangrijke gegevens die je meeneemt.

Informatieveiligheidsbeleid

- Wijs een veiligheidscoördinator aan als neventaak voor kleinere bedrijven of toegewijde functie voor grotere organisaties.
- Richt een back-upmechanisme in voor het geval van informatieverlies of systeemuitval en test dit mechanisme periodiek.
- Stel een continuïteitsprocedure op die je regelmatig test en evalueert.

Casus

De vertegenwoordiger van bedrijf A, een tech-start-up, reist af naar land B. In land B zal de vertegenwoordiger een internationale conferentie bijwonen en ook werk van zijn bedrijf presenteren. Bedrijf A hoopt zo potentiële investeerders voor hun start-up te werven, dat is hard nodig als ze willen groeien.

Eenmaal geland in land B, staat de vertegenwoordiger in de rij voor de paspoort-controle. Het paspoort is in orde. Dan wordt hem door de douane gevraagd zijn laptop en datadragers af te geven voor controle. De vertegenwoordiger is hier niet over te spreken. Er staat namelijk zeer gevoelige informatie op de laptop en datadragers over het unieke idee waarmee bedrijf A groot wil worden. De douane geeft aan geen reden te hoeven opgeven voor een doorzoeking en dat dit routine is, maar dat de gefrustreerde reactie van de vertegenwoordiger wel erg verdacht is. Ze nemen de laptop en datadragers tijdelijk in beslag voor onderzoek. Ze geven aan contact met de vertegenwoordiger op te nemen als het onderzoek is afgerond.

Een week later wordt de vertegenwoordiger gebeld door de douane: het onderzoek is afgerond en er is niks verdachts gevonden. De vertegenwoordiger mag zijn spullen weer komen ophalen, maar houdt een knagend gevoel over aan het voorval. Wat als de douane alles heeft kunnen lezen en misschien zelfs gekopieerd heeft? En wie heeft het nog meer kunnen inzien?

Op de website 'Maak je bedrijf weerbaar' vind je meer informatie over de maatregelen om je omgeving te beschermen.

2.3 Bescherm je samenwerking

Samenwerken in Nederland en internationaal is essentieel voor je bedrijf én biedt kansen. Maar het brengt ook risico's met zich mee. Een samenwerking vergroot het aantal verbindingen dat je bedrijf heeft met externe partijen, die daardoor meer toegang kunnen krijgen tot je kennis en technologie. Ook kwaadwillende partijen zoeken samenwerking op, bijvoorbeeld om toegang tot je kennis te krijgen, of om die in te zetten voor ongewenste doeleinden. Weet daarom vóórdat je een samenwerking aangaat met wie je écht te maken hebt. Zo verklein je de kans op ongewenste kennisoverdracht en misbruik van je kennis.

Door het extra risico van samenwerking te beheersen help je je bedrijf veilig te groeien. Due diligence naar potentiële partners is daarbij een essentiële stap. Ook uit publiek beschikbare informatie leer je al veel over een partij. Stel jezelf, vóórdat je een samenwerking of partnerschap aangaat, onder meer deze vragen en tref maatregelen om veilig samen te kunnen werken.

Maatregelen voor het beschermen van je samenwerking

Veilig internationaal samenwerken en due diligence

- Onderzoek potentiële partners goed voordat je gaat samenwerken, zodat je de risico's kent: Is de partner verbonden aan een overheid? Denk daarbij aan staatsgeleide bedrijven of instellingen. Is de partner verbonden aan het leger of de defensie-industrie?
- Wie is de 'ultimate beneficial owner' (UBO): de eigenaar, belanghebbende of degene met zeggenschap?
- Heeft de organisatie een aantoonbare reputatie in de relevante sector? Ontbreekt expertise, of is onduidelijk hoe de samenwerking aansluit bij de normale activiteiten van de partner? Wees dan extra alert.
- Welke andere activiteiten onderneemt de partner? Is deze verbonden aan meerdere bedrijven, instellingen of organisaties?
- Welke IE-rechten heeft de potentiële partner geregistreerd en in welke landen? Dit geeft een indruk van de belangen van de partner. Onderzoek dit in databanken als Espacenet, DesignView en TMView. Het Octrooicentrum Nederland kan je hierbij ondersteunen.
- Verloopt het contact via een andere entiteit (andere naam of ander adres) dan de partnerorganisatie zelf, of verandert dit tijdens het proces?
- Geeft de partner geen duidelijke antwoorden over de beoogde toepassing van onderzoeksresultaten? Maakt de partner om onduidelijke redenen bezwaar tegen standaardbepalingen, of stelt deze excessieve geheimhoudingseisen voor?
- Maak duidelijke afspraken met je samenwerkingspartner(s) over hoe jullie omgaan met gegevens en controleer regelmatig of jullie je aan deze afspraken houden.

Leg ter voorbereiding contact met de Nederlandse ambassade in het land van je potentiële partner. Die heeft vaak een goed kennisnetwerk en weet mogelijk of de partner daar bekend is. Ook andere overheidsnetwerken kunnen je ondersteunen bij zakendoen in het buitenland. **Bekijk de pagina 'Ondernemen in het buitenland' voor meer informatie**.

Risicofactoren bij potentiële investeerders, leveranciers of partners

- Er is weinig tot geen informatie over de opdrachtgever of financier te vinden, bijvoorbeeld geen website.
- De partner gebruikt een entiteit (andere naam of ander adres) die ongebruikelijk is voor dit type financiering.
- De opdrachtgever of financier biedt uitzonderlijk gunstige voorwaarden en vraagt daar bijna niets voor terug.
- De opdrachtgever of financier wil resultaten niet laten publiceren, stelt uitzonderlijk strenge IE-eisen, of eist geheimhouding over eindgebruikers en specificaties.

Casus

De Nederlandse hightech-onderneming A ontwikkelt gezichtsherkenningssoftware. Het idee achter de software is dat het gebruikt kan worden door sociale media-apps, om de kwaliteit van zogenaamde gezichtsfilters te verbeteren. De hightech-onderneming wordt benaderd door een bedrijf waar het nog niet eerder van gehoord heeft, afkomstig uit land B. Het bedrijf presenteert zich als een opkomend sociale mediaplatform en legt uit hoe het gebruik wil maken van de software van onderneming A, om ook voor hun sociale media gebruik te kunnen maken van leuke gezichtsfilters. Zij stellen voor de dienst te willen afnemen. Ook bieden zij aan om diagnostische gegevens van hun gebruikers terug te geven aan hightech-onderneming A, om de software nóg efficiënter te maken.

Hightech-onderneming A is zich ervan bewust dat de gezichtsherkenningssoftware naast het creëren van grappige filters op sociale media, potentieel óók misbruikt kan worden. Zo kunnen autoritaire regimes de hoogontwikkelde software bijvoorbeeld gebruiken om personen op te sporen op het internet. Zoals altijd doet hightech-onderneming A een verkennend onderzoek via openbare bronnen. En zo vindt hightech-onderneming A dat het bedrijf uit land B actief wordt gesteund door de autoritaire regering van land B. Het is algemeen bekend dat deze regering zich veelvuldig schuldig maakt aan de onderdrukking van bepaalde bevolkingsgroepen in land B. Hightech-onderneming A ziet dat er een directe connectie is tussen de overheid van land B en het 'opkomende sociale media platform' uit land B. Hightech-onderneming A ziet een te groot risico op misbruik van hun software voor het schenden van mensenrechten in land B. Met als gevolg dat export van het product van hightech-onderneming A zeer onwenselijke gevolg.

Op de website 'Maak je bedrijf weerbaar' vind je meer informatie over de maatregelen om je samenwerking te beschermen.

2.4 Bescherm je groei

Jouw bedrijf kan groeien door investeringen, je personeel, het opzetten van buitenlandse vestigingen en export. Maar groei maakt je ook kwetsbaar. Onbetrouwbaar kapitaal, personeel met toegang tot bedrijfsgeheimen, fouten bij export, of regels die je over het hoofd ziet, kunnen je duur komen te staan. Om veilig te groeien kun je de volgende maatregelen nemen.

Maatregelen voor het beschermen van je groei

Personeel

- Verifieer identiteit van kandidaten en onderzoek CV's grondig, controleer of personen zijn wie ze beweren te zijn.
- Pas het 'need-to-know'-principe toe. Geef geen onnodige toegang tot processen of informatie die niet nodig zijn voor het werk.
- Houd toegangsrechten van medewerkers bij in een rechtenmatrix voor overzicht en controle.
- Zet accounts direct op non-actief en neem bedrijfsmiddelen in na beëindiging van het dienstverband.
- Maak regels voor verantwoord gebruik van ICT-bedrijfsmiddelen.
- Train personeel in verantwoord en veilig omgaan met gevoelige kennis, technologie en informatie.

Vestiging buitenland

- Verdiep je grondig in lokale wetten en regels rond de ondernemingsvorm die je kiest.
- Controleer lokale wetten en regels als je data of software op lokale servers wilt plaatsen, sommige autoriteiten kunnen data opeisen.
- Controleer of je technologie valt onder lokale exportcontroles bij het betreden van nieuwe markten.

Investeringen

- Doe grondig onderzoek naar partijen waarvan je investeringen zoekt, inclusief alle gerelateerde partijen (investeringsconsortia, fondsbeheerders, alternatieve contacten), de herkomst van de gelden, onverwachte commerciële, politieke of militaire banden en of partijen onder Nederlandse exportcontroles of sancties vallen.
- Voer een vroege risicoanalyse uit voor beter geïnformeerde beslissingen, mitigerende maatregelen en een sterkere onderhandelingspositie.
- Bepaal bij buitenlandse investeerders welke data en informatie geschikt zijn om te delen.
- Controleer zo nodig bij BTI of de transactie een meldingsplicht heeft onder de Wet investeringen, fusies en overnames (Wet vifo) of compliance pagina in deze handleiding.

Casus

De frustratie had zich geleidelijk opgebouwd, maar afgelopen donderdag was voor werknemer A toch écht de druppel die de emmer deed overlopen. Deze donderdag had hij een functioneringsgesprek met zijn manager. Eigenlijk had werknemer A gehoopt dat hij promotie zou krijgen tot teamleider. Dit zou meer dan verdiend zijn geweest na 15 jaar zwoegen aan verschillende nieuwe voertuigmodellen, zo vond werknemer A zelf. In plaats daarvan kreeg hij tegenvallend nieuws te horen: de positie was naar collega B gegaan. Werknemer A had collega B nota bene zelf nog ingewerkt. Voor werknemer A was de maat nu vol. Sinds deze tegenvaller is werknemer A alleen maar bezig geweest met wraak. Hij heeft zich voorgenomen om – onopvallend, maar geleidelijk – de blauwdrukken van een revolutionair, nieuw voertuigdesign van zijn werkgever te kopiëren en te verkopen aan de hoogste bieder. Voor werknemer A maakt het niet meer uit wie deze hoogste bieder is.

Op de website ‘Maak je bedrijf weerbaar’ vind je meer informatie over de maatregelen om je groei te beschermen.

3 Wettelijke kaders en compliance

3. Wettelijke kaders en compliance

Er zijn in Nederland verschillende wetten die betrekking hebben op economische veiligheid en weerbaarheid. Het huidige geopolitieke landschap vergroot de essentie van wet- en regelgeving en vraagt soms om uitbreiding ervan. Deze handleiding beschrijft de wet- en regelgeving die van toepassing is op het beschermen van jouw kennis en technologie.

Investeringstoetsing: de Wet vifo

Op 1 juni 2023 trad de Wet Veiligheidstoets investeringen, fusies en overnames (Wet vifo) in werking. De wet introduceert een veiligheidstoets voor investeringen, fusies en overnames die mogelijk een risico vormen voor de nationale veiligheid. De toets geldt voor specifieke vitale aanbieders, beheerders van bedrijfscampussen en ondernemingen die beschikken over (zeer) sensitieve technologie. Het kabinet heeft besloten tot een uitbreiding van deze wet per 1 januari 2027. Het voornemen is het toevoegen van 6 technologieën waarbinnen een veiligheidstoets kan plaatsvinden.

Huidige technologieën (sinds 2023)

- Kwantumtechnologie (quantum)
- Fotonicatechnologie
- Halfgeleidertechnologie (semiconductors/chips)
- High assuranceproducten (informatiebeveiliging)
- Dual-use producten (goederen en technologie voor zowel civiel als militair gebruik)
- Militaire goederen (defensie-industrie)

Nieuwe technologieën (per 1 januari 2027)

- Biotechnologie (deels, zoals stamceltechnologie en zaadveredeling)
- Kunstmatige intelligentie (AI)
- Geavanceerde materialen
- Nanotechnologie
- Sensor- en navigatietechnologie
- Nucleaire technologie voor medisch gebruik

Vitale aanbieders zijn partijen die een dienst aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. Vitale aanbieders in de telecom-, gas- en elektriciteitssector hebben te maken met hun eigen sectorale investeringstoetsing, afgestemd op de kenmerken van de sector. Onder de Wet vifo vallen daarnaast vitale aanbieders uit allerlei andere sectoren waarover private bedrijven zeggenschap kunnen krijgen, zoals in het bankwezen en het havengebied.

Een fusie, overname of investering is mogelijk risicovol als die kan leiden tot:

- Verstoring van de continuïteit van de vitale infrastructuur. Processen zoals energievoorziening en telecom zijn zo essentieel voor onze samenleving dat uitval of verstoring voor ernstige maatschappelijke ontwrichting zorgt;
- Het weglekken van hoogwaardige kennis of technologie, die via fusies, overnames of investeringen in handen kan komen van een kwaadwillende partij;
- Risicovolle strategische afhankelijkheden, bijvoorbeeld situaties waarin Nederland door een ander land (politiek) onder druk kan worden gezet.

Een melding maken in het kader van de Wet vifo

Valt je voorgenomen verwervingsactiviteit binnen de reikwijdte van de Wet vifo? Dan heb je een wettelijke meldplicht bij het Bureau Toetsing Investeringen (BTI). Zowel investeerders als de onderneming zelf moeten een wijziging van zeggenschap of invloed melden bij het BTI. De wet schrijft melding voor bij:

- Wijzigingen van zeggenschap vanaf 50% bij vitale aanbieders en sensitieve technologie; en
- Wijzigingen van zeggenschap vanaf 10% bij zeer sensitieve technologie.

Je kunt een melding maken op de website van het BTI. Kijk voor meer informatie over de Wet vifo op de website van het BTI. www.bureautoetsinginvesteringen.nl

Exportcontrole van strategische goederen

Produceert je bedrijf strategische goederen? Dan gelden er mogelijk regels bij het exporteren van je goederen, technologie of diensten, omdat die kunnen worden ingezet voor ongewenst eindgebruik. Soms is daarom een exportvergunning van de Nederlandse overheid nodig. Dat geldt onder andere voor de volgende categorieën:

1. Militaire goederen

Militaire goederen staan op de Gemeenschappelijke EU-lijst van militaire goederen. Voorbeelden zijn pantservoertuigen, oorlogsschepen en specialistische militaire apparatuur.

2. Dual-use-goederen

Dual-use-goederen kennen zowel een civiele als een militaire toepassing. Bepaalde brandvertragers worden bijvoorbeeld in de bouw gebruikt, maar ook als grondstof voor gifgas.

3. Strategische diensten

Strategische diensten hangen samen met strategische goederen. Denk hierbij aan reparaties en onderhoud van militaire of dual-use-goederen, gebruiksinstructies en bepaalde softwareleveranties.

4. Sanctiegoederen

Sommige sancties verbieden de export van bepaalde goederen naar het gesanctioneerde land, of onderwerpen die aan een vergunningplicht.

Hoe weet je of je met exportregels te maken hebt?

- Welke dual-use-goederen een exportvergunning vereisen, staat in bijlage I van de EU Dual-Use Verordening (2021/821).
- Militaire goederen staan op de gemeenschappelijke EU-lijst van militaire goederen.
- Je bent zelf verantwoordelijk om na te gaan of je een exportvergunning nodig hebt. Meer informatie vind je op de website van de Rijksoverheid. Twijfel je? Neem dan contact op met de Centrale Dienst voor In- en Uitvoer (CDIU) van de Douane.
- Kom je verdachte aanvragen of bestellingen tegen? Neem dan contact op met de Unit Contra-proliferatie van de AIVD en de MIVD. Heb je een ABRO-autorisatie, neem dan contact op met het Nationaal Bureau Industrieveiligheid van de AIVD en MIVD.

4 Stappenplan economische veiligheid

4. Stappenplan economische veiligheid

Een gericht plan voor de bescherming van jouw kennis en technologie geeft je bedrijf grip op risico's. Met het EV-stappenplan breng je stap voor stap in kaart wat jouw belangrijkste assets zijn en hoe je deze kunt beschermen. Zo versterk je wat je al goed doet en bescherm je je bedrijf tegen kwaadwillenden.

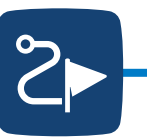
Stap 1: Weet wat je sterk maakt

Begin met het in kaart brengen van de technologie, kennis, processen en data die je bedrijf uniek en competitief maken. Denk aan intellectueel eigendom, klant- en werknemersgegevens en de ondersteunende systemen die deze assets mogelijk maken. Prioriteer je assets door ze te rangschikken van hogere naar lagere waarde en bedenk concreet wat het voor je bedrijf betekent als je deze assets verliest of ze in verkeerde handen vallen.

Stap 2: Ken de risico's

Maak een overzicht van je assets met bijbehorende risico's, zodat je inzicht krijgt in mogelijke kwetsbaarheden. Risico's komen uit verschillende hoeken: statelijke actoren, daaraan gelieerde partijen of (cyber)criminelen die via verschillende wegen toegang proberen te krijgen tot je waardevolle kennis en processen. Denk aan digitale systemen die gehackt kunnen worden, personeel met toegang tot gevoelige informatie, toeleveranciers waar je afhankelijk van bent, of investeerders.

Ook je fysieke omgeving en internationale reizen brengen specifieke risico's met zich mee. Door deze risico's systematisch in kaart te brengen per risicogebied, maak je makkelijker een inschatting van de waarschijnlijkheid dat een risico zich voordoet en de impact die dit zou hebben op je bedrijf.



Stap 3: Maak een actieplan

Je hebt je kennis en technologie geprioriteerd en kent de risico's, hun waarschijnlijkheid en mogelijke impact. Nu zet je die kennis om in een gericht actieplan dat je bedrijf weerbaarder maakt. Met dat inzicht stel je gerichte maatregelen op: je plan richt zich op de grootste risico's voor je meest waardevolle assets en identificeert kleinere risico's waarmee je op termijn aan de slag kunt. Zo investeer je je tijd en middelen daar waar ze het meest opleveren.

Aan de slag

De EV-scan
Start met de de EV-scan om inzicht te krijgen in de kwetsbaarheden van jouw bedrijf, Je ontdekt aan de hand van 20 vragen wat de eerste stappen zijn die je kunt zetten om je weerbaarheid te vergroten. **De EV-scan vind je op de website**.

EV Stappenplan praktijkgids
Met de praktijkgids doorloop je stap voor stap het EV-stappenplan: je brengt je belangrijkste assets en risico's in kaart en vertaalt die naar concrete maatregelen en een actieplan. Zo bed je economische veiligheid structureel in, in je bedrijfsvoering. **De praktijkgids is beschikbaar op de website**.

Economische veiligheid in de praktijk
Ter verdieping en inspiratie vind je op de website vier afleveringen van de Podcast 'Bescherm wat je sterk maakt'. **Deze podcast biedt meer achtergrond en verhalen over economische veiligheid in de praktijk**.

Meer weten over economische veiligheid of relevante wet- en regelgeving?

Heb je na het lezen van deze handleiding nog vragen over economische veiligheid in het algemeen of over de wet- en regelgeving waar je mee te maken kunt krijgen?

Op **de website 'Maak je bedrijf weerbaar'** vind je de uitgebreide maatregelen, de EV-scan, het EV-stappenplan en praktijkverhalen van andere ondernemers.

Kom je er via de website niet uit of heb je advies nodig over jouw specifieke situatie? Dan kun je altijd terecht bij het Ondernemersloket Economische Veiligheid via **veiligondernemen@rvo.nl**. Het Ondernemersloket beantwoordt je vraag of brengt je in contact met de juiste overheidsinstantie.

Deze brochure is een uitgave van:

Ministerie van Economische Zaken en Klimaat
Postbus 20401 | 2500 EK Den Haag
t 070 379 89 11 (ma t/m vrij 9.00 – 21.00 uur)

Oktober 2026